An introduction to the algebra of rings and fields

(Text for Math 332 Winter 2023 and Winter 2025 at Drexel University)

Darij Grinberg

draft, June 24, 2025

Contents

1. Preface **8**
1.1. What is this? . . . 8
1.2. Plan . . . 9
1.3. Notations . . . 10
1.4. Refresher on modular arithmetic . . . 10
1.5. Homework set #0: (de)motivating questions . . . 13

2. Rings and ideals **18**
2.1. Defining rings ([DumFoo04, §7.1]) . . . 18
2.1.1. The definition . . . 18
2.1.2. Some examples of rings . . . 19
2.1.3. Notes on the definitions . . . 28
2.2. Calculating in rings . . . 30
2.2.1. What works in arbitrary rings . . . 30
2.2.2. What doesn't work in arbitrary rings . . . 34
2.2.3. Idempotents . . . 34
2.3. Subrings ([DumFoo04, §7.1]) . . . 35
2.3.1. Definition . . . 35
2.3.2. Examples . . . 36
2.3.3. A first application . . . 41
2.3.4. More computational exercises . . . 43
2.3.5. The center of a ring, and the centralizer of a subset . . . 44
2.4. Zero divisors and integral domains ([DumFoo04, §7.1]) . . . 46
2.5. Units and fields ([DumFoo04, §7.1]) . . . 48
2.5.1. Units and inverses . . . 48

2.5.2. Some exercises on inverses . . . 53
2.5.3. Fields . . . 54
2.6. Fields and integral domains: some connections ([DumFoo04, §7.1]) 55
2.6.1. Fields vs. integral domains . . . 55
2.6.2. When is $\mathbb{Z}/n$ a field? . . . 56
2.6.3. Application: Fermat's Little Theorem . . . 57
2.6.4. Division in a commutative ring . . . 59
2.7. Ring morphisms ([DumFoo04, §7.3]) . . . 60
2.7.1. Definition and examples . . . 60
2.7.2. Basic properties of ring morphisms . . . 66
2.7.3. The image of a ring morphism . . . 68
2.7.4. Basic properties of ring isomorphisms . . . 69
2.7.5. Injective morphisms and their images . . . 71
2.7.6. Advanced exercises on ring isomorphisms . . . 72
2.8. Ideals and kernels ([DumFoo04, §7.1]) . . . 73
2.8.1. Kernels . . . 73
2.8.2. Ideals . . . 73
2.8.3. Principal ideals . . . 75
2.8.4. Other examples of ideals . . . 76
2.9. Quotient rings ([DumFoo04, §7.3]) . . . 80
2.9.1. Quotient groups . . . 81
2.9.2. Quotient rings . . . 82
2.9.3. More examples of quotient rings . . . 86
2.9.4. The canonical projection . . . 93
2.9.5. The universal property of quotient rings: elementwise form 94
2.9.6. The universal property of quotient rings: abstract form . . 100
2.9.7. Injectivity means zero kernel . . . 102
2.9.8. The First Isomorphism Theorem for sets . . . 102
2.9.9. The First Isomorphism Theorem for rings . . . 108
2.9.10. A few remarks on the first isomorphism theorem . . . 113
2.10. Direct products of rings ([DumFoo04, §7.6]) . . . 115
2.10.1. Direct products of two rings . . . 115
2.10.2. Direct products of any number of rings . . . 116
2.10.3. Examples . . . 118
2.10.4. Direct products and idempotents . . . 121
2.10.5. Boolean rings . . . 123
2.11. A few operations on ideals ([DumFoo04, §7.3]) . . . 125
2.12. The Chinese Remainder Theorem ([DumFoo04, §7.6]) . . . 130
2.12.1. Introduction . . . 130
2.12.2. The Chinese Remainder Theorem for two ideals . . . 131
2.12.3. Application to integers . . . 134
2.12.4. Comaximality for products of ideals . . . 135
2.12.5. The Chinese Remainder Theorem for k ideals . . . 138
2.12.6. Applying to integers again . . . 142

2.12.7. Remark on noncommutative rings . . . 147
2.13. Euclidean rings and Euclidean domains ([DumFoo04, §8.1]) . . . 148
2.13.1. All ideals of $\mathbb{Z}$ are principal . . . 148
2.13.2. Euclidean rings and Euclidean domains . . . 149
2.13.3. The (extended) Euclidean algorithm . . . 158
2.14. Principal ideal domains ([DumFoo04, §8.1 and §8.2]) . . . 165
2.14.1. Principal ideal domains . . . 165
2.14.2. Divisibility in commutative rings . . . 165
2.14.3. Gcds and lcms . . . 167
2.14.4. Associate elements . . . 168
2.14.5. Uniqueness of gcds and lcms in an integral domain . . . 170
2.14.6. Existence of gcds and lcms in a PID . . . 170
2.14.7. More about gcds and lcms . . . 172
2.15. Unique factorization domains ([DumFoo04, §8.3]) . . . 174
2.15.1. Irreducible and prime elements . . . 174
2.15.2. Irreducible factorizations and UFDs . . . 177
2.15.3. Gcds and lcms in a UFD . . . 181
2.15.4. Any PID is a UFD . . . 182
2.15.5. A synopsis . . . 183
2.16. Application: Fermat's $p = x^2 + y^2$ theorem ([DumFoo04, §8.3]) . . . 184
2.16.1. Fermat's two-squares theorem . . . 184
2.16.2. Non-primes and numbers of representations . . . 189
2.16.3. Other forms $x^2 + ny^2$ . . . 189
2.16.4. Coda . . . 191
2.17. More about ideals and quotient rings . . . 193
2.17.1. The second isomorphism theorem for rings . . . 193
2.17.2. The third isomorphism theorem for rings . . . 194
2.17.3. The inverse image of an ideal . . . 194
2.17.4. The fourth isomorphism theorem for rings . . . 195
2.17.5. Prime and maximal ideals . . . 196

3. Modules ([DumFoo04, Chapter 10]) 197
3.1. Definition and examples ([DumFoo04, §10.1]) . . . 197
3.1.1. Definition of modules . . . 197
3.1.2. Submodules and scaling . . . 199
3.1.3. Examples . . . 200
3.1.4. Left vs. right R-modules in general . . . 202
3.2. A couple generalities . . . 203
3.2.1. Negation, subtraction and scaling . . . 203
3.2.2. Finite sums . . . 204
3.2.3. Some exercises . . . 205
3.3. More operations on modules and submodules . . . 206
3.3.1. Direct products and direct sums . . . 206
3.3.2. Restriction of modules . . . 210

3.3.3. More examples . . . 213
3.4. Abelian groups as $\mathbb{Z}$-modules ([DumFoo04, §10.1]) . . . 216
3.4.1. The action of $\mathbb{Z}$ by repeated addition . . . 216
3.4.2. A few words on $\mathbb{Q}$-modules and $\mathbb{R}$-modules . . . 218
3.4.3. Repeated addition vs. scaling . . . 219
3.5. Module morphisms ([DumFoo04, §10.2]) . . . 220
3.5.1. Definition . . . 220
3.5.2. Simple examples . . . 221
3.5.3. Ring morphisms as module morphisms . . . 223
3.5.4. General properties of linearity . . . 224
3.5.5. Adding, subtracting and scaling R-linear maps . . . 225
3.5.6. Kernels and images . . . 226
3.6. Quotient modules . . . 227
3.6.1. Definition . . . 228
3.6.2. Examples . . . 229
3.6.3. The universal property of quotient modules . . . 230
3.6.4. The First Isomorphism Theorem for modules . . . 231
3.7. Spanning, linear independence, bases and free modules ([DumFoo04, §10.3]) . . . 234
3.7.1. Definitions . . . 234
3.7.2. Spans are submodules . . . 237
3.7.3. Free modules . . . 238
3.8. The universal property of a free module ([DumFoo04, §10.3]) . . . 250
3.9. Bilinear maps . . . 253
3.10. Multilinear maps . . . 257
3.11. Algebras over commutative rings ([DumFoo04, §10.1]) . . . 258
3.11.1. Definition . . . 258
3.11.2. Examples . . . 259
3.11.3. Rings as $\mathbb{Z}$-algebras . . . 263
3.11.4. The underlying structures . . . 263
3.11.5. Commutative R-algebras . . . 263
3.11.6. Subalgebras . . . 264
3.11.7. R-algebra morphisms . . . 264
3.11.8. Direct products of algebras . . . 265
3.12. Defining algebras: the case of $\mathbb{H}$ . . . 265

4. Monoid algebras and polynomials ([DumFoo04, Chapter 9]) 270
4.1. Monoid algebras . . . 270
4.1.1. Definition . . . 270
4.1.2. Examples . . . 272
4.1.3. Pretending that the elements of M belong to R $[M]$ . . . 277
4.1.4. General properties of monoid algebras . . . 277
4.2. Polynomial rings . . . 281
4.2.1. Univariate polynomials . . . 281

4.2.2. Bivariate polynomials . . . 282
4.2.3. Multivariate polynomials . . . 284
4.2.4. Evaluation, aka substitution for univariate polynomials . 285
4.2.5. Evaluation, aka substitution for multivariate polynomials 289
4.2.6. Constant polynomials . . . 292
4.2.7. Coefficients . . . 292
4.2.8. Renaming indeterminates . . . 293
4.2.9. A remark on noncommutative R . . . 294
4.3. Univariate polynomials . . . 295
4.3.1. Degrees and coefficients . . . 295
4.3.2. Division with remainder . . . 299
4.3.3. Roots . . . 305
4.3.4. Application to $\mathbb{Z}/p$: Wilson revisited . . . 310
4.3.5. Application to $\mathbb{Z}/p$: Sum of k-th powers . . . 312
4.3.6. $F[x]$ is a Euclidean domain . . . 315
4.3.7. Lagrange interpolation . . . 317
4.4. Intermezzo: quotients of R-algebras . . . 325
4.5. Adjoining roots . . . 327
4.5.1. Examples . . . 327
4.5.2. The general construction . . . 336
4.6. Field extensions from adjoining roots . . . 341

5. Finite fields **345**
5.1. Basics . . . 345
5.2. The characteristic of a field . . . 347
5.3. Tools . . . 353
5.3.1. Splitting polynomials . . . 353
5.3.2. Splitting fields . . . 355
5.3.3. The Idiot's Binomial Formula and the Frobenius endomorphism . . . 358
5.3.4. The derivative of a polynomial . . . 361
5.4. Existence of finite fields . . . 365
5.5. Uniqueness of finite fields . . . 369
5.5.1. Annihilating polynomials and minimal polynomials . . . 369
5.5.2. Minimal polynomials in finite fields . . . 376
5.5.3. Each finite field is obtained from $\mathbb{Z}/p$ by a single root adjunction . . . 379
5.5.4. Proof of the uniqueness . . . 382
5.6. Lemmas on p-th powers . . . 383
5.7. An application of root adjunction . . . 385
5.8. Quadratic residues: an introduction . . . 392
5.8.1. Definitions and examples . . . 392
5.8.2. Counting squares . . . 394
5.8.3. Euler's QR criterion . . . 395

5.8.4. The arithmetic of Legendre symbols . . . 398
5.8.5. When -1 is a QR . . . 400
5.8.6. Quadratic reciprocity . . . 401
5.8.7. A sum of Legendre symbols . . . 403
5.8.8. Gaussian sums . . . 406
5.8.9. Proof of quadratic reciprocity for two odd primes . . . 410
5.8.10. Jacobsthal's explicit formulas for $p = x^2 + y^2$ . . . 415

6. Polynomials II **431**
6.1. Multivariate polynomials again . . . 431
6.1.1. Example 1: $R[x,y]/y$ . . . 431
6.1.2. Example 2: $R[x,y]/\left(x^2+y^2-1\right)$ . . . 434
6.1.3. Indeterminates one at a time . . . 436
6.1.4. More examples? . . . 438
6.2. Degrees and the deg-lex order . . . 440
6.2.1. Degrees . . . 440
6.2.2. The deg-lex order . . . 441
6.2.3. Leading coefficients, monomials and terms . . . 444
6.3. Division with remainder and Gröbner bases . . . 445
6.3.1. The case of principal ideals . . . 445
6.3.2. The case of arbitrary ideals . . . 450
6.3.3. Monomial orders . . . 460
6.4. Solving polynomial systems using Gröbner bases . . . 462
6.5. Factorization of polynomials . . . 467
6.5.1. Factoring univariate polynomials . . . 467
6.5.2. Factoring multivariate polynomials . . . 471

7. Modules over a PID (specifically, over $\mathbb{Z}$) **473**
7.1. Classifying finite abelian groups . . . 473
7.1.1. The classification theorem . . . 473
7.1.2. On modules and matrices . . . 474
7.1.3. Every finite $\mathbb{Z}$-module is finitely presented . . . 475
7.1.4. Understanding cokernels of diagonal matrices . . . 477
7.1.5. The proof strategy . . . 479
7.1.6. Row and column operations and congruent matrices . . . 480
7.1.7. The Smith normal form algorithm . . . 482
7.1.8. A few words on arbitrary rings . . . 485
7.1.9. Solving systems of linear equations over $\mathbb{Z}$ . . . 486
7.1.10. Step 8: streamlining direct products of $\mathbb{Z}/n$'s . . . 486
7.1.11. Uniqueness of the SNF . . . 490
7.2. Application: Primitive roots . . . 490

This work is licensed under a Creative Commons "CC0 1.0 Universal" license.

PUBLIC DOMAIN

* * *

This is a text (or, more honestly, a glorified set of lecture notes) for my Math 332 course at Drexel University in Winter 2023. At the moment, it is somewhat of a draft (and much of it is copypasted from my Math 533 course in Winter 2021).

1. Preface

1.1. What is this?

These notes are written for the second part of a groups-first undergraduate abstract algebra sequence, or for an introductory graduate course on rings and fields. They cover the basic properties of **rings**, **modules** and **fields**, in particular **polynomial rings** and **finite fields**, while assuming that the reader is fluent in the basic language of groups (and in elementary number theory, such as the properties of prime numbers and greatest common divisors). The content is mostly introductory, and the main results obtained are

- the Chinese Remainder Theorem for rings and ideals,
- the construction of monoid algebras (including polynomial rings as a particular case),
- the main properties of univariate polynomial rings,
- the existence and uniqueness of finite fields $\mathbb{F}_{p^n}$ of all prime-power orders,
- the law of quadratic reciprocity (with a proof in the odd/odd case), and
- two proofs of Fermat's theorem about writing primes p as sums of two squares (one giving an "explicit" expression in terms of Jacobsthal sums).

The last sections briefly introduce Gröbner bases (without proofs) and the Smith normal form (over $\mathbb{Z}$, with an outlined proof). Some properties of the Fibonacci sequence are explored as applications. Thus, the text is suited to a quarter-long course, less to a semester-long one.

This text is written rather informally and sometimes tersely. I assume that the reader has encountered proofs before, as she will have to fill in some details and understand some hints. Unlike my notes on combinatorics, this text is not trying to fill any expository gaps, since the literature on abstract algebra is already vast and includes some rather detailed and rigorous texts (e.g., Warner [Warner90], Jacobson [JacobsXX], Zariski/Samuel [ZarSam86]).

On occasion, I have tried to mildly innovate, e.g., by constructing the polynomial ring as a monoid algebra, or by involving the Fibonacci numbers in a few places as a "grass-touching" example. I also attempt to view the subject through a more constructive lens than usual (Section 6.5 is a noticeable example), although I am nowhere as consistent about it as a text dedicated to constructive algebra (such as [Edward22]) would be.

A quarter is not much time, and this text reflects the necessary tradeoffs. I would have loved to cover some Galois theory, more about quadratic number rings, more about multivariate polynomials, Gröbner bases with proofs, linear algebra with proofs, the Smith normal form over non-$\mathbb{Z}$ rings, tensor products, determinants, exact sequences, ..., but I have not managed to fit this into

a quarter-long course. A reader who whets her appetite by this text will almost surely have to satisfy it elsewhere (e.g., [Aluffi16], [Bosch18], [CoLiOs15], [Cox12], [DumFoo04], [Edward22], [Elman22], [Goodma16], [JacobsXX], [Knapp16], [Laurit09], [Leinst24], [LidNie00], [Lorsch20a], [Lorsch20b], [McNult16], [Rotman3e], [Sharif22], [Siksek19], [Steinb06], [Stewar15], [Waerde91]).

The original template for the structure of this text was the book *Abstract Algebra* by Dummit and Foote ([DumFoo04] in the bibliography), specifically a subset of [DumFoo04, Chapters 7–14]. However, I have ended up deviating from [DumFoo04] in the presentation, in the ordering, in the exercises and digressions, and even in some of the terminology.

The course has a website:

`https://www.cip.ifi.lmu.de/~grinberg/t/23wa/`

on which you can find homework sets. Also, old homework sets can be found at the website of my Math 533 course from Winter 2021:

`https://www.cip.ifi.lmu.de/~grinberg/t/21w/`

I thank Bogdan Nica and Tommy Pett for reporting mistakes in the text that follows, and Keith Conrad for pedagogical and thematic suggestions.

1.2. Plan

This text is split into 6 chapters:

2. **Rings and ideals.** Just like the notion of a group is an abstract model for a set of symmetries or invertible operations in general, the notion of a ring models a set of numbers or things made out of numbers (such as polynomials or matrices). More formally, a ring is a set equipped with two operations called "addition" and "multiplication" and two elements called "zero" and "unity" that satisfy certain axioms. We will explore both specific examples and general properties of rings, and we will study features of rings such as subrings and ideals, and certain classes of rings such as integral domains and fields.

3. **Modules.** Modules are the natural generalization of vector spaces when the underlying number system is replaced by a ring. In particular, we will learn some of the basics of abstract linear algebra (the theory of vector spaces over fields) here.

4. **Monoid algebras and polynomials.** This is a generalization of the classical notion of polynomials, which replaces the monomials by something much more general (the elements of a monoid). Among other things, this will give us a precise definition of polynomials. We will study univariate polynomials (i.e., polynomials in one indeterminate) in more detail,

establishing in particular some of their unique features (division with remainder and Euclidean algorithm). This will help us "adjoin" a root of a polynomial to a commutative ring or field.

5. **Finite fields.** Finite fields are "miniature versions" of our familiar number systems; they are sets with extremely well-behaved "addition" and "multiplication" operations but only finitely many elements. We will build up some of their basic theory and see a few of their many applications.

6. **Polynomials II.** We will study polynomials in more detail, focussing now mostly on multivariate polynomials. We will give a very introductory treatment of Gröbner bases (explaining their simplest uses, but not proving any of their nontrivial properties). We will explain how polynomials with integer coefficients can be factored (into irreducibles), and address some parts of the ancient question of "how do you solve a system of polynomial equations?".

7. **Modules over a PID.** To be specific, we will be studying modules over $\mathbb{Z}$ only. In particular, we will prove the structure theorem for finite abelian groups, and construct the Smith normal form of a matrix. As an application, we will prove the existence of primitive roots in a finite field.

1.3. Notations

We shall use the following notations:

- We let $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- The notation $|S|$ denotes the size (i.e., the number of elements) of a set S.
- Unlike algebraic geometers, we do accept noncommutative rings as rings (see below for the definition). Unlike [DumFoo04], we don't accept nonunital rings (i.e., rings without a 1) as rings. This will be discussed in more detail below.

1.4. Refresher on modular arithmetic

We will use modular arithmetic (specifically, the notion of residue classes modulo n, and the algebraic operations on these classes). An introduction to modular arithmetic can be found in almost any textbook on abstract algebra (see, e.g., [Grinbe19, §3.4]), and I assume that you have seen it at least in some form, since it underlies the standard definition of cyclic groups. Let me nevertheless give a summary as a reminder.

For the rest of this section, we fix an integer n. Two integers a and b are said to be **congruent** (to each other) **modulo** n if and only if $n \mid a - b$. The short notation for this is "$a \equiv b \bmod n$", but we shall shorten this even further to

"$a \underset{n}{\equiv} b$" in this subsection, so that $\underset{n}{\equiv}$ becomes a binary relation on the set $\mathbb{Z}$ of all integers.

For example, $5 \underset{2}{\equiv} 9$ (since $2 \mid 5-9$) but $5 \underset{2}{\not\equiv} 8$ (since $2 \nmid 5-8$). (As usual, "$a \underset{n}{\not\equiv} b$" means "not $a \underset{n}{\equiv} b$".)

The binary relation $\underset{n}{\equiv}$ is an equivalence relation. It is called **congruence modulo** n. Its equivalence classes are called the **residue classes of integers modulo** n. Explicitly, for every integer a, the residue class that contains a is the set

$$\begin{aligned}&\{\text{all integers that are congruent to } a \text{ modulo } n\}\\ &= \{\text{all integers that differ from } a \text{ by a multiple of } n\}\\ &= \{\ldots,\ a-2n,\ a-n,\ a,\ a+n,\ a+2n,\ a+3n,\ \ldots\}.\end{aligned}$$

We denote this class by $\overline{a}$. Two integers a and b satisfy $\overline{a} = \overline{b}$ if and only if $a \underset{n}{\equiv} b$.

In particular, the residue class $\overline{0}$ of 0 consists of all integers that are multiples of n. That is:

$$\overline{0} = \{\ldots,\ -3n,\ -2n,\ -n,\ 0,\ n,\ 2n,\ 3n,\ \ldots\}.$$

The residue class $\overline{n}$ of n consists of the very same integers, since an integer is congruent to n modulo n if and only if it is congruent to 0 modulo n. In other words, $\overline{n} = \overline{0}$. Likewise, $\overline{2n} = \overline{0}$ and $\overline{3n} = \overline{0}$ and so on. Likewise, $\overline{n+1} = \overline{1}$ and $\overline{n+2} = \overline{2}$ and so on. On the other hand, the n residue classes $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ are all distinct, since no two of the integers $0, 1, \ldots, n-1$ are congruent modulo n.

Here are some examples:

- For $n = 2$, the only two residue classes modulo n are

  $$\overline{0} = \{\text{all even integers}\} = \{\ldots, -6, -4, -2, 0, 2, 4, \ldots\} \qquad \text{and}$$
  $$\overline{1} = \{\text{all odd integers}\} = \{\ldots, -5, -3, -1, 1, 3, 5, \ldots\}.$$

  For any other integer a, the residue class $\overline{a}$ of a modulo 2 is either $\overline{0}$ or $\overline{1}$, depending on whether a is even or odd. For instance, $\overline{2} = \overline{4} = \overline{6} = \cdots = \overline{0}$ whereas $\overline{1} = \overline{3} = \overline{5} = \cdots = \overline{1}$.

- For $n = 5$, there are five residue classes modulo n, namely

  $$\begin{aligned}\overline{0} &= \{\ldots, -10, -5, 0, 5, 10, \ldots\},\\ \overline{1} &= \{\ldots, -9, -4, 1, 6, 11, \ldots\},\\ \overline{2} &= \{\ldots, -8, -3, 2, 7, 12, \ldots\},\\ \overline{3} &= \{\ldots, -7, -2, 3, 8, 13, \ldots\},\\ \overline{4} &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}.\end{aligned}$$

- For $n = 1$, there is only one residue class modulo n, namely

$$\overline{0} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = \mathbb{Z}.$$

- The case $n = 0$ is special: Here, no two distinct integers a and b are congruent modulo n (because only 0 is divisible by 0). Thus, for each integer a, the residue class $\overline{a}$ of a modulo 0 is just the singleton set $\{a\}$. Hence, there are infinitely many residue classes modulo 0, one for each integer.

As you see, the residue classes $\overline{a}$ modulo n differ from their underlying integers a in that different integers a, b lead to the same residue class $\overline{a} = \overline{b}$ when their difference is a multiple of n. Thus, working with residue classes of integers modulo n can be viewed as working with integers but pretending that n equals 0 (so that two integers that differ by a multiple of n are equal).

The set of all residue classes of integers modulo n will be called $\mathbb{Z}/n$ or $\mathbb{Z}/n\mathbb{Z}$ (or sometimes $\mathbb{Z}_n$, but this symbol is unfortunately also used for other purposes). This set $\mathbb{Z}/n$ has size n if n is positive[1], size $-n$ if n is negative, and infinite size if $n = 0$ (indeed, $\mathbb{Z}/0$ is just $\mathbb{Z}$ "with its elements relabelled"[2]).

We note that, from the viewpoint of group theory, the residue classes modulo n are the cosets of the subgroup $n\mathbb{Z} = \{\text{all multiples of } n\}$ in the group $(\mathbb{Z}, +, 0)$. Thus, the set $\mathbb{Z}/n\mathbb{Z}$ of these residue classes is the quotient of the group $(\mathbb{Z}, +, 0)$ by this subgroup $n\mathbb{Z}$. This is where the notation $\mathbb{Z}/n\mathbb{Z}$ comes from. (The notation $\mathbb{Z}/n$ is just shorthand for that.)

We can furthermore define the sum, the difference and the product of any two residue classes modulo n. Namely, if $\overline{a}$ and $\overline{b}$ are two residue classes mod-

[1]Indeed, when n is positive, the n distinct residue classes modulo n are

$$\begin{aligned}
\overline{0} &= \{\ldots,\ -3n,\ -2n,\ -n,\ 0,\ n,\ 2n,\ 3n,\ \ldots\}, \\
\overline{1} &= \{\ldots,\ -3n+1,\ -2n+1,\ -n+1,\ 1,\ n+1,\ 2n+1,\ 3n+1,\ \ldots\}, \\
\overline{2} &= \{\ldots,\ -3n+2,\ -2n+2,\ -n+2,\ 2,\ n+2,\ 2n+2,\ 3n+2,\ \ldots\}, \\
&\ldots, \\
\overline{n-1} &= \{\ldots,\ -2n-1,\ -n-1,\ -1,\ n-1,\ 2n-1,\ 3n-1,\ 4n-1,\ \ldots\}.
\end{aligned}$$

[2]You may be unused to this; some textbooks carefully avoid the $n = 0$ case when considering $\mathbb{Z}/n$. And indeed, $\mathbb{Z}/0$ behaves unlike the "other" $\mathbb{Z}/n$'s in some regard (for example, $\mathbb{Z}/0$ is infinite, whereas $\mathbb{Z}/n$ is finite for each nonzero n). But the underlying idea is still the same: Two integers a and b are congruent modulo 0 if and only if 0 divides $a - b$; but 0 only divides 0 itself (since the only multiple of 0 is 0), so this means that a and b are congruent modulo 0 if and only if a and b are equal. Hence, each residue class modulo 0 just consists of a single number. Thus, the elements of $\mathbb{Z}/0$ are the one-element sets $\ldots, \{-2\}, \{-1\}, \{0\}, \{1\}, \{2\}, \ldots$. They are added and multiplied just as the corresponding integers: $\{a\} + \{b\} = \{a + b\}$ and $\{a\} \cdot \{b\} = \{a \cdot b\}$.

ulo n, then we set

$$\overline{a} + \overline{b} = \overline{a+b};$$
$$\overline{a} - \overline{b} = \overline{a-b};$$
$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

In other words, to add (or subtract, or multiply) two residue classes, we just add (or subtract, or multiply) the underlying numbers and take the residue class of the result. It takes a bit of thought to prove that this is well-defined (i.e., that the values $\overline{a+b}$, $\overline{a-b}$ and $\overline{ab}$ really depend only on the residue classes $\overline{a}$ and $\overline{b}$ and not on their chosen representatives a and b), but this is fairly easy and well-known. These operations (addition, subtraction and multiplication) on residue classes are called **modular arithmetic**.

Here are some examples:

- If $n = 24$, then

$$\overline{23} + \overline{5} = \overline{23+5} = \overline{28} = \overline{4} \qquad \left(\text{since } 28 \underset{24}{\equiv} 4\right).$$

  This is actually the known fact that "5 hours after 23 o'clock is 4 o'clock" (although here in the US, you would usually say "11 PM" instead of "23 o'clock", and "4 AM" instead of "4 o'clock"). The 24 hours of a day thus naturally correspond to the residue classes modulo 24, and reckoning with time is a matter of modular arithmetic.

- If $n = 12$, then

$$\overline{4} \cdot \overline{9} = \overline{4 \cdot 9} = \overline{36} = \overline{0} \qquad \left(\text{since } 36 \underset{12}{\equiv} 0\right).$$

The addition of residue classes that we defined above turns the set $\mathbb{Z}/n\mathbb{Z}$ of all these residue classes into a group $\left(\mathbb{Z}/n\mathbb{Z},\ +,\ \overline{0}\right)$. When n is positive, this group is known as the **cyclic group of order** n. However, the multiplication is of interest too, and in fact is one of the main protagonists of this course.

1.5. Homework set #0: (de)motivating questions

The following exercises should be viewed as food for thought. Some of them are easy, some hard, some close to impossible at the current state. Just think about each of them for a little while (5 minutes? 15 minutes? an hour if you like them?). These exercises are illustrative of some of the elementary applications of abstract algebra. This course will teach you to solve some of them. Solution sketches can be found in [21w, solutions to Homework set 0].

Exercise 1.5.1.

(a) Factor the polynomial $a^3 + b^3 + c^3 - 3abc$.

(b) Factor the polynomial $bc(b-c) + ca(c-a) + ab(a-b)$.

(c) How general have your methods been? Did you use tricks specific to the given polynomials, or do you have an algorithm for factoring any polynomial (say, with integer coefficients)?

Exercise 1.5.2. Simplify $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$.

Exercise 1.5.3. Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_n$ be n integers, and let $b_1, b_2, \ldots, b_n$ be n further integers. The Gaussian elimination tells you how to solve the system

$$\begin{aligned} a_1 x_1 + a_2 x_2 + \cdots + a_n x_n &= 0; \\ b_1 x_1 + b_2 x_2 + \cdots + b_n x_n &= 0 \end{aligned}$$

for n unknowns $x_1, x_2, \ldots, x_n \in \mathbb{Q}$. The answer, in general, will have the form "all $\mathbb{Q}$-linear combinations (i.e., linear combinations with rational coefficients) of a certain bunch of vectors". (More precisely, "a certain bunch of vectors" are $n-2$ or $n-1$ or n vectors with rational coordinates, depending on the rank of the $2 \times n$-matrix $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ b_1 & b_2 & \cdots & b_n \end{pmatrix}$.)

Now, how can you solve the above system for n unknowns $x_1, x_2, \ldots, x_n \in \mathbb{Z}$? Will the answer still be "all $\mathbb{Z}$-linear combinations (i.e., linear combinations with integer coefficients) of a certain bunch of vectors"?

What about more general systems of linear equations to be solved for integer unknowns?

Exercise 1.5.4. You are given a 5×5-grid of lamps, each of which is either on or off. For example, writing 1 for "on" and 0 for "off", it may look as follows:

1	0	0	1	1
1	1	0	0	1
1	0	0	1	0
0	1	1	1	1
0	1	0	0	0

In a single move, you can toggle any lamp (i.e., turn it on if it was off, or turn it off if it was on); however, this will also toggle every lamp adjacent to it. ("Adjacent to it" means "having a grid edge in common with it"; thus, a lamp will have 2 or 3 or 4 adjacent lamps.) For example, if we toggle the second lamp (from the left) in the

topmost row in the above example grid, then we obtain

1	**0**	**0**	1	1
1	**1**	0	0	1
1	0	0	1	0
0	1	1	1	1
0	1	0	0	0

(where the boldfaced numbers correspond to the lamps that have been affected by the move).

Assume that all lamps are initially off. Can you (by a strategically chosen sequence of moves) achieve a state in which all lamps are on?

[*Remark:* You can play this game on `https://codepen.io/wintlu/pen/ZJJLGz` .]

Exercise 1.5.5.

(a) How many of the numbers $0, 1, \ldots, 6$ appear as remainders of a perfect square divided by 7 ?

(b) How many of the numbers $0, 1, \ldots, 13$ appear as remainders of a perfect square divided by 14 ?

What about replacing 7 or 14 by n? Can you do better than just squaring them all?

[For example, 3 of the numbers $0, 1, \ldots, 4$ appear as remainders of a perfect square divided by 5 – namely, the three numbers $0, 1, 4$.]

Exercise 1.5.6. Solve the following system of equations:

$$a^2 + b + c = 1;$$
$$b^2 + c + a = 1;$$
$$c^2 + a + b = 1$$

for three complex numbers a, b, c.

The next exercise requires some preliminary discussion.

The following triangular table shows the binomial coefficients $\binom{n}{m}$ for $n \in$

$\{0,1,\ldots,7\}$ and $m \in \{0,1,\ldots,n\}$:

							$k=0$ ↙								
$n=0$	$\to$						1		$k=1$ ↙						
$n=1$	$\to$					1		1		$k=2$ ↙					
$n=2$	$\to$				1		2		1		$k=3$ ↙				
$n=3$	$\to$			1		3		3		1		$k=4$ ↙			
$n=4$	$\to$		1		4		6		4		1		$k=5$ ↙		
$n=5$	$\to$	1		5		10		10		5		1		$k=6$ ↙	
$n=6$	$\to$		1		6		15		20		15		6		1		$k=7$ ↙
$n=7$	$\to$	1		7		21		35		35		21		7		1	

(This is part of what is known as *Pascal's triangle*.)

Now, in this table, let us replace each even number by a 0 and each odd number by a 1. We obtain

							$k=0$ ↙								
$n=0$	$\to$						1		$k=1$ ↙						
$n=1$	$\to$					1		1		$k=2$ ↙					
$n=2$	$\to$				1		0		1		$k=3$ ↙				
$n=3$	$\to$			1		1		1		1		$k=4$ ↙			
$n=4$	$\to$		1		0		0		0		1		$k=5$ ↙		
$n=5$	$\to$	1		1		0		0		1		1		$k=6$ ↙	
$n=6$	$\to$		1		0		1		0		1		0		1		$k=7$ ↙
$n=7$	$\to$	1		1		1		1		1		1		1		1	

This looks rather similar to the third evolutionary stage of Sierpinski's triangle:

(Each 0 in the above table corresponds to a white △ triangle, and each 1 corresponds to a black ▲ triangle.)

Exercise 1.5.7. Where does this similarity come from?

Exercise 1.5.8. A *conic* means a curve of the form

$$\left\{(x,y) \in \mathbb{R}^2 \mid ax^2 + bxy + cy^2 + dx + ey + f = 0\right\},$$

where a, b, c, d, e, f are six real numbers such that $(a,b,c,d,e,f) \neq (0,0,0,0,0,0)$. Examples of conics are

- any circle, e.g., the unit circle $\left\{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\right\}$;
- more generally, any ellipse;
- any parabola, e.g., $\left\{(x,y) \in \mathbb{R}^2 \mid x^2 + y = 0\right\}$;
- any hyperbola, e.g., $\left\{(x,y) \in \mathbb{R}^2 \mid xy = 1\right\}$ or $\left\{(x,y) \in \mathbb{R}^2 \mid x^2 - y^2 = 1\right\}$;
- the union of any two lines, e.g., $\left\{(x,y) \in \mathbb{R}^2 \mid xy = 0\right\}$.

A conic is said to be *nondegenerate* if it is not the union of two lines.

(a) What is the maximum number of points in which a nondegenerate conic can intersect a line?

(b) What is the maximum number of points in which two nondegenerate conics can intersect each other?

2. Rings and ideals

2.1. Defining rings ([DumFoo04, §7.1])

2.1.1. The definition

You may have seen rings before, but beware: There are at least 4 non-equivalent notions of a "ring", and the one you know might be different from the one we'll use. Let us define the one we want:[3]

Definition 2.1.1. A **ring** means a set R equipped with

- two binary operations (i.e., maps from $R \times R$ to R) that are called **addition** and **multiplication** and are denoted by $+$ and $\cdot$, and
- two elements of R that are called **zero** and **unity** and are denoted by 0 and 1,

such that the following properties (the "**ring axioms**") hold:

- $(R, +, 0)$ is an abelian group. In other words:
  - The operation $+$ is associative (i.e., we have $a + (b + c) = (a + b) + c$ for any $a, b, c \in R$).
  - The element 0 is a neutral element for the operation $+$ (i.e., we have $a + 0 = 0 + a = a$ for any $a \in R$).
  - Each element $a \in R$ has an inverse for the operation $+$ (i.e., an element $b \in R$ satisfying $a + b = b + a = 0$).
  - The operation $+$ is commutative (i.e., we have $a + b = b + a$ for any $a, b \in R$).
- $(R, \cdot, 1)$ is a monoid. In other words:
  - The operation $\cdot$ is associative (i.e., we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for any $a, b, c \in R$).

[3] Let us recall the notion of a **monoid**, which will be briefly used in this definition.

Essentially, a monoid is just "a group without inverses". The formal definition is as follows: A **monoid** is a set S equipped with a binary operation $*$ (that is, a map from $S \times S$ to S) and a specified element $e \in S$ such that

- the operation $*$ is associative (i.e., we have $a * (b * c) = (a * b) * c$ for any $a, b, c \in S$, where we are using the notation $x * y$ for the image of a given pair (x, y) under the operation $*$), and
- the element e is a neutral element for this operation $*$ (i.e., we have $a * e = e * a = a$ for any $a \in S$).

We denote this monoid by $(S, *, e)$.

  - The element 1 is a neutral element for the operation $\cdot$ (i.e., we have $a \cdot 1 = 1 \cdot a = a$ for any $a \in R$).

  Note that we **do not** require that the operation $\cdot$ be commutative; nor do we require elements to have inverses for it.

- The **distributive laws** hold in R: That is, for all $a, b, c \in R$, we have

$$(a+b) \cdot c = a \cdot c + b \cdot c \qquad \text{and} \qquad a \cdot (b+c) = a \cdot b + a \cdot c.$$

- We have $0 \cdot a = a \cdot 0 = 0$ for each $a \in R$.

The zero of R and the unity of R don't necessarily have to be the numbers 0 and 1; we just call them 0 and 1 because they behave similarly to said numbers. If things can get ambiguous (i.e., if they actually differ from the numbers 0 and 1), then we will call them 0_R and 1_R instead (see below for some examples of this).

The unity 1 of R is also known as the **identity** or the **one** of R (but beware the ambiguity of the latter words).

The product $a \cdot b$ of two elements $a, b \in R$ is often denoted ab (so we omit the $\cdot$ sign) or occasionally $a \times b$ (we will avoid the latter notation).

The inverse of an element $a \in R$ in the abelian group $(R, +, 0)$ will be called the **additive inverse** of a, and is denoted $-a$.

If $a, b \in R$, then the **difference** $a - b$ is defined to be the element $a + (-b) \in R$.

Definition 2.1.2. A ring R is said to be **commutative** if its multiplication is commutative (i.e., if $ab = ba$ for all $a, b \in R$).

2.1.2. Some examples of rings

You have probably seen various rings in your mathematical life. Here are some examples:

- The sets $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ (endowed with the usual addition, the usual multiplication, the usual 0 and the usual 1) are commutative rings. The same holds for the set $\mathbb{C}$ of complex numbers[4].

[4] This course will not rely overly much on complex numbers, as we will be working in more abstract settings most of the time. Thus, if you ignore everything I say about complex numbers and $\mathbb{C}$, you will miss out on some examples and applications, but still understand the core of this course.

However, it will still be rather helpful to understand the construction of the complex numbers, since we will imitate this construction later on. This construction is covered in detail in [Grinbe19, §4.1] or in [BeaBla19, §A.5]. See also Grant Sanderson's video `https://www.youtube.com/watch?v=5PcpBw5Hbwo` on the geometric meaning of complex numbers.

(Notice that existence of **multiplicative** inverses – i.e., inverses for the operation $\cdot$ – is not required.)

- The set $\mathbb{N}$ of nonnegative integers[5] (again endowed with the usual addition, the usual multiplication, the usual 0 and the usual 1) is **not** a ring, since $(\mathbb{N}, +, 0)$ is not a group (only a monoid). It's what is called a **semiring**.

  (Don't be fooled by the existence of negative numbers: The number 2 has no additive inverse in $\mathbb{N}$, even though -2 is an additive inverse for it in $\mathbb{Z}$.)

- We can define a commutative ring $\mathbb{Z}'$ as follows: We define a binary operation $\widetilde{\times}$ on the set $\mathbb{Z}$ by setting

$$a \mathbin{\widetilde{\times}} b = -ab \qquad \text{for all } (a,b) \in \mathbb{Z} \times \mathbb{Z}.$$

  Now, let $\mathbb{Z}'$ be the **set** $\mathbb{Z}$, endowed with the usual addition $+$ and the (unusual) multiplication $\widetilde{\times}$ and with the (usual) zero $0_{\mathbb{Z}'} = 0$ and the (unusual) unity $1_{\mathbb{Z}'} = -1$. It is easy to check that $\mathbb{Z}'$ is a commutative ring. It is an example of a ring whose unity is **not** equal to the integer 1; the two "1"s in the equality $1_{\mathbb{Z}'} = -1$ mean different things (the first "1" is the unity of $\mathbb{Z}'$, while the second "1" is the number 1). This is why it is important to never omit the subscript $\mathbb{Z}'$ in "$1_{\mathbb{Z}'}$".

  Note that I am denoting this new ring by $\mathbb{Z}'$ rather than by $\mathbb{Z}$, even though **as a set** it is identical with $\mathbb{Z}$. I do this because I want to refer to a ring by just one single letter instead of having to specify the addition and multiplication every time; but this cannot go well if we use the same letter for different rings. A ring is not just a set, but rather the entire package consisting of the set, the addition, the multiplication, the zero and the unity. The rings $\mathbb{Z}$ and $\mathbb{Z}'$ have the same underlying set, but they differ in the rest of the package (specifically, in the multiplication and the unity).

  This all said, $\mathbb{Z}'$ is not a very interesting ring: It is essentially "a copy of $\mathbb{Z}$, except that every integer n has been renamed as $-n$". To formalize this intuition, we would need to introduce the notion of a **ring isomorphism**, which I will do soon (Definition 2.7.1 **(b)**); the main idea is that the bijection

$$\varphi : \mathbb{Z} \to \mathbb{Z}', \qquad n \mapsto -n$$

[5] Recall once again that $\mathbb{N}$ is defined to be $\{0, 1, 2, \ldots\}$.

[6] satisfies

$$\begin{aligned} \varphi(a+b) &= \varphi(a) + \varphi(b) && \text{for all } (a,b) \in \mathbb{Z} \times \mathbb{Z}; \\ \varphi(a \cdot b) &= \varphi(a) \mathbin{\widetilde{\times}} \varphi(b) && \text{for all } (a,b) \in \mathbb{Z} \times \mathbb{Z}; \\ \varphi(0) &= 0_{\mathbb{Z}'}; \\ \varphi(1) &= 1_{\mathbb{Z}'} \end{aligned}$$

(where the "0" and the "1" without subscripts are the usual numbers 0 and 1), and thus the ring $\mathbb{Z}'$ can be viewed as the ring $\mathbb{Z}$ with its elements "relabelled" using this bijection.

- The polynomial rings

$$\begin{aligned} \mathbb{Z}[x] &= \{\text{all polynomials in one indeterminate } x \text{ with integer coefficients}\}, \\ \mathbb{Q}[x] &= \{\text{all polynomials in one indeterminate } x \text{ with rational coefficients}\}, \\ \mathbb{R}[x,y] &= \{\text{all polynomials in two indeterminates } x, y \text{ with real coefficients}\} \end{aligned}$$

and

$$\begin{aligned} &\mathbb{R}[z_1, z_2, \ldots, z_n] \\ &= \{\text{all polynomials in } n \text{ indeterminates } z_1, z_2, \ldots, z_n \text{ with real coefficients}\} \end{aligned}$$

(and many others, such as $\mathbb{Z}[a,b]$ or $\mathbb{C}[u,p,q]$) are commutative rings. (We won't give a formal definition of polynomials until Chapter 4.2, but you probably already have a rough idea of what polynomials are, and this idea should suffice for now.)

- The set of all functions $\mathbb{Q} \to \mathbb{Q}$ is a commutative ring, where addition and multiplication are defined pointwise (i.e., addition is defined by

$$(f+g)(x) = f(x) + g(x) \qquad \text{for all } f, g : \mathbb{Q} \to \mathbb{Q} \text{ and } x \in \mathbb{Q},$$

and multiplication is defined by

$$(fg)(x) = f(x) \cdot g(x) \qquad \text{for all } f, g : \mathbb{Q} \to \mathbb{Q} \text{ and } x \in \mathbb{Q},$$

), where the zero is the "constant-0" function (sending every $x \in \mathbb{Q}$ to 0), and where the unity is the "constant-1" function (sending every $x \in \mathbb{Q}$ to 1). Of course, the same construction works if we consider functions $\mathbb{R} \to \mathbb{C}$, or functions $\mathbb{C} \to \mathbb{Q}$, or many other kinds of functions.

More generally, if R is a ring, and if S is any set, then the set of all functions $S \to R$ is a ring (with $+$, $\cdot$, 0 and 1 defined as above). If R is commutative, then so is this new ring. (For some reason, [DumFoo04] requires S to be nonempty here, but this is unnecessary.)

[6] This notation means "the map φ from $\mathbb{Z}$ to $\mathbb{Z}'$ that sends each n to $-n$".

When we specify a ring, we don't need to provide its zero 0 and its unity 1 (although, of course, they need to exist); they are uniquely determined by the operations $+$ and $\cdot$. This is because they are neutral elements for the operations $+$ and $\cdot$; but the neutral element of an operation is always unique.[7]

Here are some more examples of rings:

- The set $\mathbb{S}$ of all real numbers of the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$ (endowed with the usual notions of "addition" and "multiplication" defined for real numbers) is a commutative ring. The "hard" part of proving this is showing that the product of two numbers of this form is again a number of this form; but this is just a matter of computation:

$$\begin{aligned}\left(a + b\sqrt{5}\right)\left(c + d\sqrt{5}\right) &= ac + bc\sqrt{5} + ad\sqrt{5} + bd \cdot 5 \\ &= \underbrace{\left(ac + 5bd\right)}_{\in \mathbb{Q}} + \underbrace{\left(bc + ad\right)}_{\in \mathbb{Q}}\sqrt{5}.\end{aligned}$$

  Associativity, distributivity, etc. come for "free", or, as we say, are **inherited from** $\mathbb{R}$ (meaning that we already know that they hold for $\mathbb{R}$, so they must automatically hold for $\mathbb{S}$). Only the existence of additive inverses (i.e., of inverses for the operation $+$) does not come for free (sure, every element of $\mathbb{S}$ has an additive inverse of $\mathbb{R}$, but we must show that it has an additive inverse of $\mathbb{S}$), but it is easy to check (the additive inverse of $a + b\sqrt{5} \in \mathbb{S}$ is $(-a) + (-b)\sqrt{5} \in \mathbb{S}$).

  The standard notation for this ring is $\mathbb{Q}\left[\sqrt{5}\right]$, not $\mathbb{S}$. We will eventually see it as a particular case of a general construction.

- We could define a different ring structure on the set $\mathbb{S}$ (that is, a ring which, as a set, is identical with $\mathbb{S}$, but has a different choice of operations) as follows: We define a binary operation $*$ on $\mathbb{S}$ by setting

$$\left(a + b\sqrt{5}\right) * \left(c + d\sqrt{5}\right) = ac + bd\sqrt{5}$$
$$\text{for all } (a, b) \in \mathbb{Q} \times \mathbb{Q} \text{ and } (c, d) \in \mathbb{Q} \times \mathbb{Q}.$$

  This is well-defined, because every element of $\mathbb{S}$ can be written in the form $a + b\sqrt{5}$ for a **unique** pair $(a, b) \in \mathbb{Q} \times \mathbb{Q}$. This is a consequence of the irrationality of $\sqrt{5}$. You could not do this with $\sqrt{4}$ instead of $\sqrt{5}$!

  Now, let $\mathbb{S}'$ be the set $\mathbb{S}$, endowed with the usual addition $+$ and the (unusual) multiplication $*$, with the (usual) zero $0_{\mathbb{S}'} = 0$ and with the

[7] To wit: If $*$ is a binary operation on a set S, and if u and v are two neutral elements for $*$, then $u * v = u$ (by the neutrality of v) and $u * v = v$ (by the neutrality of u), so that $u = u * v = v$. You have probably seen this argument in group theory, but it does not require a group, just an arbitrary binary operation.

(unusual) unity $1_{\mathbb{S}'} = 1 + \sqrt{5}$ (not the integer 1). It is easy to check that $\mathbb{S}'$ is a commutative ring. The **sets** $\mathbb{S}$ and $\mathbb{S}'$ are identical, but the **rings** $\mathbb{S}$ and $\mathbb{S}'$ are not: For example, the ring $\mathbb{S}'$ has two nonzero elements whose product is 0 (namely, $1 * \sqrt{5} = 0$), whereas the ring $\mathbb{S}$ has no such things. Thus, we don't just have $\mathbb{S}' \neq \mathbb{S}$ as rings, but there is also no way to regard $\mathbb{S}'$ as "a copy of $\mathbb{S}$ with its elements renamed" (like we did with $\mathbb{Z}'$ and $\mathbb{Z}$). So a ring is much more than just a set; the $+$, $\cdot$, 0 and 1 matter.

- The set $\mathbb{S}_3$ of all real numbers of the form $a + b\sqrt[3]{5}$ with $a, b \in \mathbb{Q}$ (endowed with the usual addition, etc.) is **not** a ring. Indeed, multiplication is not a binary operation on this set $\mathbb{S}_3$, as you can see by noticing that

$$\underbrace{\left(1 + 1\sqrt[3]{5}\right)}_{\in \mathbb{S}_3} \underbrace{\left(1 + 1\sqrt[3]{5}\right)}_{\in \mathbb{S}_3} = 1 + 2\sqrt[3]{5} + \left(\sqrt[3]{5}\right)^2 \notin \mathbb{S}_3.$$

  (Strictly speaking, this requires some work to prove – how can we be sure there are no $a, b \in \mathbb{Q}$ that satisfy $1 + 2\sqrt[3]{5} + \left(\sqrt[3]{5}\right)^2 = a + b\sqrt[3]{5}$? – but I'm just making a point about how not everything that looks like a ring is a ring. For a complete proof of this claim, see Exercise 5.2.1 **(d)**.)

- For any $n \in \mathbb{N}$, the set $\mathbb{R}^{n \times n}$ of all $n \times n$-matrices with real entries (endowed with matrix addition, matrix multiplication, the zero matrix and the identity matrix) is a ring. It is not commutative unless $n \leq 1$, since we don't usually have $AB = BA$ for matrices.

  More generally: If R is any ring, and if $n \in \mathbb{N}$, then the set $R^{n \times n}$ of all $n \times n$-matrices with entries in R (endowed with matrix addition, matrix multiplication, the zero matrix and the identity matrix) is a ring. This is called the $n \times n$**-matrix ring** over R; it is denoted by $R^{n \times n}$ or $M_n(R)$ or $\mathrm{M}_n(R)$. Of course, the matrix addition is defined in terms of the addition of R, and the matrix multiplication is defined in terms of both $+$ and $\cdot$ operations of R. Matrix rings are one of the main reasons people are studying noncommutative rings.

  Note that if R is not commutative, then this ring $R^{n \times n}$ is not commutative even for $n = 1$.

  [Here I was asked what a 0×0-matrix is. Well, it pays off to be literal: It is a table with 0 rows, 0 columns and 0 entries.]

At this point, the "endowed with..." phrase has become somewhat of a ritual incantation: Most of our rings are endowed with the exact operations ($+$ and $\cdot$) and special elements (0 and 1) you would guess if I just told you the set. Thus, in future, I will omit this phrase unless I actually mean to endow the ring with some unexpected operations. In particular, if I say that a set of numbers is a ring, then I automatically understand it to be endowed with the usual addition,

the usual multiplication, the usual zero 0 and the usual unity 1, unless I say otherwise.

We continue with our litany of examples:

- Another famous noncommutative ring is the ring of **Hamilton quaternions** $\mathbb{H}$. Its elements are the "formal expressions" of the form $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{R}$. (To be more rigorous, you can define them to be 4-tuples (a, b, c, d) with $a, b, c, d \in \mathbb{R}$; the "formal" sum $a + bi + cj + dk$ can be viewed as just a fancy way to write such a 4-tuple.) Addition is defined by the distributive law:

$$\begin{aligned}&(a + bi + cj + dk) + \left(a' + b'i + c'j + d'k\right) \\ &= \left(a + a'\right) + \left(b + b'\right) i + \left(c + c'\right) j + \left(d + d'\right) k.\end{aligned}$$

  Multiplication is also defined by the distributive law using the formulas

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j$$

  (and the rule that any real number should commute with any of i, j, k). For example, the distributive law yields

$$(1 + i)(2 + k) = 2 + k + \underbrace{i \cdot 2}_{=2i} + \underbrace{ik}_{=-j} = 2 + k + 2i + (-j) = 2 + 2i - j + k.$$

  We will see in Section 3.12 that this $\mathbb{H}$ is indeed a ring. It is not commutative. It is used in computer graphics (quaternions encode rotations in 3D space), physics and number theory(!). In particular, Lagrange's four-squares theorem, which says that any positive integer can be written as a sum of four perfect squares, can be proved using quaternions!

- If you like the empty set, you will enjoy the **zero ring**. This is the ring which is defined as the one-element set $\{0\}$, endowed with the only possible operations $+$ and $\cdot$ and its only possible 0 and 1 (there is only one possibility for each of these, since the ring only has element!). So its zero and its unity are both 0 (nobody said that they have to be distinct!), and it has $0 + 0 = 0$ and $0 \cdot 0 = 0$.

  The zero ring is, of course, commutative. It plays the same role in the world of rings as the empty set does in the world of sets: It contains no interesting information whatsoever, but its existence is important for things to work.

  Generally, a **trivial ring** is defined to be a ring containing only one element. Every trivial ring can be viewed as the zero ring with its element 0 relabelled.

- For every integer n, the residue classes[8] of integers modulo n form a commutative ring, which is called $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/n$ or $\mathbb{Z}_n$ (depending on the author; beware that $\mathbb{Z}_n$ has two different meanings). You already know its additive group $(\mathbb{Z}/n, +, 0)$, which is classically called the **cyclic group of order** n. The multiplication is defined just as addition is: namely, we set
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b} \qquad \text{for any } a, b \in \mathbb{Z}.$$
(where the overline means "residue class modulo n"). This is all known as **modular arithmetic**.

  The ring $\mathbb{Z}/n$ has n elements when $n > 0$. In particular, $\mathbb{Z}/1\mathbb{Z}$ is a trivial ring. In contrast, as we already mentioned in Section 1.4, the ring $\mathbb{Z}/0\mathbb{Z}$ is just $\mathbb{Z}$ with its elements relabelled (since a residue class modulo 0 only contains a single integer).

- Here is yet another very small ring: Let F_4 be a set consisting of four distinct elements $0, 1, a, b$. Define two binary operations $+$ and $\cdot$ on F_4 by the following tables:

$x+y$	$y=0$	$y=1$	$y=a$	$y=b$
$x=0$	0	1	a	b
$x=1$	1	0	b	a
$x=a$	a	b	0	1
$x=b$	b	a	1	0

$x \cdot y$	$y=0$	$y=1$	$y=a$	$y=b$
$x=0$	0	0	0	0
$x=1$	0	1	a	b
$x=a$	0	a	b	1
$x=b$	0	b	1	a

  .

  Then, I claim that F_4 is a ring (with zero 0 and unity 1). This can be proved by meticulously checking that all the ring axioms are satisfied. Arguably, this is rather boring[9]. Eventually, we will find a way around this busywork by constructing this ring F_4 in a different (more conceptual) way.

[8] See Section 1.4 for a refresher on residue classes.

[9] For example, checking associativity of multiplication requires proving $(ab)\,c = a\,(bc)$ for $4^3 = 64$ different triples $(a, b, c) \in (F_4)^3$.

This ring F_4 is easily seen to be commutative (since the table for $x \cdot y$ is symmetric across the diagonal). Its additive group $(F_4, +, 0)$ is the famous Klein four-group, characterized by the fact that it has four elements and each element x satisfies $x + x = 0$.

Note that both rings F_4 and $\mathbb{Z}/4$ are commutative rings with 4 elements each. But they are rather different; in particular, F_4 is not just "$\mathbb{Z}/4$ with its labels taken off"[10].

- Here is one more ring with 4 elements: Let D_4 be a set consisting of four distinct elements $0, 1, a, b$. Define a binary operation $+$ on D_4 in the same way as for F_4 in the previous example (i.e., using the exact same table). Define a new binary operation $\cdot$ on D_4 by the following table:

$x \cdot y$	$y = 0$	$y = 1$	$y = a$	$y = b$
$x = 0$	0	0	0	0
$x = 1$	0	1	a	b
$x = a$	0	a	0	a
$x = b$	0	b	a	1

.

Then, D_4 is a commutative ring (with zero 0 and unity 1). This ring differs crucially from both $\mathbb{Z}/4$ and F_4.

- Yet another ring with 4 elements is the ring B_4, which again consists of four distinct elements $0, 1, a, b$ and again has the same binary operation $+$ as F_4 and D_4, but now has a multiplication $\cdot$ given by the table

$x \cdot y$	$y = 0$	$y = 1$	$y = a$	$y = b$
$x = 0$	0	0	0	0
$x = 1$	0	1	a	b
$x = a$	0	a	a	0
$x = b$	0	b	0	b

.

This is again a commutative ring with zero 0 and unity 1.

More examples of rings can be found below (e.g., in Exercises 2.3.2, 2.10.6 and 2.3.6) and in the next few exercises.

[10] Here is one difference: Every element $x \in F_4$ satisfies $x + x = 0$, but not every element $x \in \mathbb{Z}/4$ satisfies this.

Exercise 2.1.1. There is a certain ring F_8 consisting of eight distinct elements $0, 1, a, b, c, d, e, f$. Its addition $+$ and its multiplication $\cdot$ are given by the following tables:

$x+y$	$y=0$	$y=1$	$y=a$	$y=b$	$y=c$	$y=d$	$y=e$	$y=f$
$x=0$	0							
$x=1$		0						
$x=a$		b	0					
$x=b$		a	1					
$x=c$		d	e		0			
$x=d$		c	f		1			
$x=e$		f	c		a			
$x=f$		e	d		b			

$x\cdot y$	$y=0$	$y=1$	$y=a$	$y=b$	$y=c$	$y=d$	$y=e$	$y=f$
$x=0$								
$x=1$		1						
$x=a$		a	c		b			
$x=b$		b						
$x=c$		c	b		e			
$x=d$								
$x=e$								
$x=f$								

.

Oops, I lost most of the entries! Reconstruct all missing entries in the tables. (You can take it for granted that F_8 really is a ring.)

[**Hint:** Start by showing that "0" and "1" really are the zero and the unity.]

Recall that complex numbers were defined as pairs (a, b) of real numbers, with entrywise addition

$$(a, b) + (c, d) = (a + c,\ b + d)$$

and a certain weird-looking multiplication

$$(a, b) \cdot (c, d) = (ac - bd,\ ad + bc).$$

By setting $i = (0, 1)$, and identifying each real number r with the complex number $(r, 0)$, we can then write each complex number (a, b) in the familiar form $a + bi$.

In the next exercise, we will define a different kind of "numbers": the **dual numbers**[11]. They, too, are defined as pairs (a, b) of real numbers, and again they are added entrywise, but their multiplication is different from the multiplication of complex numbers:

Exercise 2.1.2. We define a **dual number** to be a pair (a, b) of two real numbers a and b.

We let $\mathbb{D}$ be the set of all dual numbers.

Define an addition $+$ and a multiplication $\cdot$ on $\mathbb{D}$ by setting

$$(a, b) + (c, d) = (a + c,\ b + d) \qquad \text{and}$$
$$(a, b) \cdot (c, d) = (ac,\ ad + bc)$$

for all $(a, b) \in \mathbb{D}$ and $(c, d) \in \mathbb{D}$. (Note that the only difference to complex numbers is the definition of $\cdot$, which is lacking a $-bd$ term.)

(a) Prove that $\mathbb{D}$ becomes a commutative ring when equipped with these two operations and with the zero $(0, 0)$ and the unity $(1, 0)$.

This ring $\mathbb{D}$ will be called the **ring of dual numbers**.

We shall identify each real number r with the dual number $(r, 0)$.

We let ε denote the dual number $(0, 1)$.

(b) Prove that, for any $a, b \in \mathbb{R}$, we have $a + b\varepsilon = (a, b)$ in $\mathbb{D}$ (where a, of course, means the dual number $(a, 0)$).

(c) Prove that $\varepsilon^2 = 0$ in $\mathbb{D}$.

The usefulness of dual numbers stems from the fact that the dual number ε is a sort of "algebraic infinitesimal" (in the sense that $\varepsilon \neq 0$ but $\varepsilon^2 = 0$). We will eventually see (in Exercise 5.3.10) that by evaluating a polynomial at a dual number of the form $(a, 1)$, we obtain not only the value of the polynomial at a but also its derivative at a.

2.1.3. Notes on the definitions

Remark 2.1.3. Our above definition of a ring has some redundancies:

First of all, the $0 \cdot a = a \cdot 0 = 0$ axiom follows from distributivity and the groupness of $(R, +, 0)$. This is why it appears in [DumFoo04] as a theorem ([DumFoo04, Proposition 1 on page 226]), not as an axiom.

Second, we can drop the "abelian" in the axiom "$(R, +, 0)$ is an abelian group"; in other words, we can drop the requirement that addition be commutative. This is because this requirement can be derived from the remaining axioms (see [DumFoo04, page 223]). But this is a bit artificial. I am

[11] Do they really deserve to be called "numbers"? Matter of taste. But with the adjective "dual", the terminology is unambiguous.

> aiming not for a minimal set of axioms, but for a reasonable set of axioms that strikes the balance between usefulness (i.e., important things are easy to derive from the axioms) and verifiability (i.e., it is easy to check these axioms in meaningful cases).

The kind of rings we defined above aren't the same kind of rings [DumFoo04] defines. The latter differ in that they are "lacking a unity". I will call them **nonunital rings**:

> **Definition 2.1.4.** A **nonunital ring** is defined in the same way as we defined a ring, except we no longer require a unity, and we replace the axiom "$(R, \cdot, 1)$ is a monoid" by "the operation $\cdot$ is associative". In particular, any ring is a nonunital ring, but not vice versa.

Note that the word "nonunital" means "we don't require a unity", not "the ring must not have a unity".

For example, the set $2\mathbb{Z}$ of all even integers (i.e., the set $\{\ldots, -4, -2, 0, 2, 4, \ldots\}$) is a nonunital ring (when equipped with the usual operations), but not a ring in our sense.

Beware:

- What we call a ring is called a "ring with identity" (or "ring with 1") in [DumFoo04].
- What we call a nonunital ring is just called a "ring" in [DumFoo04].

For an enlightening polemic about why rings in our sense (i.e., rings with a unity) are a more important concept than nonunital rings, see [Poonen18].

Historically, the concept of a ring originated in the late 19th century in number-theoretical considerations of Dedekind, Kronecker and Hilbert, and emerged gradually from particular cases. Until the late 1930s, its definition was rather fluid: Different authors imposed fewer or more axioms depending on their specific needs. By the 1970s perhaps, the definition had stabilized (thanks to the work of Noether and the textbook [Waerde91] by van der Waerden), except for the questions as to whether a ring should always have a unity (i.e., the very point on which we disagree with [DumFoo04]) and occasionally as to whether a ring should always be commutative (we believe they should not, but a number of mathematicians whose entire career is built on the study of commutative rings prefer to have fewer words to type).

More on the history of rings can be found in `https://mathshistory.st-andrews.ac.uk/HistTopics/Ring_theory/` .

2.2. Calculating in rings

2.2.1. What works in arbitrary rings

You can think of a commutative ring as a "generalized number system". In particular, all computations that can be performed with the operations $+$, $-$ and $\cdot$ on integers can be similarly made in any commutative ring. To some extent, this holds also for general (noncommutative) rings.

For instance, if $a_1, a_2, \ldots, a_n$ are n elements of a ring, then the sum $a_1 + a_2 + \cdots + a_n$ is well-defined, and can be computed by adding the elements $a_1, a_2, \ldots, a_n$ together in any order[12]. More generally, finite sums of the form $\sum_{s \in S} a_s$ are defined when the a_s belong to a ring[13], and these sums behave just like finite sums of numbers.

The same holds for finite products when the ring is commutative. If the ring is not commutative, then finite products in a specified order – like $a_1 a_2 \cdots a_n$ – are still well-defined[14], but unordered finite products – like $\prod_{s \in S} a_s$ – are not, unless you have "local commutativity" (i.e., the a_s commute with each other).[15]

In any ring, subtraction satisfies the rules you would expect: For any two elements a, b of a ring, we have

$$\begin{aligned} (-a)\, b &= a\, (-b) = -(ab)\,; \\ (-a)\, (-b) &= ab; \\ (-1)\, a &= -a. \end{aligned}$$

See [DumFoo04, §7.1, Proposition 1] for the easy proofs. Furthermore, any

[12] This means that, for example, the four sums $((a_1 + a_2) + a_3) + a_4$ and $(a_3 + (a_2 + a_4)) + a_1$ and $(a_2 + a_3) + (a_4 + a_1)$ are equal (for fixed elements a_1, a_2, a_3, a_4 of a ring).

This fact is known as **general commutativity** (or **generalized commutativity**), and is true not just for rings but also (more generally) for arbitrary abelian monoids (where $+$ is the operation of the monoid). For a proof, see (e.g.) [Grinbe15, Theorem 2.118 **(a)**] (which superficially only discusses real numbers, but gives a proof that applies verbatim to any ring) or `https://proofwiki.org/wiki/General_Commutativity_Theorem` (where the operation we call $+$ is called $\circ$).

[13] It should be kept in mind that empty sums (i.e., sums of the form $\sum_{s \in \varnothing} a_s$) are defined to equal the zero of the ring.

[14] This means that the product is the same no matter "where the parentheses are placed". For example, a product $abcde$ of five elements can be computed as $(((ab)\, c)\, d)\, e$ or as $a\, (b\, (c\, (de)))$ or as $(a\, (bc))\, (de)$ or in several other ways, and all these ways lead to the same result.

This fact is known as **general associativity** (or **generalized associativity**), and is true not just for rings but also (more generally) for arbitrary monoids. For a proof, see (e.g.) [Ford22, Lemma 2.1.4] or `https://groupprops.subwiki.org/wiki/Associative_implies_generalized_associative` or `https://math.stackexchange.com/questions/2459697/prove-generalized-associative-law` .

[15] It should be kept in mind that empty products (i.e., products of the form $\prod_{s \in \varnothing} a_s$) are defined to equal the unity of the ring.

three elements a, b, c of a ring satisfy the "subtractive distributivity laws"

$$a(b-c) = ab - ac \qquad \text{and} \qquad (a-b)c = ac - bc.$$

(These follow easily from the standard distributivity laws that are part of the ring axioms.) Moreover, distributivity holds for finite sums as well:

$$\sum_{s \in S} a_s b = \left(\sum_{s \in S} a_s \right) b \qquad \text{and} \qquad \sum_{s \in S} b a_s = b \left(\sum_{s \in S} a_s \right).$$

If n is an integer and a is an element of a ring R, then we define an element na of R by

$$na = \begin{cases} \underbrace{a + a + \cdots + a}_{n \text{ addends}}, & \text{if } n \geq 0; \\ -\left(\underbrace{a + a + \cdots + a}_{-n \text{ addends}} \right), & \text{if } n < 0 \end{cases}.$$

This defines the product of an integer with an element of R. This new "multiplication" operation is usually called "**scaling**" rather than "multiplication", since its two inputs are of different types: The first is an integer, while the second is an element of R. In general, it is unrelated to the product of two elements of R, although these operations usually agree when $\mathbb{Z}$ is a subset of R (unless the multiplication of R is defined in a particularly pathological way[16]).

We note that $0a = 0$ for any $a \in R$, where the "0" on the left hand side is the integer 0. This is because an empty sum is defined to be 0.

If n is a nonnegative integer and a is an element of a ring R, then we define an element a^n of R (called the **n-th power** of a) by

$$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ factors}}.$$

In particular, applying this definition to $n = 0$, we obtain

$$a^0 = (\text{empty product}) = 1_R \qquad \text{for each } a \in R.$$

Furthermore, $a^1 = a$ for each $a \in R$.

Thus we can scale elements of a ring by integers, and take them to nonnegative integer powers. These operations satisfy the identities you would expect them to satisfy: For example, for any $a, b \in R$ (with R being a ring) and any

[16] If R is the ring $\mathbb{Z}'$ defined in Subsection 2.1.2, then the two operations do not agree, i.e., the expression "na" has different values depending on whether you are viewing it as a product of two elements of R or as a product of an integer with an element of R. But this is no surprise, since our definition of $\mathbb{Z}'$ relied on deliberately altering the multiplication.

$n, m \in \mathbb{Z}$, we have

$$\begin{aligned} (n+m)\, a &= na + ma; \\ n\,(a+b) &= na + nb; \\ (nm)\, a &= n\,(ma)\,; \\ (-1)\, a &= -a. \end{aligned}$$

Furthermore, for any $a \in R$ and any $n, m \in \mathbb{N}$, we have

$$\begin{aligned} a^{n+m} &= a^n a^m; \\ a^{nm} &= \left(a^n\right)^m. \end{aligned}$$

Also,

$$\begin{aligned} 1^n &= 1 \qquad \text{for } n \in \mathbb{N}; \\ 0^n &= \begin{cases} 0, & \text{if } n > 0; \\ 1, & \text{if } n = 0 \end{cases} \qquad \text{for } n \in \mathbb{N} \end{aligned}$$

(where, of course, the "1" and "0" stand for 1_R and 0_R, except for the two "0"s in "$n > 0$" and in "$n = 0$".)

Moreover, if $a, b \in R$ satisfy $ab = ba$, then we have

$$a^i b^j = b^j a^i \qquad \text{for } i, j \in \mathbb{N} \tag{1}$$

and

$$(ab)^n = a^n b^n \qquad \text{for } n \in \mathbb{N} \tag{2}$$

and (the binomial formula)

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad \text{for } n \in \mathbb{N}. \tag{3}$$

All of this is proved just as for numbers.

Exercise 2.2.1. Actually prove these equalities (1), (2) and (3).

Exercise 2.2.2. Prove that the three equalities (1), (2) and (3) can fail if we don't require $ab = ba$. For instance, find two 2×2-matrices $a, b \in \mathbb{Q}^{2\times 2}$ that violate (1) for $i = j = 2$, violate (2) for $n = 2$ and violate (3) for $n = 2$.

We note that even when two elements a and b of a ring R don't satisfy $ab = ba$, the n-th power $(a+b)^n$ can be expanded using distributivity; the result will just not usually be as nice as (3). For example,

$$(a+b)^3 = a^3 + a^2 b + aba + ab^2 + ba^2 + bab + b^2 a + b^3.$$

The following exercise generalizes the well-known "geometric sum" formula $1 + q + q^2 + \cdots + q^{n-1} = \dfrac{1-q^n}{1-q}$ (for $q \neq 1$):

Exercise 2.2.3. Let R be any ring. Let $a, b \in R$ satisfy $ab = ba$. Let $n \in \mathbb{N}$. Prove that

$$a^n - b^n = (a-b) \cdot \underbrace{\sum_{k=0}^{n-1} a^k b^{n-1-k}}_{=a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1}}.$$

(Note that when $n = 0$, the sum $\sum_{k=0}^{n-1} a^k b^{n-1-k}$ is an empty sum and thus equals 0 by definition.)

The following exercises provide some practice with calculating in rings:

Exercise 2.2.4.

(a) Without computing the integer 7^4, prove that $\overline{7}^4 = \overline{1}$ in the ring $\mathbb{Z}/10$.

(b) Find a simple rule for the k-th power $\overline{7}^k$ of the element $\overline{7}$ in the ring $\mathbb{Z}/10$. Specifically, this rule should express $\overline{7}^k$ in terms of the remainder that k leaves when divided by 4.

(c) What is the units digit of the number 7^{9999} ?

Exercise 2.2.5.

(a) Prove that every element $x \in \mathbb{Z}/7$ satisfies $x^7 = x$ in $\mathbb{Z}/7$.

(b) In the ring $\mathbb{H}$ of Hamilton quaternions (see Subsection 2.1.2), compute ijk and $(1+i+j+k)^2$.

Next, recall the ring F_4 constructed in Subsection 2.1.2, with its four elements $0, 1, a, b$.

(c) Prove that $a^4 = a$ in this ring.

(d) What is b^4 ?

[Part **(a)** is generalized in Proposition 2.6.4 below, whereas parts **(c)** and **(d)** are generalized in Proposition 2.6.6.]

Exercise 2.2.6.

(a) In the ring $\mathbb{H}$ of Hamilton quaternions (see Subsection 2.1.2), prove that $(ai+bj+ck)^2 = -\left(a^2+b^2+c^2\right)$ for any $a, b, c \in \mathbb{R}$.

(b) Conclude that there are infinitely many quaternions $w \in \mathbb{H}$ satisfying $w^2 = -1$.

2.2.2. What doesn't work in arbitrary rings

Here are some things that might feel less familiar. Again, we let R be a ring, and we let a, b be two elements of R.

- It is not always true that $a \neq 0$ and $b \neq 0$ implies $ab \neq 0$. This fails in the ring $\mathbb{Z}/6$ (for example, you can pick $a = \overline{2}$ and $b = \overline{3}$ to get $ab = \overline{2} \cdot \overline{3} = \overline{2 \cdot 3} = \overline{6} = \overline{0}$, even though a and b are $\neq \overline{0}$) and in matrix rings like $\mathbb{Z}^{2\times 2}$ (here you can pick $a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ to get $ab = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, even though neither a nor b is the zero matrix).
- It is not always true that $ab = 1$ implies $ba = 1$. This would be true in the classical matrix rings $\mathbb{R}^{n\times n}$ and $\mathbb{C}^{n\times n}$, in any commutative ring (for obvious reasons), and in any finite ring (for less obvious reasons), but may fail in arbitrary rings. (Counterexamples are not easy to find; see [DumFoo04, §7.1, exercise 30 (a)] for one.)

2.2.3. Idempotents

The next few exercises are concerned with the notion of "idempotent elements" of a ring. This is a useful notion, but more importantly, the exercises should provide some practice with calculations in rings.

Definition 2.2.1. Let R be a ring.

(a) An element a of R is said to be **idempotent** if it satisfies $a^2 = a$.

(b) An element a of R is said to be **involutive** if it satisfies $a^2 = 1$.

Some examples first: The idempotent elements of $\mathbb{R}$ are 0 and 1. The involutive elements of $\mathbb{R}$ are 1 and -1. The ring $\mathbb{Z}/6$ has four idempotent elements ($\overline{0}$, $\overline{1}$, $\overline{3}$ and $\overline{4}$) and two involutive elements ($\overline{1}$ and $\overline{5}$). A matrix ring like $\mathbb{R}^{n\times n}$ usually has infinitely many idempotent elements (viz., all projection matrices on subspaces of $\mathbb{R}^n$) and infinitely many involutive elements (viz., all matrices A satisfying $A^2 = I_n$; for instance, all reflections across hyperplanes are represented by such matrices).

Exercise 2.2.7. Let p be a prime number, and let k be a positive integer.

(a) Prove that the only idempotent elements of the ring $\mathbb{Z}/p^k$ are $\overline{0}$ and $\overline{1}$.

(b) Now assume furthermore that $p \neq 2$. Prove that the only involutive elements of the ring $\mathbb{Z}/p^k$ are $\overline{1}$ and $\overline{-1}$.

Exercise 2.2.8. Let R be a ring. Prove the following:

(a) If a is an idempotent element of R, then $1 - a \in R$ is again idempotent.

(b) If a is an involutive element of R, then $-a \in R$ is again involutive.

(c) If a is an idempotent element of R, then $a^n = a$ for each positive $n \in \mathbb{N}$.

(d) If a is an idempotent element of R, then $(1+a)^n = 1 + (2^n - 1)\, a$ for each $n \in \mathbb{N}$.

(e) If a is an involutive element of R, then $(1+a)^n = 2^{n-1}\,(1+a)$ for each positive $n \in \mathbb{N}$.

Exercise 2.2.9. Let R be a ring.

(a) Let $a \in R$. Prove that if a is idempotent, then $1 - 2a$ is involutive.

(b) Now, assume that 2 is **cancellable** in R; this means that if u and v are two elements of R satisfying $2u = 2v$, then $u = v$. Prove that the converse of the claim of part **(a)** holds: If $a \in R$ is such that $1 - 2a$ is involutive, then a is idempotent.

(c) Now, let $R = \mathbb{Z}/4\mathbb{Z}$. Find an element $a \in R$ such that $1 - 2a$ is involutive, but a is not idempotent.

Exercise 2.2.9 **(a)** assigns an involutive element to each idempotent element of R. If 2 is invertible in R (that is, if the element $2 \cdot 1_R$ has a multiplicative inverse), then this assignment is a bijection (as can be easily derived from Exercise 2.2.9 **(b)**). Note that this assignment, when applied to a matrix ring $\mathbb{R}^{n\times n}$, is exactly the assignment you would expect from the geometric point of view: To the orthogonal projection on a hyperplane H, it assigns the reflection in the hyperplane H. Exercise 2.2.9 **(c)** shows that we cannot drop the "2 is cancellable" condition in Exercise 2.2.9 **(b)**.

2.3. Subrings ([DumFoo04, §7.1])

2.3.1. Definition

Groups have subgroups; vector spaces have subspaces (and so do topological spaces, although the two notions have little in common). Not surprisingly, the same is true for rings, and you can guess the definition:

Definition 2.3.1. Let R be a ring. A **subring** of R is a subset S of R such that

- we have $a + b \in S$ for any $a, b \in S$;

- we have $ab \in S$ for any $a, b \in S$;
- we have $-a \in S$ for any $a \in S$;
- we have $0 \in S$ (where the 0 means the zero of R);
- we have $1 \in S$ (where the 1 means the unity of R).

The five conditions in Definition 2.3.1 are called the "**subring axioms**". The first of these five axioms is often reformulated as "S is closed under addition"; the second then becomes "S is closed under multiplication"; the third becomes "S is closed under negation". Thus, a subring of a ring is a subset that is closed under addition, closed under multiplication, closed under negation, and contains the zero and the unity.

The following is essentially obvious:

Proposition 2.3.2. Let S be a subring of a ring R. Then, S automatically is a ring in its own right (with its operations $+$ and $\cdot$ obtained by restricting the corresponding operations of R, and with its elements 0 and 1 passed down from R).

2.3.2. Examples

Here are some examples of subrings:

- From the classical construction of the number systems, you know that $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Each of these three "$\subseteq$" signs can be strengthened to "is a subring of" (for example, $\mathbb{Z}$ is a subring of $\mathbb{Q}$).
- We can extend this chain further to the right: $\mathbb{C}$ is a subring of $\mathbb{H}$ (the quaternions).
- However, we **cannot** extend this chain to the left: The only subring of $\mathbb{Z}$ is $\mathbb{Z}$ itself. Indeed, a subring of $\mathbb{Z}$ would have to contain 0 and 1 (by definition), thus also any sum of the form $1 + 1 + \cdots + 1$ (since a subring is closed under addition), i.e., any positive integer, and therefore also any negative integer (since it is closed under negation), and thus any integer. But this means that it is $\mathbb{Z}$.
- There are lots of rings between $\mathbb{Z}$ and $\mathbb{Q}$ (that is, rings $\mathbb{B}$ such that $\mathbb{Z}$ is a subring of $\mathbb{B}$ and $\mathbb{B}$ in turn is a subring of $\mathbb{Q}$). You will see some of these in Exercise 2.3.2. Here is another: Let $\mathbb{Q}_{\text{odd}}$ be the ring of all rational numbers of the form

$$\frac{a}{b} \qquad \text{with } a \in \mathbb{Z} \text{ being arbitrary and } b \in \mathbb{Z} \text{ being odd.}$$

Then, $\mathbb{Q}_{\text{odd}}$ is a subring of $\mathbb{Q}$ (this is pretty easy to check[17]), and $\mathbb{Z}$ is a subring of $\mathbb{Q}_{\text{odd}}$.

- There are myriad rings between $\mathbb{Q}$ and $\mathbb{R}$. For example, the ring $\mathbb{S}$ from Subsection 2.1.2 is one of these.

- There are no rings between $\mathbb{R}$ and $\mathbb{C}$. That is, if a subring of $\mathbb{C}$ contains $\mathbb{R}$ as a subring, then this subring must be either $\mathbb{R}$ or $\mathbb{C}$ itself. This is not hard to prove (but I won't do so here).

- There are rings between $\mathbb{Z}$ and $\mathbb{C}$ that are neither subrings nor "superrings" of $\mathbb{R}$. A particularly important one is the ring $\mathbb{Z}[i]$ of **Gaussian integers**. A **Gaussian integer** is a complex number of the form $a+bi$ where a and b are integers (and where i is the imaginary unit $\sqrt{-1}$). For example, $3+5i$ and $-7+8i$ are Gaussian integers. It is easy to see that $\mathbb{Z}[i]$ is indeed a subring of $\mathbb{C}$, and of course $\mathbb{Z}$ is a subring of $\mathbb{Z}[i]$. But $\mathbb{Z}[i]$ is not an intermediate stage on the $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ "chain"; it is a "detour".

  Likewise, there is a ring $\mathbb{Q}[i]$ of **Gaussian rationals**, which are defined just as Gaussian integers but using rational numbers (instead of integers) for a and b. This ring $\mathbb{Q}[i]$ is sandwiched between $\mathbb{Q}$ and $\mathbb{C}$.

- Recall the ring of functions from $\mathbb{Q}$ to $\mathbb{Q}$. Similarly, there is a ring of functions from $\mathbb{R}$ to $\mathbb{R}$. The latter has a subring consisting of all **continuous** functions from $\mathbb{R}$ to $\mathbb{R}$. To see that this is indeed a subring, you need to show that the sum and the product of two continuous functions are continuous, that the negation $-f$ of a continuous function f is continuous, and that the constant-0 and constant-1 functions are continuous.

- Let $n \in \mathbb{N}$, and let R be any ring. Recall the matrix ring $R^{n\times n}$, consisting of all $n \times n$-matrices with entries in R. Then,

$$\begin{aligned} R^{n\leq n} &:= \{\text{all upper-triangular } n\times n\text{-matrices with entries in } R\} \\ &= \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ 0 & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n,n} \end{pmatrix} \;\mid\; a_{i,j} \in R \text{ for all } i \leq j \right\} \end{aligned}$$

[17] For example, in order to check that $\mathbb{Q}_{\text{odd}}$ is closed under addition, we need to verify that the sum of two numbers of the form $\frac{a}{b}$ (with $a \in \mathbb{Z}$ being arbitrary and $b \in \mathbb{Z}$ being odd) is again a number of this form. But this follows easily from the formula $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, along with the fact that a product of two odd numbers is odd.

is a subring of $R^{n\times n}$ (because the sum and the product of two upper-triangular matrices are again upper-triangular, and because the zero matrix and the identity matrix are upper-triangular). Similarly,

$$\begin{aligned} R^{n\geq n} &:= \{\text{all lower-triangular } n\times n\text{-matrices with entries in } R\} \\ &= \left\{ \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ a_{2,1} & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \;\mid\; a_{i,j} \in R \text{ for all } i \geq j \right\} \end{aligned}$$

is a subring of $R^{n\times n}$. The intersection $R^{n\leq n} \cap R^{n\geq n}$ of these two subrings is again a subring of $R^{n\times n}$ (and its elements are the diagonal $n\times n$-matrices). However,

$$\begin{aligned} R^{n\times n}_{\text{symm}} &:= \{\text{all symmetric } n\times n\text{-matrices with entries in } R\} \\ &= \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \;\mid\; a_{i,j} = a_{j,i} \in R \text{ for all } i,j \right\} \end{aligned}$$

is **not** a subring of $R^{n\times n}$ unless $n \leq 1$ or R is trivial (since in all other cases, it is easy to find two symmetric matrices whose product is not symmetric[18]).

Warning 2.3.3. Beware that our Definition 2.3.1 does not agree with the definition of a "subring" in [DumFoo04].

Indeed, [DumFoo04] does **not** require $1 \in S$ for a subring, because [DumFoo04] does not require rings to have a 1 in the first place. Thus, for example, the nonunital ring $2\mathbb{Z}$ is a subring of $\mathbb{Z}$ in [DumFoo04]'s sense (but not in our sense, since we don't even count $2\mathbb{Z}$ as a ring). Even more confusingly, it can happen that S and R are two rings in our sense (i.e., they both have unities), and S is a subring of R in [DumFoo04]'s sense (i.e., S satisfies our definition of a subring, minus the "$1 \in S$" axiom), but not a subring of R in our sense (because its unity is not the unity of R). For example, the zero ring is a subring of $\mathbb{Z}$ in [DumFoo04]'s sense, but not in ours (since the unity of the zero ring is the number 0). Alas, there are less pathological examples, too, so this isn't something you can ignore. For example, you can pretend that each 2×2-matrix is secretly a 3×3-matrix by inserting a zero row at the bottom and a zero column at the right (i.e., identifying each 2×2-matrix

[18] For example, if $n = 2$, then the two symmetric matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ have product $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, which is not symmetric.

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with the 3×3-matrix $\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ 0 & 0 & 0 \end{pmatrix}$; note that I am not saying you **should** do that), and this makes $\mathbb{R}^{2\times 2}$ a subring of $\mathbb{R}^{3\times 3}$ in [DumFoo04]'s sense, but not in ours. Of course, this is one of the situations where you really need subscripts under the "1" to avoid confusing different unities.

The following exercises provide several more examples of subrings:

Exercise 2.3.1. Let c, d and g be three integers with $g \neq 0$. Assume that d is not a perfect square (i.e., not the square of an integer).

Let $\zeta = \dfrac{c + \sqrt{d}}{g}$. (This is a real number if $d \geq 0$, and a complex number if $d < 0$.) Set

$$X := \{a + b\zeta \mid a, b \in \mathbb{Z}\} \qquad \text{and}$$
$$Y := \{a + b\zeta \mid a, b \in \mathbb{Q}\}.$$

(a) Prove that Y is always a subring of $\mathbb{C}$.

(b) Prove that X is a subring of $\mathbb{C}$ if and only if we have $g \mid 2c$ and $c^2 \equiv d \bmod g^2$.

[**Hint:** Show that $g^2\zeta^2 = 2cg\zeta + \left(d - c^2\right)$.]

Note that the ring Y in Exercise 2.3.1 **(a)** generalizes the ring $\mathbb{Q}[i]$ of Gaussian rationals (obtained by setting $c = 0$ and $d = -1$ and $g = 1$), whereas the ring X in Exercise 2.3.1 **(b)** generalizes the ring $\mathbb{Z}[i]$ of Gaussian integers (obtained in the same way).

Exercise 2.3.2. Fix an integer m. An **m-integer** shall mean a rational number r such that there exists a $k \in \mathbb{N}$ satisfying $m^k r \in \mathbb{Z}$.

For example:

- Each integer r is an m-integer (since $m^k r \in \mathbb{Z}$ for $k = 0$).
- The rational number $\dfrac{5}{12}$ is a 6-integer (since $6^k \cdot \dfrac{5}{12} \in \mathbb{Z}$ for $k = 2$), but neither a 2-integer nor a 3-integer (since multiplying it by a power of 2 will not "get rid of" the prime factor 3 in the denominator, and vice versa[19]).
- The 1-integers are the integers (since $1^k r = r$ for all r).
- Every rational number r is a 0-integer (since $0^k r \in \mathbb{Z}$ for $k = 1$).

Let R_m denote the set of all m-integers. Prove that R_m is a subring of $\mathbb{Q}$.

[19] To make this more rigorous: If we had $2^k \cdot \dfrac{5}{12} \in \mathbb{Z}$ for some $k \in \mathbb{N}$, then we would have $12 \mid 2^k \cdot 5$, which would entail that $3 \mid 12 \mid 2^k \cdot 5$, and thus 3 would appear as a factor in the

The ring R_m in Exercise 2.3.2 is an example of a ring "between $\mathbb{Z}$ and $\mathbb{Q}$" (in the sense that $\mathbb{Z}$ is a subring of R_m, while R_m is a subring of $\mathbb{Q}$). Note that $R_1 = \mathbb{Z}$ and $R_0 = \mathbb{Q}$, whereas $R_2 = R_4 = R_8 = \cdots$ is the ring of all rational numbers that can be written in the form $a/2^k$ with $a \in \mathbb{Z}$ and $k \in \mathbb{N}$.

Here is another example of a subring of a matrix ring $R^{n\times n}$:

Exercise 2.3.3. Let $n \in \mathbb{N}$. Let R be any ring. An $n \times n$-matrix $A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \in R^{n\times n}$ will be called **centrosymmetric** if it satisfies

$$a_{i,j} = a_{n+1-i,\ n+1-j} \qquad \text{for all } i,j \in \{1,2,\ldots,n\}.$$

(Visually, this means that A is preserved under "180°-rotation", i.e., that any two cells of A that are mutually symmetric across the center of the matrix have the same entry. For example, a centrosymmetric 4×4-matrix has the form $\begin{pmatrix} a & b & c & d \\ e & f & g & h \\ h & g & f & e \\ d & c & b & a \end{pmatrix}$ for $a, b, \ldots, h \in R$.)

Prove that the set $\{$all centrosymmetric $n \times n$-matrices with entries in $R\}$ is a subring of $R^{n\times n}$.

[**Hint:** This can be done in a particularly slick way as follows: Let W be the $n \times n$-matrix obtained from the identity matrix I_n by a horizontal reflection (or, equivalently, a vertical reflection). For example, if $n = 4$, then $W = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$. Now, show that an $n \times n$-matrix A is centrosymmetric if and only if it satisfies $AW = WA$.]

Subrings can be used to answer a curious question: How small can a noncommutative ring be? A moment of thought leads us to the ring $(\mathbb{Z}/2)^{2\leq 2}$ of upper-triangular matrices with entries in $\mathbb{Z}/2$; this ring is noncommutative and has size 8 (since there are 2 choices for each of the three entries of such a matrix, not counting the bottom-left entry because that entry must be $\overline{0}$). Thus, a noncommutative ring can have size 8. A smaller size is not possible, as follows from the following exercise:

Exercise 2.3.4. Let R be a finite ring. Assume that its size $|R|$ is either a prime number p or a product pq of two (not necessarily distinct!) prime numbers p and q. Our goal is to show that R is commutative.

---

prime factorization of $2^k \cdot 5$. But this is absurd. Hence, $2^k \cdot \dfrac{5}{12} \in \mathbb{Z}$ cannot hold. Similarly, $3^k \cdot \dfrac{5}{12} \in \mathbb{Z}$ cannot hold.

Consider the abelian group $(R, +, 0)$. If $u_1, u_2, \ldots, u_k$ are any elements of R, then $\langle u_1, u_2, \ldots, u_k \rangle$ shall denote the subgroup of this abelian group $(R, +, 0)$ generated by $u_1, u_2, \ldots, u_k$. (Explicitly, this subgroup consists of all sums of the form $a_1 u_1 + a_2 u_2 + \cdots + a_k u_k$ with $a_1, a_2, \ldots, a_k \in \mathbb{Z}$.)

Let $x, y \in R$. Consider the following chain of subgroups of $(R, +, 0)$:

$$0 \leq \langle 1 \rangle \leq \langle x, 1 \rangle \leq R.$$

(The symbol $\leq$ means "subgroup of".)

(a) Prove that at least one of the three "$\leq$" signs in this chain must be an "$=$" sign.

(b) Prove that $xy = yx$ if the first "$\leq$" sign is a "$=$" sign.

(c) Prove that $xy = yx$ if the second "$\leq$" sign is a "$=$" sign.

(d) Prove that $xy = yx$ if the third "$\leq$" sign is a "$=$" sign.

(e) Conclude that R is commutative.

[**Hint:** In part **(a)**, recall Lagrange's theorem about subgroups, and observe that a number m of the form p or pq cannot have a nontrivial chain of three divisors $1 \mid d \mid e \mid m$. Parts **(b)**, **(c)** and **(d)** are easy in their own ways.]

See Exercise 2.12.7 for a generalization of Exercise 2.3.4 **(e)**.

The following exercise gives a way to construct new subrings out of old ones:

Exercise 2.3.5.

(a) Let R be a ring. Let S and T be two subrings of R. Prove that $S \cap T$ is again a subring of R.

(b) For each integer m, define the subring R_m of $\mathbb{Q}$ as in Exercise 2.3.2. Prove that $R_m \cap R_n = R_{\gcd(m,n)}$ for all $m, n \in \mathbb{Z}$.

[**Hint:** Part **(a)** is easy. Part **(b)** requires a bit of elementary number theory.]

2.3.3. A first application

We haven't proved much so far, but we are already able to reap some first rewards. Namely, we shall prove two properties of the famous Fibonacci sequence. We recall its definition:

Definition 2.3.4. The **Fibonacci sequence** is the sequence of integers defined recursively by

$$f_0 = 0, \qquad f_1 = 1, \qquad \text{and} \qquad f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 2.$$

The first entries of this sequence are

n	0	1	2	3	4	5	6	7	8	9	10	11	12
f_n	0	1	1	2	3	5	8	13	21	34	55	89	144

.

Much more about this sequence can be found (e.g.) in [Vorobi02] or [Grinbe21]. The entries $f_0, f_1, f_2, \ldots$ of this sequence are known as the **Fibonacci numbers**.

We shall prove the following two facts:

Proposition 2.3.5. The Fibonacci sequence $(f_0, f_1, f_2, \ldots)$ satisfies

$$f_{n+m} = f_n f_{m+1} + f_{n-1} f_m$$

for all positive integers n and all nonnegative integers m.

Proposition 2.3.6. The Fibonacci sequence $(f_0, f_1, f_2, \ldots)$ satisfies

$$f_d \mid f_{dn} \qquad \text{for any nonnegative integers } d \text{ and } n.$$

There are many proofs of these propositions (see, e.g., [Grinbe21, Exercise 4.9.3] and [Grinbe21, Exercise 4.9.7] for generalizations proved in a very elementary way). We will give a proof that uses a certain commutative subring $\mathcal{F}$ of the matrix ring $\mathbb{Z}^{2\times 2}$ as a tool:

Exercise 2.3.6. Let A be the 2×2-matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{Z}^{2\times 2}$. Consider also the identity matrix $I_2 \in \mathbb{Z}^{2\times 2}$.

(a) Prove that $A^2 = A + I_2$.

Now, let $\mathcal{F}$ be the subset

$$\{aA + bI_2 \mid a, b \in \mathbb{Z}\} = \left\{ \begin{pmatrix} b & a \\ a & a+b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

of the matrix ring $\mathbb{Z}^{2\times 2}$.

(b) Prove that the set $\mathcal{F}$ is a **commutative** subring of $\mathbb{Z}^{2\times 2}$.

Next, let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence.

(c) Prove that $A^n = f_n A + f_{n-1} I_2$ for all positive integers n.

(d) Prove that $f_{n+m} = f_n f_{m+1} + f_{n-1} f_m$ for all positive integers n and all $m \in \mathbb{N}$. (This is Proposition 2.3.5.)

Now, define a further matrix $B \in \mathcal{F}$ by $B = (-1)\, A + 1 I_2 = I_2 - A$.

(e) Prove that $B^2 = B + I_2$ and $B^n = f_n B + f_{n-1} I_2$ for all positive integers n.

(f) Prove that $A^n - B^n = f_n (A - B)$ for all $n \in \mathbb{N}$.

(g) Prove that $f_d \mid f_{dn}$ for any nonnegative integers d and n. (This is Proposition 2.3.6.)

[**Hint:** In part **(b)**, don't forget to check commutativity! It is not inherited from $\mathbb{Z}^{2\times 2}$, since $\mathbb{Z}^{2\times 2}$ is not commutative.

One way to prove part **(d)** is by comparing the $(1,1)$-th entries of the two (equal) matrices $A^n A^{m+1}$ and A^{n+m+1}, after first using part **(c)** to compute these matrices.

For part **(g)**, compare the $(1,1)$-th entries of the matrices $A^d - B^d$ and $A^{dn} - B^{dn}$, after first proving that $A^d - B^d \mid A^{dn} - B^{dn}$ in the commutative ring $\mathcal{F}$. Note that divisibility is a tricky concept in general rings, but $\mathcal{F}$ is a commutative ring, which lets many arguments from the integer setting go through unchanged in $\mathcal{F}$.]

2.3.4. More computational exercises

Exercise 2.3.7. Let R be any ring. For any two elements $a, b \in R$, we define the element $[a, b]$ of R by

$$[a, b] := ab - ba.$$

This element $[a, b]$ is called the **commutator** of a and b (as it "measures" how much a and b violate the commutative law $ab = ba$). Don't confuse it with the group-theoretical commutator $aba^{-1}b^{-1}$, which is also denoted by $[a, b]$ (but is defined for groups rather than rings).

Prove that every three elements $a, b, c \in R$ satisfy the **Leibniz identity**

$$[a, bc] = [a, b]\, c + b\, [a, c]$$

and the **Jacobi identity**

$$[a, [b, c]] + [b, [c, a]] + [c, [a, b]] = 0.$$

Exercise 2.3.8. Let R be any ring. The determinant of a 2×2-matrix $A \in R^{2\times 2}$ is usually defined only when R is commutative, but let us (for this specific exercise) define it in general by the formula

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} := ad - bc \qquad \text{for any } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R^{2\times 2}.$$

Prove that the equality $\det(AB) = \det A \cdot \det B$ holds for every pair of two matrices $A, B \in R^{2\times 2}$ if and only if R is commutative.

[**Hint:** The "if"-direction can be considered well-known from linear algebra.]

Exercise 2.3.9. Let R be a commutative ring in which $2 \cdot 1_R = 0_R$. (Examples of such rings are $\mathbb{Z}/2$ or polynomial rings over $\mathbb{Z}/2$.)

Prove that the set of all idempotent elements $a \in R$ is a subring of R.

Exercise 2.3.10. Let R be a commutative ring in which $8 \cdot 1_R = 0_R$. (Examples of such rings are $\mathbb{Z}/2$, $\mathbb{Z}/4$ and $\mathbb{Z}/8$, but there are also many others, such as polynomial rings over $\mathbb{Z}/8$.)

Prove that the set of all elements $a \in R$ satisfying $(1-2a)^2 = 1$ is a subring of R.

2.3.5. The center of a ring, and the centralizer of a subset

Here is yet another way to construct subrings of a ring:

Definition 2.3.7. Let R be a ring.

(a) An element $a \in R$ is said to be **central** if all $b \in R$ satisfy $ab = ba$. (In other words, a is central if and only if a commutes with every element of R.)

(b) The **center** of R is the set of all central elements of R. This set is denoted by $Z(R)$.

Exercise 2.3.11. Let R be a ring. Prove that:

(a) The center $Z(R)$ of R is a commutative subring of R.

(b) We have $Z(R) = R$ if and only if R is commutative.

(c) All elements of the form $n \cdot 1_R$ for $n \in \mathbb{Z}$ belong to $Z(R)$.

Exercise 2.3.12.

(a) Prove that $Z(\mathbb{C}) = \mathbb{C}$ and $Z(\mathbb{H}) = \mathbb{R}$ (where $\mathbb{H}$ is the ring of quaternions).

(b) Compute $Z\left(\mathbb{R}^{2\times 2}\right)$ and $Z\left(\mathbb{R}^{2\leq 2}\right)$. (In other words, find the 2×2-matrices that commute with all 2×2-matrices, and find the upper-triangular 2×2-matrices that commute with all upper-triangular 2×2-matrices.)

The previous exercise illustrates a somewhat slippery point: If R is a subring of a ring S, then $Z(R)$ doesn't have to be a subring of $Z(S)$. An element of R that commutes with all elements of R might still fail to commute with some elements of S.

Exercise 2.3.13. Let R be a ring. Let $a, b \in R$ be such that $a + b$ is central. Prove that $ab = ba$.

Exercise 2.3.14. Let R be a ring. Let $a, b \in R$ be such that ab is central. Prove that $(ab)^n = a^n b^n$ for all $n \in \mathbb{N}$.

A generalization of the center is the "centralizer" of a subset of a ring:[20]

Definition 2.3.8. Let R be a ring. Let S be a subset of R.

(a) An element $a \in R$ is said to **centralize** S if and only if all $b \in S$ satisfy $ab = ba$. (In other words, a centralizes S if and only if a commutes with every element of S.)

(b) The **centralizer** of S in R is the set of all elements of R that centralize S. This set is denoted by $Z_R(S)$.

Note that $Z_R(R) = Z(R)$ is the center of R.

Exercise 2.3.15. Let R be a ring. Let S be a subset of R. Prove that:

(a) The centralizer $Z_R(S)$ is a subring of R.

(b) We have $Z_R(\varnothing) = Z_R(\{0\}) = Z_R(\{1\}) = R$. (This shows, in particular, that $Z_R(S)$ is not always commutative.)

(c) If T is a subset of S, then $Z_R(S) \subseteq Z_R(T)$.

(d) If T is a subset of $Z_R(S)$, then S is (in turn) a subset of $Z_R(T)$.

Exercise 2.3.16. Let R be the matrix ring $\mathbb{R}^{2\times 2}$. In this ring R, consider the two matrices

$$A := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad B := \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

(a) Describe the centralizer $Z_R(\{A, B\})$.

(b) Describe the centralizer $Z_R(\{A + B\})$.

(c) Describe the centralizer $Z_R(\{A - B\})$.

Exercise 2.3.17. Let R be a ring. Let S be a subset of R. Prove the following:

(a) We have $S \subseteq Z_R(Z_R(S))$.

[20] If you have seen centralizers in groups, you'll recognize this as an analogous notion.

(b) If $R = \mathbb{Q}$ and $S = \mathbb{Z}$, then S is a proper subset of $Z_R(Z_R(S))$.

(c) However, we always have $Z_R(S) = Z_R(Z_R(Z_R(S)))$.

2.4. Zero divisors and integral domains ([DumFoo04, §7.1])

Here comes a rather unsurprising definition:

Definition 2.4.1. An element of a ring R is said to be **nonzero** if it is $\neq 0$. (Here, 0 means 0_R.)

As we saw above, it can happen that a product of two nonzero elements of a ring R is zero. Let us give this phenomenon a name (at least in a commutative setting):

Definition 2.4.2. Let R be a commutative ring. A nonzero element $a \in R$ is called a **zero divisor** if there is a nonzero $b \in R$ such that $ab = 0$.

This definition is slightly controversial: Some people don't require a to be nonzero. Thus, to them, 0 is a zero divisor unless R is trivial. It's not a very well-conceived definition, but it's not used very much either.

Here are some examples:

- The elements $\overline{2}$, $\overline{3}$ and $\overline{4}$ of the ring $\mathbb{Z}/6$ are zero divisors, since they are nonzero but satisfy $\overline{2} \cdot \overline{3} = \overline{6} = \overline{0} = 0_{\mathbb{Z}/6}$ and $\overline{3} \cdot \overline{2} = \overline{6} = \overline{0} = 0_{\mathbb{Z}/6}$ and $\overline{4} \cdot \overline{3} = \overline{12} = \overline{0} = 0_{\mathbb{Z}/6}$. The element $\overline{0}$ is not a zero divisor (since our definition requires a zero divisor to be nonzero). The elements $\overline{1}$ and $\overline{-1}$ are not zero divisors either; indeed, it is easy to see that for any commutative ring R, neither 1_R nor -1_R is a zero divisor.
- If a is an idempotent element of a commutative ring R (see Definition 2.2.1 **(a)**), but equals neither 0 nor 1, then a is a zero divisor, since $a(1-a) = a - \underbrace{a^2}_{=a} = a - a = 0$.

Zero divisors themselves aren't very useful, but their non-existence (in some rings) is:

Definition 2.4.3. Let R be a commutative ring. Assume that $0 \neq 1$ in R. (By this, we mean $0_R \neq 1_R$; that is, the zero and the unity of R are distinct. In other words, we assume that the ring R is not trivial.) We say that R is an **integral domain** if all nonzero $a, b \in R$ satisfy $ab \neq 0$.

Equivalently, a commutative ring R with $0 \neq 1$ (in R, that is) is an integral domain if and only if R has no zero divisors.

Here are some examples:

- The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are integral domains.
- Any subring of an integral domain is clearly an integral domain as well. Thus, e.g., the ring $\mathbb{S}$ from Subsection 2.1.2 (i.e., the subring of $\mathbb{R}$ consisting of the numbers of the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$) is an integral domain.
- The ring $\mathbb{Z}/n$ is an integral domain if and only if n is 0 or a prime or minus a prime. We will prove this later.
- The ring $\mathbb{S}'$ from Subsection 2.1.2 (i.e., the ring whose elements are numbers of the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$, with multiplication $*$ given by $\left(a + b\sqrt{5}\right) * \left(c + d\sqrt{5}\right) = ac + bd\sqrt{5}$) is not an integral domain, since it has $1 * \sqrt{5} = 0$.
- The ring of all functions from $\mathbb{Q}$ to $\mathbb{Q}$ is not an integral domain, since any two functions with disjoint supports will multiply to 0. (For a specific example, we have $\delta_0 \cdot \delta_1 = 0$, where δ_y (for $y \in \mathbb{Q}$) is the function that sends y to 1 and all other rational numbers to 0.)
- We required an integral domain to be commutative in Definition 2.4.3. If we dropped this requirement, then the ring $\mathbb{H}$ of quaternions would be an integral domain, but the matrix ring $\mathbb{R}^{2\times 2}$ would not be.

Exercise 2.4.1. Consider the ring $\mathbb{R}^{2\times 2}$ of all 2×2-matrices with real entries. Define two subsets $\mathcal{P}$ and $\mathcal{M}$ of $\mathbb{R}^{2\times 2}$ by

$$\mathcal{P} := \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \qquad \text{and}$$
$$\mathcal{M} := \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

(a) Show that $\mathcal{P}$ and $\mathcal{M}$ are commutative subrings of $\mathbb{R}^{2\times 2}$.

(b) Prove that $\mathcal{P}$ is not an integral domain.

(c) Prove that $\mathcal{M}$ is a field.

Exercise 2.4.2.

(a) Recall the commutative ring $\mathcal{F}$ from Exercise 2.3.6 **(b)**. Prove that $\mathcal{F}$ is an integral domain.

(b) Let $\mathcal{F}_{\mathbb{Q}}$ be the ring defined just like $\mathcal{F}$, but using $\mathbb{Q}$ instead of $\mathbb{Z}$ (that is, it is the subring $\{aA + bI_2 \mid a, b \in \mathbb{Q}\}$ of $\mathbb{Q}^{2\times 2}$). Is $\mathcal{F}_{\mathbb{Q}}$ an integral domain?

(c) Let $\mathcal{F}_{\mathbb{R}}$ be the ring defined just like $\mathcal{F}$, but using $\mathbb{R}$ instead of $\mathbb{Z}$ (that is, it is the subring $\{aA + bI_2 \mid a, b \in \mathbb{R}\}$ of $\mathbb{R}^{2\times 2}$). Is $\mathcal{F}_{\mathbb{R}}$ an integral domain?

[**Hint:** For part **(a)**, argue that the determinant

$$\det(aA + bI_2) = \det \begin{pmatrix} b & a \\ a & a+b \end{pmatrix} = -a^2 + ab + b^2 = \frac{5b^2 - (2a-b)^2}{4}$$

of any nonzero matrix $aA + bI_2 \in \mathcal{F} \setminus \{0\}$ is nonzero, since $\sqrt{5}$ is irrational. Now recall that $\det(AB) = \det A \cdot \det B$ for any $A, B \in \mathbb{R}^{2\times 2}$.]

Warning 2.4.4. Let R be a commutative ring, and let S be a subring of R. It can happen that some element $a \in S$ is a zero divisor in R (that is, there is a nonzero $b \in R$ such that $ab = 0$) but not a zero divisor in S (that is, there exists no nonzero $b \in S$ such that $ab = 0$). This should not be too surprising (R has more elements than S, so it should be "easier" to find the required b in R than in S), although an explicit example is not easy to construct at this point. (Using the concept of quotient rings we will learn later, we can take $R = \mathbb{Z}[x] / (2x)$ and $S = \mathbb{Z}$ and $a = 2$, where we view S as a subring of R in the "obvious" way by identifying each integer $n \in \mathbb{Z}$ with the corresponding residue class $\overline{n} \in R$.)

2.5. Units and fields ([DumFoo04, §7.1])

2.5.1. Units and inverses

By definition, any ring R has an addition, a subtraction and a multiplication. Division, on the other hand, is not guaranteed: Even the ring $\mathbb{Z}$ doesn't really have division (unless you count division with remainder, which is a different story). However, any ring R has **some** elements that can be divided by; the simplest such element is its unity 1. Let us introduce a name for these elements:

Definition 2.5.1. Let R be a ring.

(a) An element $a \in R$ is said to be a **unit** of R (or **invertible** in R) if there exists a $b \in R$ such that $ab = ba = 1$. In this case, b is unique and is known as the **inverse** (or **multiplicative inverse**, or **reciprocal**) of a, and is denoted by a^{-1}.

(b) We let $R^\times$ denote the set of all units of R.

A few comments:

- It goes without saying that the "1" refers to the unity of the ring R.

- We required $ab = ba = 1$ rather than merely $ab = 1$ because R is not necessarily commutative. When R is commutative, of course, $ab = 1$ suffices.
- Why is b unique in Definition 2.5.1 **(a)**? Because if b_1 and b_2 are two such b's (for the same a), then $ab_1 = b_1 a = 1$ and $ab_2 = b_2 a = 1$, so that $b_1 \underbrace{ab_2}_{=1} = b_1 1 = b_1$ and thus $b_1 = \underbrace{b_1 a}_{=1} b_2 = 1b_2 = b_2$. This is the exact same argument that proves the uniqueness of inverses in a group.
- Don't confuse "unit" (= invertible element) with "unity" (= neutral element for multiplication). The unity is always a unit, but not vice versa!
- Some people write R^* or R^x for $R^\times$.

Here are some examples of units:

- The units of the ring $\mathbb{Q}$ are all nonzero elements of $\mathbb{Q}$. (This is because every nonzero element of $\mathbb{Q}$ has a reciprocal, and this reciprocal again lies in $\mathbb{Q}$.) The same holds for $\mathbb{R}$ and for $\mathbb{C}$.
- The units of the ring $\mathbb{Z}$ are 1 and -1 (with inverses 1 and -1, respectively). No other integer is a unit of $\mathbb{Z}$. For example, 2 has an inverse $\frac{1}{2}$ in $\mathbb{Q}$, but not in $\mathbb{Z}$.
- The units of the matrix ring $\mathbb{R}^{n\times n}$ are the invertible $n \times n$-matrices. You have seen many ways to characterize them in your linear algebra class. You might even remember that the set $\left(\mathbb{R}^{n\times n}\right)^\times$ of these units is known as the **n-th general linear group** of $\mathbb{R}$, and is called $\mathrm{GL}_n(\mathbb{R})$ or $\mathrm{GL}(n, \mathbb{R})$.
- In the ring of all functions from $\mathbb{Q}$ to $\mathbb{Q}$, the units are the functions that never vanish (i.e., that don't take 0 as a value). Inverses can be computed pointwise.
- Recall the ring $\mathbb{Z}[i]$ of Gaussian integers. Its only units are $1, i, -1, -i$. This is Corollary 2.16.7 further below.
- A truly trivial example: The zero of a ring R is a unit if and only if R is a trivial ring.

Our next example we state as a proposition:[21]

[21] Two integers a and b are said to be **coprime** (to each other) if and only if $\gcd(a, b) = 1$. Some authors say "relatively prime" instead of "coprime".

Proposition 2.5.2. Let $n \in \mathbb{Z}$.

(a) The units of the ring $\mathbb{Z}/n$ are precisely the residue classes $\overline{a} \in \mathbb{Z}/n$ where $a \in \mathbb{Z}$ is coprime to n.

(b) Let $a \in \mathbb{Z}$. Then, $\overline{a} \in \mathbb{Z}/n$ is a unit of $\mathbb{Z}/n$ if and only if a is coprime to n.

Proof. We begin by proving part **(b)**, which is the stronger claim. (Part **(a)** will then easily follow.)

(b) This is an "if and only if" statement. We shall prove its "if" (i.e., "$\Longleftarrow$") and "only if" (i.e., "$\Longrightarrow$") parts separately:

$\Longleftarrow$: Assume that $a \in \mathbb{Z}$ is coprime to n. Bezout's theorem[22] tells us that there exist $x, y \in \mathbb{Z}$ with $xa + yn = \gcd(a, n)$. Consider these x, y. We have $xa + yn = \gcd(a, n) = 1$ (since a is coprime to n). Thus, $xa \equiv xa + yn = 1 \bmod n$. Translating this into the language of residue classes, we obtain $\overline{xa} = \overline{1}$ in $\mathbb{Z}/n$. Hence, $\overline{x} \cdot \overline{a} = \overline{xa} = \overline{1}$ in $\mathbb{Z}/n$. Since the ring $\mathbb{Z}/n$ is commutative, this shows that $\overline{a}$ is invertible (with inverse $\overline{x}$). In other words, $\overline{a}$ is a unit of $\mathbb{Z}/n$.

$\Longrightarrow$: Conversely, assume that $\overline{a}$ is a unit of $\mathbb{Z}/n$. Thus, $\overline{a}$ has an inverse $\overline{b} \in \mathbb{Z}/n$. This inverse $\overline{b}$ satisfies $\overline{ab} = \overline{1}$; in other words, $ab \equiv 1 \bmod n$. But this easily yields that[23] $\gcd(ab, n) = \gcd(1, n) = 1$. In other words, ab is coprime to n. Hence, a is coprime to n as well (since any common divisor of a and n must be a common divisor of ab and n).

(a) This follows easily from part **(b)**. □

Here are some examples of Proposition 2.5.2:

- The units of the ring $\mathbb{Z}/12$ are $\overline{1}, \overline{5}, \overline{7}, \overline{11}$ (because among the integers $0, 1, \ldots, 11$, it is the four numbers $1, 5, 7, 11$ that are coprime to 12).
- The units of the ring $\mathbb{Z}/5$ are $\overline{1}, \overline{2}, \overline{3}, \overline{4}$.
- The only unit of the ring $\mathbb{Z}/2$ is $\overline{1}$.

Next, we shall show some general properties of units in rings:

[22] **Bezout's theorem** (from elementary number theory) states that for any two integers a and b, there exist two integers x and y satisfying $xa + yb = \gcd(a, b)$. In other words, the greatest common divisor of two integers a and b can always be written as a linear combination of a and b with integer coefficients.

See, e.g., [Grinbe19, Theorem 2.9.12] for a proof of Bezout's theorem.

[23] We are using the fact that if u and v are two integers satisfying $u \equiv v \bmod n$, then $\gcd(u, n) = \gcd(v, n)$. This is just a restatement of the classical result that the gcd of two integers does not change if we add a multiple of one to the other.

Theorem 2.5.3. Let R be a ring. Then, the set $R^\times$ is a multiplicative group. More precisely: $(R^\times, \cdot, 1)$ is a group.

Proof. It suffices to show the following facts:

1. The unity 1 of R belongs to $R^\times$.
2. If $a, b \in R^\times$, then $ab \in R^\times$.
3. If $a \in R^\times$, then a has an inverse in $R^\times$.

All other group axioms for $R^\times$ follow from the ring axioms of R. So let us prove these three facts.

Proof of Fact 1: Fact 1 is obvious (as 1 has inverse 1).

Proof of Fact 2: Let $a, b \in R^\times$. Thus, the elements a, b are units, and thus have inverses a^{-1}, b^{-1}, respectively. These satisfy $aa^{-1} = a^{-1}a = 1$ and $bb^{-1} = b^{-1}b = 1$. Now, $a \underbrace{bb^{-1}}_{=1} a^{-1} = aa^{-1} = 1$ and $b^{-1} \underbrace{a^{-1}a}_{=1} b = b^{-1}b = 1$, so that ab is invertible as well (with inverse $b^{-1}a^{-1}$). That is, $ab \in R^\times$. This proves Fact 2.

Proof of Fact 3: Let $a \in R^\times$. Thus, a has an inverse a^{-1} in R. This inverse a^{-1}, in turn, has an inverse (namely, a), and thus also lies in $R^\times$. Hence, a has an inverse in $R^\times$. This proves Fact 3. □

The group $R^\times$ from Theorem 2.5.3 is known as the **group of units** of R. Thus, every ring R produces **two** groups: the additive group $(R, +, 0)$ (which contains all elements of R) and the multiplicative group of units $(R^\times, \cdot, 1)$ (which only contains the units). We record two important consequences of our proof of Theorem 2.5.3:

Theorem 2.5.4 (Shoe-sock theorem)**.** Let R be a ring. Let a, b be two units of R. Then, ab is a unit of R, and its inverse is $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. See the proof of Fact 2 in the proof of Theorem 2.5.3. □

Theorem 2.5.5. Let R be a ring. Let a be a unit of R. Then, a^{-1} is a unit of R, and its inverse is $\left(a^{-1}\right)^{-1} = a$.

Proof. See the proof of Fact 3 in the proof of Theorem 2.5.3. □

Clearly, if R is a commutative ring, then its group of units $R^\times$ is abelian. Sometimes, more can be said about it. In particular, we will eventually see (Theorem 7.2.1) that the group $(\mathbb{Z}/n)^\times$ is cyclic whenever n is prime. For other n, it sometimes is and sometimes isn't (see Exercise 7.2.5). Here is a simple example:

Example 2.5.6. As we have seen, the ring $\mathbb{Z}/12$ has 4 units: $\overline{1}, \overline{5}, \overline{7}, \overline{11}$. Thus, the group of units $(\mathbb{Z}/12)^\times$ is $\left\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\right\}$. It is easy to see that each of these units squares to $\overline{1}$ (since $\overline{1}^2 = \overline{5}^2 = \overline{7}^2 = \overline{11}^2 = \overline{1}$); hence, this group is isomorphic to the Klein four-group (a direct product of two cyclic groups of order 2).

Here are a few exercises on units and inverses in some special rings. The first exercise ([21w, homework set #2, Exercise 5 **(a)**]) will come useful later:

Exercise 2.5.1. Let p be a prime. Prove that the only units of the ring $\mathbb{Z}/p$ that are their own inverses (i.e., the only $m \in (\mathbb{Z}/p)^\times$ that satisfy $m^{-1} = m$) are $\overline{1}$ and $\overline{-1}$.

Exercise 2.5.2. Let p be a prime. Let k be a positive integer. Prove that the number of units of the ring $\mathbb{Z}/p^k$ is $p^k - p^{k-1}$.

Exercise 2.5.3. Let R be the ring $(\mathbb{Z}/2)^{2\times 2}$ of all 2×2-matrices with entries in $\mathbb{Z}/2$. This ring has size $2^4 = 16$, since each such matrix has 4 entries and there are 2 options for each entry.

(a) Find the group of units $R^\times$ of this ring.

(b) Prove that this group $R^\times$ is isomorphic to the symmetric group S_3 (that is, the group of all permutations of the set $\{1, 2, 3\}$).

Exercise 2.5.4. Let $\mathbb{D}$ be the ring of dual numbers, as defined in Exercise 2.1.2. Prove the following:

(a) A dual number $a + b\varepsilon$ (with $a, b \in \mathbb{R}$) is a unit of $\mathbb{D}$ if and only if $a \neq 0$.

(b) If $a, b \in \mathbb{R}$ satisfy $a \neq 0$, then the inverse of the dual number $a + b\varepsilon$ is $\dfrac{1}{a} - \dfrac{b}{a^2}\varepsilon$.

Exercise 2.5.5. Recall the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$ from Definition 2.3.4, and recall the matrix A and the commutative ring $\mathcal{F}$ from Exercise 2.3.6 **(b)**.

We extend the Fibonacci sequence $(f_0, f_1, f_2, \ldots)$ to an infinite-in-both-directions "sequence" $(\ldots, f_{-2}, f_{-1}, f_0, f_1, f_2, \ldots)$ by requiring that it satisfy the original recursive equation $f_n = f_{n-1} + f_{n-2}$ for all $n \in \mathbb{Z}$ (not just for $n \geq 2$). Thus, the negatively indexed Fibonacci numbers $f_{-1}, f_{-2}, f_{-3}, \ldots$ are computed recursively by solving this recursive equation $f_n = f_{n-1} + f_{n-2}$ for f_{n-2}. For instance, $f_{-1} = f_1 - f_0 = 1 - 0 = 1$ and $f_{-2} = f_0 - f_{-1} = 0 - 1 = -1$.

(a) Prove that the matrix A is a unit of $\mathcal{F}$ (that is, it has an inverse in $\mathcal{F}$).

(b) Prove that $A^n = f_n A + f_{n-1} I_2$ for all $n \in \mathbb{Z}$.

(c) Prove that $f_{-n} = (-1)^n f_n$ for each $n \in \mathbb{Z}$.

(d) Prove that the units of $\mathcal{F}$ are precisely the powers A^k of the matrix A (with $k \in \mathbb{Z}$). (This includes its positive powers $A^1, A^2, A^3, \ldots$, its negative powers $A^{-1}, A^{-2}, A^{-3}, \ldots$ and its zeroth power $A^0 = I_2$.)

[**Hint:** Part **(d)** is surprisingly tricky! Recall again that $\det(aA + bI_2) = -a^2 + ab + b^2$ for any $a, b \in \mathbb{Z}$. Show that this determinant $\det(aA + bI_2)$ has to be 1 or -1 if $aA + bI_2$ is a unit of $\mathcal{F}$. Thus, we must have $-a^2 + ab + b^2 \in \{1, -1\}$ if $aA + bI_2$ is a unit. But this means that the pair (a, b) is a "golden pair" in the terminology of [Grinbe21, Exercise 5.4.10], and the set of all "golden pairs" can be described explicitly in terms of the Fibonacci sequence [Grinbe21, Exercise 5.4.10].]

Remark 2.5.7. Let R be a ring, and let S be a subring of R. Then, any unit u of S is also a unit of R (since its inverse belongs to S and therefore to R, and thus u has an inverse in R). This is in stark contrast to the situation for non-zero-divisors (which we discussed in Warning 2.4.4).

2.5.2. Some exercises on inverses

The following exercises prove surprising results and make for good practice with the definition of an inverse[24]:

Exercise 2.5.6. Let R be a ring. Let a and b be two elements of R.

Prove that if $1 - ab$ is invertible, then so is $1 - ba$.

Better yet, prove the following: If c is an inverse of $1 - ab$, then $1 + bca$ is an inverse of $1 - ba$.

Note that Exercise 2.5.6 yields a well-known result in functional analysis (see `https://math.stackexchange.com/questions/79217`).

Exercise 2.5.7. Let R be a ring. Let a and b be two units of R such that $a + b$ is a unit as well.

(a) Prove that $a^{-1} + b^{-1}$, too, is a unit, and its inverse is

$$\left(a^{-1} + b^{-1}\right)^{-1} = a \cdot (a + b)^{-1} \cdot b = b \cdot (a + b)^{-1} \cdot a.$$

(b) Show on an example that $\left(a^{-1} + b^{-1}\right)^{-1}$ can be different from $ab \cdot (a + b)^{-1}$.

Let us next define some weaker variants of inverses:

Definition 2.5.8. Let R be a ring. Let a be an element of R.

(a) A **left inverse** of a shall mean an element $b \in R$ satisfying $ba = 1$.

(b) A **right inverse** of a shall mean an element $b \in R$ satisfying $ab = 1$.

[24] Keep in mind that a ring is not always commutative!

Thus, an inverse of a is the same as a left inverse of a that simultaneously is a right inverse of a. It is clear that the notions of "left inverse" and "right inverse" can be defined in any monoid, not just in a ring, since they rely only on the multiplication and the unity. As already mentioned, a left or right inverse doesn't have to be a (proper) inverse in general, although it is hard to find examples where it isn't. The following exercise (a result of Jacobson) might give a hint as to why:

Exercise 2.5.8. Let R be a ring. Let a and b be two elements of R such that $ab = 1$ but $ba \neq 1$. Let $w = 1 - ba$.

(a) Prove that $aw = wb = 0$.

(b) Conclude that $a\left(b + wa^k\right) = 1$ for all $k \in \mathbb{N}$.

(c) Prove that the elements $b + wa^k$ for all $k \in \mathbb{N}$ are distinct.

(d) Conclude that a has infinitely many right inverses.

(e) Conclude that R cannot be finite.

[**Hint:** The only hard part here is **(c)**. Show first that $wa^i \neq 0$ for all $i \in \mathbb{N}$; then show that $wa^i \neq w$ for all positive integers i.]

The next exercise ([21w, homework set #2, Exercise 1]) provides another source of units in certain rings:

Exercise 2.5.9. Let R be a ring. An element $a \in R$ will be called **nilpotent** if there exists some $n \in \mathbb{N}$ such that $a^n = 0$. (For instance, the element $\overline{18} \in \mathbb{Z}/24$ is nilpotent, since $\overline{18}^3 = \overline{0}$. Note that the zero 0 is nilpotent in any ring, but other nilpotent elements may or may not exist. For another example, the element $\varepsilon \in \mathbb{D}$ in Exercise 2.1.2 is nilpotent.)

Let $a \in R$ be a nilpotent element.

(a) Prove that $1 - a \in R$ is a unit.

(b) Let $u \in R$ be a unit satisfying $ua = au$. Prove that $u - a \in R$ is a unit.

[**Hint:** Treat the geometric series $\dfrac{1}{1-x} = 1 + x + x^2 + \cdots$ as an inspiration, noting that the infinite sum on the right hand side will become a finite sum if the nilpotent element a is substituted for x.]

2.5.3. Fields

As we saw, some rings (such as $\mathbb{Z}$) have few units, while other rings (such as $\mathbb{Q}$) have many. The rings with the most units are the "fields":

Definition 2.5.9. Let R be a commutative ring. Assume that $0 \neq 1$ in R. We say that R is a **field** if every nonzero element of R is a unit.

Examples:

- The rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields. The ring $\mathbb{Z}$ is not (since 2 is not a unit).
- The ring $\mathbb{S}$ of all real numbers of the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$ (as defined in Subsection 2.1.2) is a field. Indeed, the inverse of a nonzero element $a + b\sqrt{5}$ is

$$\left(a + b\sqrt{5}\right)^{-1} = \frac{1}{a + b\sqrt{5}} = \frac{a - b\sqrt{5}}{a^2 - b^2 \cdot 5} = \frac{a}{a^2 - 5b^2} + \frac{-b}{a^2 - 5b^2}\sqrt{5}$$

  (the denominators here are nonzero because $a + b\sqrt{5} \neq 0$ entails $a^2 - 5b^2 \neq 0$). So this is why they taught you rationalizing denominators in high school!
- The Hamiltonian quaternions $\mathbb{H}$ are not a field, but for a stupid reason: they are noncommutative. Otherwise, they would be a field. A noncommutative ring in which each nonzero element is invertible is called a **division ring** or **skew-field**.
- Let n be a positive integer. The ring $\mathbb{Z}/n$ is a field if and only if n is prime. (We will prove this below.)
- The ring F_4 constructed in Subsection 2.1.2 as well as the ring F_8 defined in Exercise 2.1.1 are fields.

2.6. Fields and integral domains: some connections ([DumFoo04, §7.1])

2.6.1. Fields vs. integral domains

The notions of fields and integral domains are closely related:

Proposition 2.6.1.

(a) Every field is an integral domain.

(b) Every **finite** integral domain is a field. (Here, of course, "finite" means "finite as a set".)

Proof. **(a)** Let F be a field. We must show that F is an integral domain.

Let $a, b \in F$ be nonzero. We must show that ab is nonzero.

Indeed, a and b are nonzero, and thus are units (since F is a field). Thus, they have inverses a^{-1} and b^{-1}.

Now, if we had $ab = 0$, then we would have $\underbrace{ab}_{=0} b^{-1}a^{-1} = 0$, which would yield $0 = a\underbrace{bb^{-1}}_{=1}a^{-1} = aa^{-1} = 1$, which would contradict the fact that $0 \neq 1$ in F (since F is a field). Thus, we cannot have $ab = 0$. In other words, ab is nonzero. This proves that F is an integral domain. Thus, Proposition 2.6.1 **(a)** is proved.

(b) Let R be a **finite** integral domain. We must show that R is a field.

Let $a \in R$ be nonzero. We must show that a is a unit.

Since R is an integral domain, we know that $ab \neq 0$ for any $b \neq 0$. Thus, $ax \neq ay$ for any two distinct elements x and y of R (because if x and y are two distinct elements of R, then $x - y \neq 0$, and thus the previous sentence yields $a(x-y) \neq 0$; but this rewrites as $ax - ay \neq 0$, so that $ax \neq ay$). In other words, the map

$$R \to R, \qquad x \mapsto ax$$

is injective. Hence, this map is also bijective (since any injective map between two **finite** sets of the **same size** is bijective – this is one of the Pigeonhole Principles[25]). Thus, in particular, this map is surjective, and hence takes 1 as a value. In other words, there exists an $x \in R$ such that $ax = 1$. Since R is commutative, this x must be an inverse of a, and thus we conclude that a is a unit. This finishes the proof of Proposition 2.6.1 **(b)**. □

Without the word "finite", Proposition 2.6.1 **(b)** would not be true; for instance, $\mathbb{Z}$ is an integral domain but no field. The polynomial ring $\mathbb{R}[x]$ (consisting of univariate polynomials with real coefficients) is another example of an integral domain that is not a field. (We will prove this later.)

2.6.2. When is $\mathbb{Z}/n$ a field?

Our above study of units of $\mathbb{Z}/n$ lets us now easily obtain the following:

Corollary 2.6.2. Let n be a positive integer. Then, the following chain of equivalences holds:

$$(\mathbb{Z}/n \text{ is an integral domain}) \iff (\mathbb{Z}/n \text{ is a field}) \iff (n \text{ is prime}).$$

Proof. The first of the two $\iff$ signs follows from Proposition 2.6.1 (since $\mathbb{Z}/n$ is finite). Let's now prove the second.

[25] To be specific, this is what I call the "Pigeonhole Principle for Injections". See [Grinbe21, Theorem 6.1.3], for example.

$\Longrightarrow$: Assume that $\mathbb{Z}/n$ is a field. Then, every nonzero element of $\mathbb{Z}/n$ is a unit. Hence, the $n-1$ residue classes $\overline{1}, \overline{2}, \ldots, \overline{n-1}$ are units of $\mathbb{Z}/n$ (since they are nonzero). Therefore, the $n-1$ integers $1, 2, \ldots, n-1$ are coprime to n (by Proposition 2.5.2 **(b)**). Hence, n is either 1 or prime. However, if n was 1, then we would have $\overline{0} = \overline{1}$, which would mean that $0 = 1$ in $\mathbb{Z}/n$; but this is forbidden for a field. Thus, n cannot be 1, and therefore must be prime.

$\Longleftarrow$: Assume that n is prime. Then, $n > 1$, so that $\overline{0} \neq \overline{1}$. That is, $0 \neq 1$ in $\mathbb{Z}/n$. Furthermore, if $\overline{a}$ (for some integer a) is a nonzero element of $\mathbb{Z}/n$, then the integer a is not divisible by n (since $\overline{a}$ is nonzero), so that a is coprime to n (since n is prime), and this entails (by Proposition 2.5.2 **(b)**) that $\overline{a}$ is a unit of $\mathbb{Z}/n$. So we have shown that every nonzero element of $\mathbb{Z}/n$ is a unit. In other words, $\mathbb{Z}/n$ is a field. □

Note that the positivity of n in Corollary 2.6.2 is important: The ring $\mathbb{Z}/0$ is an integral domain but not a field. (In fact, this ring is essentially $\mathbb{Z}$, except that its elements are the singleton sets $\{a\}$ instead of the integers a themselves.)

2.6.3. Application: Fermat's Little Theorem

We can use Corollary 2.6.2 to obtain an important result in elementary number theory:

Theorem 2.6.3 (Fermat's little theorem, short FℓT)**.** Let p be a prime number. Let $a \in \mathbb{Z}$. Then, $a^p \equiv a \bmod p$.

For example, $a^3 \equiv a \bmod 3$ and $a^5 \equiv a \bmod 5$ for every $a \in \mathbb{Z}$.

Before we prove Theorem 2.6.3, let us first show the following property of the field $\mathbb{Z}/p$:

Proposition 2.6.4 (Fermat's little theorem in $\mathbb{Z}/p$ form)**.** Let p be a prime number. Let $u \in \mathbb{Z}/p$. Then, $u^p = u$.

Proof of Proposition 2.6.4. We know that p is prime. Thus, Corollary 2.6.2 (applied to $n = p$) yields that $\mathbb{Z}/p$ is a field. Hence, every nonzero element of $\mathbb{Z}/p$ is a unit.

We must prove that $u^p = u$. If $u = 0$, then this is obvious (since $u^p = 0^p = 0 = u$ in this case). So let us WLOG assume that $u \neq 0$. Hence, the element $u \in \mathbb{Z}/p$ is nonzero. Therefore, u is a unit of the ring $\mathbb{Z}/p$ (since every nonzero element of $\mathbb{Z}/p$ is a unit). In other words, $u \in (\mathbb{Z}/p)^\times$.

However, the units of the ring $\mathbb{Z}/p$ are $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ (again because every nonzero element of $\mathbb{Z}/p$ is a unit). Thus, in particular, there are $p-1$ of them. This shows that the group $(\mathbb{Z}/p)^\times$ has order $p-1$. Hence, Lagrange's theorem (from group theory)[26] shows that $g^{p-1} = 1$ for each $g \in (\mathbb{Z}/p)^\times$. Applying this

[26] Recall that this theorem says the following: If G is a finite group of order m (for some $m \in \mathbb{N}$), then $g^m = 1$ for each $g \in G$ (where we are writing G multiplicatively, so that 1 denotes the neutral element of G).

to $g = u$, we obtain $u^{p-1} = 1$. Hence, $u^p = u \underbrace{u^{p-1}}_{=1} = u$. This proves Proposition 2.6.4. $\square$

We can now easily derive Theorem 2.6.3 from Proposition 2.6.4:

Proof of Theorem 2.6.3. Consider the residue class $\overline{a} \in \mathbb{Z}/p$. Applying Proposition 2.6.4 to $u = \overline{a}$, we obtain $\overline{a}^p = \overline{a}$. Thus, $\overline{a^p} = \overline{a}^p = \overline{a}$. In other words, $a^p \equiv a \bmod p$. Theorem 2.6.3 is thus proven. $\square$

We also observe:

Corollary 2.6.5 (Fermat's little theorem in the non-divisible case)**.** Let p be a prime number. Let $a \in \mathbb{Z}$ satisfy $p \nmid a$. Then, $a^{p-1} \equiv 1 \bmod p$.

Proof. Consider the residue class $\overline{a} \in \mathbb{Z}/p$. Applying Proposition 2.6.4 to $u = \overline{a}$, we obtain $\overline{a}^p = \overline{a}$. However, from $p \nmid a$, we obtain $\overline{a} \neq \overline{0}$. In other words, $\overline{a}$ is nonzero. Since $\mathbb{Z}/p$ is a field (by Corollary 2.6.2), we know that every nonzero element of $\mathbb{Z}/p$ is a unit. Thus, $\overline{a}$ is a unit (since $\overline{a}$ is nonzero). Hence, we can divide both sides of the equality $\overline{a}^p = \overline{a}$ by $\overline{a}$. As a result, we obtain $\overline{a}^{p-1} = \overline{1}$. In other words, $\overline{a^{p-1}} = \overline{1}$. In other words, $a^{p-1} \equiv 1 \bmod p$. This proves Corollary 2.6.5. $\square$

The following proposition generalizes Proposition 2.6.4 to arbitrary finite fields:[27]

Proposition 2.6.6. Let F be a finite field (i.e., a field with finitely many elements). Let $u \in F$. Then, $u^{|F|} = u$.

Proof. If $u = 0$, then this is obvious (since $u^{|F|} = 0^{|F|} = 0 = u$ in this case). So let us WLOG assume that $u \neq 0$. Hence, $u \in F \setminus \{0\}$.

However, F is a field, so that every nonzero element of F is a unit. In other words, $F \setminus \{0\} \subseteq F^\times$. Conversely, $F^\times \subseteq F \setminus \{0\}$, since 0 is not a unit of F (because if 0 were a unit, then $0 \cdot 0^{-1}$ would be 1, which contradicts the axiom $0a = 0$ for all $a \in F$). Combining these two inclusions, we find $F \setminus \{0\} = F^\times$. Hence, $|F \setminus \{0\}| = |F^\times|$, so that $|F^\times| = |F \setminus \{0\}| = |F| - 1$.

In other words, the group $F^\times$ has order $|F| - 1$. Hence, Lagrange's theorem (from group theory) shows that $g^{|F|-1} = 1$ for each $g \in F^\times$. Applying this to $g = u$, we obtain $u^{|F|-1} = 1$ (since $u \in F \setminus \{0\} = F^\times$). Hence, $u^p = u \underbrace{u^{p-1}}_{=1} = u$. This proves Proposition 2.6.6. $\square$

[27] Recall that $\mathbb{Z}/p$ is a finite field of size p whenever p is a prime. Moreover, the rings F_4 and F_8 are finite fields of sizes 4 and 8, respectively. We will see more finite fields in later chapters.

We note in passing that the converse of Fermat's little theorem does not hold in general: There are some non-prime positive integers $p > 1$ such that all $a \in \mathbb{Z}$ satisfy $a^p \equiv a \bmod p$. These integers p are called **Carmichael numbers**, and the smallest of them is 561.

Exercise 2.6.1. Actually prove that 561 is a Carmichael number, i.e., that every $a \in \mathbb{Z}$ satisfies $a^{561} \equiv a \bmod 561$.

[**Hint:** This is not as laborious as it sounds! It is not necessary to try all 561 elements of $\mathbb{Z}/561$. Instead, use the prime factorization $561 = 3 \cdot 11 \cdot 17$.]

2.6.4. Division in a commutative ring

Back to the general case. Rings have addition, subtraction and multiplication; but we can also divide two elements of a ring, as long as the denominator (i.e., the element we are dividing by) is a unit. If the ring is noncommutative, this is somewhat complicated by the fact that there are two kinds of division ("left" and "right" division); however, for commutative rings, it is as simple as for numbers:

Definition 2.6.7. Let R be a commutative ring. Let $a \in R$ and $b \in R^\times$. Then, $\dfrac{a}{b}$ means the element $ab^{-1} = b^{-1}a \in R$. This element is also written a/b, and is called the **quotient** of a by b. The operation $(a, b) \mapsto a/b$ is called **division**.

In particular, in a field, we can divide by any nonzero element.
Division satisfies the rules you would expect:

Proposition 2.6.8. Let R be a commutative ring. Then:

(a) For any $a, c \in R$ and $b, d \in R^\times$, we have

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \tag{4}$$

and

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{5}$$

(b) For any $a \in R$ and $b, c, d \in R^\times$, we have

$$\frac{a}{b} \Big/ \frac{c}{d} = \frac{ad}{bc}.$$

(c) Division undoes multiplication: Three elements $a \in R$, $b \in R^\times$ and $c \in R$ satisfy

$$\frac{a}{b} = c \qquad \text{if and only if} \qquad a = bc. \tag{6}$$

Exercise 2.6.2. Prove Proposition 2.6.8.

Exercise 2.6.3. Let p be a prime such that $p > 3$. Prove that $2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \bmod p$.

[**Hint:** First, show that $u^{p-2} = \dfrac{1}{u}$ for every nonzero $u \in \mathbb{Z}/p$. Then, recall (4).]

2.7. Ring morphisms ([DumFoo04, §7.3])

2.7.1. Definition and examples

Groups have group homomorphisms; vector spaces have vector space homomorphisms (= linear maps); topological spaces have topological space homomorphisms (= continuous maps). No wonder that an analogous concept exists for rings:[28]

Definition 2.7.1. Let R and S be two rings.

(a) A **ring homomorphism** (or, for short, **ring morphism**, or, more informally, **ring map**) from R to S means a map $f : R \to S$ that

- **respects addition** (i.e., satisfies $f(a+b) = f(a) + f(b)$ for all $a, b \in R$);
- **respects multiplication** (i.e., satisfies $f(ab) = f(a) \cdot f(b)$ for all $a, b \in R$);
- **respects the zero** (i.e., satisfies $f(0_R) = 0_S$);
- **respects the unity** (i.e., satisfies $f(1_R) = 1_S$).

(b) A **ring isomorphism** (or, informally, **ring iso**) from R to S means an invertible ring morphism $f : R \to S$ whose inverse $f^{-1} : S \to R$ is also a ring morphism.

(c) The rings R and S are said to be **isomorphic** (this is written $R \cong S$) if there exists a ring isomorphism from R to S.

Here are some examples:

- Let $n \in \mathbb{Z}$. The map

$$\pi : \mathbb{Z} \to \mathbb{Z}/n,$$
$$a \mapsto \overline{a}$$

[28] We follow the modern convention of abbreviating the word "homomorphism" as "morphism". Thus, for example, a "group morphism" is the same as a group homomorphism.

that sends each integer a to its residue class $\overline{a} = a + n\mathbb{Z}$ is a ring morphism, because any $a, b \in \mathbb{Z}$ satisfy the equalities

$$\overline{a+b} = \overline{a} + \overline{b}, \qquad \overline{a \cdot b} = \overline{a} \cdot \overline{b}, \qquad \overline{0} = 0_{\mathbb{Z}/n}, \qquad \overline{1} = 1_{\mathbb{Z}/n}.$$

(These equalities directly follow from the definition of the ring structure on $\mathbb{Z}/n$.)

- The map $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto 2a$ is **not** a ring morphism. It respects addition and the zero, but not multiplication and the unity.
- The map $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto 0$ is **not** a ring morphism. It respects addition, multiplication and the zero, but not the unity.
- However, if T is the zero ring (i.e., the 1-element ring $\{0\}$), then the map $\mathbb{Z} \to T$, $a \mapsto 0$ is a ring morphism. Comparing this example with the preceding one, we see that the ring structure (even a trivial-looking part like the unity) matters to whether a given map is a ring morphism or not.
- The map $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto a^2$ is **not** a ring morphism. It respects multiplication, the zero and the unity, but not addition (since $(a+b)^2$ is usually not the same as $a^2 + b^2$).
- Let S be a subring of a ring R. Let $i : S \to R$ be the **canonical inclusion**; this is simply the map that sends each $a \in S$ to itself. (You can view it as the restriction of the identity map $\mathrm{id}_R : R \to R$ to S.) Then, i is a ring morphism. Indeed, it respects multiplication because the multiplication of S is inherited from R (so that any $a, b \in S$ satisfy $i(ab) = \underbrace{a}_{=i(a)} \underbrace{b}_{=i(b)} = i(a)\, i(b)$); for similar reasons, it satisfies the other axioms in the definition of a ring morphism.
- Consider the map

$$\begin{aligned} f : \mathbb{C} &\to \mathbb{R}^{2\times 2}, \\ a + bi &\mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \text{(for } a, b \in \mathbb{R}\text{)}. \end{aligned}$$

This map f is a ring morphism. Indeed, it is easy to see that it respects addition, the zero and the unity. To see that it respects multiplication, you need to check that $f(zw) = f(z) \cdot f(w)$ for any $z, w \in \mathbb{C}$. But this is straightforward: Write $z = a + bi$ and $w = c + di$ and multiply out[29].

This can also be proved using linear algebra: The $\mathbb{R}$-vector space $\mathbb{C}$ has basis $(1, i)$. If $z \in \mathbb{C}$, then $f(z)$ is the 2×2-matrix that represents the

[29] In more detail: Writing $z = a + bi$ and $w = c + di$, we have $zw = (a+bi)(c+di) =$

"multiply by z" operator (i.e., the map $\mathbb{C} \to \mathbb{C}$, $u \mapsto zu$) in this basis. Since the "multiply by zw" operator is the composition of the "multiply by z" operator with the "multiply by w" operator, it thus follows that $f(zw) = f(z) \cdot f(w)$ (because composition of linear maps corresponds to multiplication of their representing matrices).

Note that the image of the map f is precisely the ring $\mathcal{M}$ defined in Exercise 2.4.1.

The ring morphism f is injective, and therefore you can use the matrix $f(z) \in \mathbb{R}^{2\times 2}$ as a "stand-in" for any complex number $z \in \mathbb{C}$. Complex numbers can thus be "represented" by 2×2-matrices with real entries. In particular, if you believe that the complex numbers are a work of the devil[30], then you can "exorcise" them out of your mathematical work by replacing every complex number z with the corresponding 2×2-matrix $f(z)$. Since f is injective, this replacement does not cause any information to be lost. Furthermore, since f is a ring morphism, addition and multiplication of complex numbers are reflected perfectly in the addition and the multiplication of 2×2-matrices, so that any calculation involving complex numbers $z, w, u, \ldots$ can be immediately reproduced with the corresponding matrices $f(z), f(w), f(u), \ldots$ instead. Only the commutativity of multiplication is less clear when you work with matrices: Two arbitrary 2×2-matrices don't usually commute, but of course two 2×2-matrices that are values of f always commute.

- Just like the ring morphism $f : \mathbb{C} \to \mathbb{R}^{2\times 2}$ can be used to represent complex numbers as 2×2-matrices with real entries, there is another ring morphism $g : \mathbb{H} \to \mathbb{R}^{4\times 4}$ that helps represent Hamilton quaternions as

---

$(ac - bd) + (ad + bc)\, i$ and thus

$$f(zw) = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}.$$

However,

$$f(z) \cdot f(w) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}.$$

Comparing these two equalities yields $f(zw) = f(z) \cdot f(w)$.

[30] Historically, mistrust of complex numbers was widespread centuries after they had been first introduced. This mistrust was eventually overcome once Hamilton defined them rigorously as pairs of real numbers (defining $a + bi$ as the pair (a, b)).

4×4-matrices with real entries. This morphism is

$$g : \mathbb{H} \to \mathbb{R}^{4\times 4},$$
$$a + bi + cj + dk \mapsto \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}.$$

Proving that this is a ring morphism is a tedious but doable exercise in calculation.

- The map $\mathbb{R}^{2\times 2} \to \mathbb{R}$, $A \mapsto \det A$ is **not** a ring morphism. It respects multiplication[31] but not addition.
- The map $\mathbb{C} \to \mathbb{C}$ that sends each complex number $z = a + bi$ (with $a, b \in \mathbb{R}$) to its complex conjugate $\overline{z} = a - bi$ is a ring isomorphism.
- Let R be a ring. Let S be any set. Let R^S be the ring of all functions from S to R (with pointwise addition and multiplication). Fix any $s \in S$. Then, the map

$$R^S \to R,$$
$$f \mapsto f(s)$$

is a ring morphism.[32] This map is known as the **evaluation morphism** at s, since all it does is evaluating a function at the constant s.

Time for another warning:

Warning 2.7.2. Our Definition 2.7.1 **(a)** again differs from [DumFoo04] in how it treats unities. Namely, [DumFoo04] does not require a ring morphism to respect the unity. Thus, the map $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto 0$ is a ring morphism according to [DumFoo04], but not according to us.

[31] This is a particular case of the famous formula

$$\det(AB) = \det A \cdot \det B$$

whenever $A, B \in R^{n\times n}$ are any two $n \times n$-matrices with entries in any commutative ring R.

[32] This is just a roundabout way of saying that any maps $g, h \in R^S$ satisfy

$$(g + h)(s) = g(s) + h(s);$$
$$(gh)(s) = g(s) \cdot h(s);$$
$$0(s) = 0;$$
$$1(s) = 1.$$

But these equalities follow from our definition of the ring structure on R^S (namely: addition is pointwise; multiplication is pointwise; the zero is the constant-0 function; the unity is the constant-1 function).

Exercise 2.7.1. Define A and $\mathcal{F}$ as in Exercise 2.3.6.

Let $\omega : \mathcal{F} \to \mathcal{F}$ be the map that sends each $aA + bI_2$ (with $a, b \in \mathbb{Z}$) to $-aA + (a+b)\, I_2$. (This is well-defined, since each element of $\mathcal{F}$ can be **uniquely** written as $aA + bI_2$ with $a, b \in \mathbb{Z}$.)

(a) Prove that ω is a ring morphism.

(b) Prove that $\omega \circ \omega = \mathrm{id}$.

(c) Conclude that ω is a ring isomorphism.

Exercise 2.7.2.

(a) Is the map

$$\begin{aligned} \mathbb{Z}^{2\times 2} &\to \mathbb{Z}^{2\times 2}, \\ A &\mapsto A^T \end{aligned}$$

(which sends each 2×2-matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to its transpose $A^T = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$) a ring morphism?

(b) Is the map

$$\begin{aligned} \mathbb{Z}^{2\times 2} &\to \mathbb{Z}^{2\times 2}, \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} &\mapsto \begin{pmatrix} d & c \\ b & a \end{pmatrix} \end{aligned}$$

a ring morphism?

Exercise 2.7.3. Let R be any ring, and let u be any unit of R. Consider the map

$$\begin{aligned} f : R &\to R, \\ a &\mapsto uau^{-1}. \end{aligned}$$

Prove that this map f is a ring isomorphism. (This map f is called **conjugation by** u. Despite its name, it has nothing to do with conjugation of complex numbers.)

Exercise 2.7.4. Let R be any ring, and let $n \in \mathbb{N}$. Recall that $R^{n\leq n}$ is the subring of $R^{n\times n}$ consisting of the upper-triangular matrices.

Consider the map

$$\delta : R^{n\times n} \to R^{n\times n},$$
$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \mapsto \begin{pmatrix} a_{1,1} & 0 & \cdots & 0 \\ 0 & a_{2,2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_{n,n} \end{pmatrix},$$

which replaces all off-diagonal entries of a matrix by 0 (but keeps the diagonal entries unchanged).

(a) Is this map δ a ring morphism?

(b) Now, consider the restriction $\delta\mid_{R^{n\leq n}}$ of the map δ to the subring $R^{n\leq n}$. Is this restriction $\delta\mid_{R^{n\leq n}}$ a ring morphism?

Exercise 2.7.5. Let R be any ring, and let $n \in \mathbb{N}$. For any $n \times n$-matrix $A \in R^{n\times n}$, we consider the "block-diagonal" matrix $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} \in R^{2n\times 2n}$, which is obtained by arranging two copies of A and two zero matrices in the form suggested by the notation (for example, if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then $\begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix} = \begin{pmatrix} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & a & b \\ 0 & 0 & c & d \end{pmatrix}$). (See, e.g., the Wikipedia for more details about block matrices.)

(a) Prove that the map

$$R^{n\times n} \to R^{2n\times 2n},$$
$$A \mapsto \begin{pmatrix} A & 0 \\ 0 & A \end{pmatrix}$$

is an injective ring morphism.

(b) Generalize this to find an injective ring morphism from $R^{n\times n}$ to $R^{kn\times kn}$ for every positive integer k.

The following exercise ([21w, homework set #2, Exercise 2]) assigns to each ring R a "mirror version" (called the **opposite ring** of R, and denoted by R^{op}). In general, this mirror version is not isomorphic to R, but often enough it is.

Exercise 2.7.6. Let R be a ring. We define a new binary operation $\widetilde{\cdot}$ on R by setting

$$a \mathbin{\widetilde{\cdot}} b = ba \qquad \text{for all } a, b \in R.$$

(Thus, $\widetilde{\cdot}$ is the multiplication of R, but with the two arguments switched.)

(a) Prove that the set R, equipped with the addition $+$, the multiplication $\widetilde{\cdot}$, the zero 0_R and the unity 1_R, is a ring.

This new ring is called the **opposite ring** of R, and is denoted by R^{op}.

Note that the **sets** R and R^{op} are identical (so a map from R to R is the same as a map from R to R^{op}); but the **rings** R and R^{op} are generally not the same (so a ring morphism from R to R is not the same as a ring morphism from R to R^{op}).

(b) Prove that the identity map $\mathrm{id} : R \to R$ is a ring isomorphism from R to R^{op} if and only if R is commutative.

(c) Now, assume that R is the matrix ring $S^{n\times n}$ for some commutative ring S and some $n \in \mathbb{N}$. Prove that the map

$$R \to R^{\mathrm{op}}, \qquad A \mapsto A^T$$

(where A^T, as usual, denotes the transpose of a matrix A) is a ring isomorphism.

Exercise 2.7.7. Let $\mathbb{H}$ be the ring of Hamilton quaternions.

(a) Prove that the map

$$\begin{aligned} \mathbb{H} &\to \mathbb{H}^{\mathrm{op}}, \\ a + bi + cj + dk &\mapsto a + bi + dj + ck \qquad (\text{for } a,b,c,d \in \mathbb{R}) \end{aligned}$$

is a ring isomorphism.

(b) Prove that the map

$$\begin{aligned} \mathbb{H} &\to \mathbb{H}^{\mathrm{op}}, \\ a + bi + cj + dk &\mapsto a - bi - cj - dk \qquad (\text{for } a,b,c,d \in \mathbb{R}) \end{aligned}$$

is a ring isomorphism as well.

The last two exercises might suggest that every ring R is somehow isomorphic to its opposite ring R^{op}. This is not the case, but a counterexample is tricky to find; one such counterexample is constructed in Exercise 2.7.10.

2.7.2. Basic properties of ring morphisms

Let us show some basic properties of ring morphisms. We start with the fact that a composition of two ring morphisms is again a ring morphism:

Proposition 2.7.3. Let R, S and T be three rings. Let $f : S \to T$ and $g : R \to S$ be two ring morphisms. Then, $f \circ g : R \to T$ is a ring morphism.

Proof. This is proved in the same way as the analogous result about groups. □

The next proposition shows that the "respects the zero" condition in the definition of a ring morphism is redundant (even though the "respects the unity" condition is not):

Proposition 2.7.4. Let R and S be two rings. Let $f : R \to S$ be a map that respects addition. Then, f automatically respects the zero.

Proof. Since f respects addition, we have $f(0_R + 0_R) = f(0_R) + f(0_R)$. Rewrite this as $f(0_R) = f(0_R) + f(0_R)$ (since $0_R + 0_R = 0_R$). Now, subtract $f(0_R)$ from both sides to get $0_S = f(0_R)$. In other words, f respects the zero. □

Note that we can restate our definition of a ring morphism as follows:

> A *ring morphism* is a map $f : R \to S$ between two rings R and S that is a group homomorphism from the additive group $(R, +, 0)$ to the additive group $(S, +, 0)$ and simultaneously a monoid homomorphism from the multiplicative monoid $(R, \cdot, 1)$ to the multiplicative group $(S, \cdot, 1)$.

It is easy to see that ring morphisms respect all sorts of operations constructed from $+$, $\cdot$, 0 and 1:

Proposition 2.7.5. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then:

(a) The map f respects finite sums; i.e., we have $f(a_1 + a_2 + \cdots + a_n) = f(a_1) + f(a_2) + \cdots + f(a_n)$ for any $a_1, a_2, \ldots, a_n \in R$.

(b) The map f respects finite products; i.e., we have $f(a_1 a_2 \cdots a_n) = f(a_1) \cdot f(a_2) \cdot \cdots \cdot f(a_n)$ for any $a_1, a_2, \ldots, a_n \in R$.

(c) The map f respects differences; i.e., we have $f(a - b) = f(a) - f(b)$ for any $a, b \in R$.

(d) The map f respects inverses; i.e., if a is a unit of R, then $f(a)$ is a unit of S, with inverse $(f(a))^{-1} = f\left(a^{-1}\right)$.

(e) The map f respects integer multiples; i.e., if $a \in R$ and $n \in \mathbb{Z}$, then $f(na) = nf(a)$.

(f) The map f respects powers; i.e., if $a \in R$ and $n \in \mathbb{N}$, then $f(a^n) = (f(a))^n$.

Proof. This is pretty straightforward, and you have probably seen the idea in group theory already. Details LTTR[33]. □

2.7.3. The image of a ring morphism

Recall that the **image** of a map $f : R \to S$ is defined to be the set $f(R) = \{f(r) \mid r \in R\}$; it is often denoted $\operatorname{Im} f$. This makes sense for arbitrary maps f between arbitrary sets R and S, not just for ring morphisms between rings. However, the image of a ring morphism has a special property:

Proposition 2.7.6. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then, $\operatorname{Im} f = f(R)$ is a subring of S.

Proof. Just check the axioms for a subring. For example, let us show that $f(R)$ is closed under multiplication:

Let $x, y \in f(R)$. We must show that $xy \in f(R)$. Since $x \in f(R)$, there exists some $a \in R$ such that $x = f(a)$. Similarly, there exists some $b \in R$ such that $y = f(b)$. Consider these a and b. From $x = f(a)$ and $y = f(b)$, we obtain

$$\begin{aligned} xy &= f(a) \cdot f(b) = f(ab) \qquad \text{(since } f \text{ respects multiplication)} \\ &\in f(R). \end{aligned}$$

This completes the proof that $f(R)$ is closed under multiplication. The other ring axioms can be verified similarly. Thus, we conclude that $f(R)$ is a subring of S. Proposition 2.7.6 is proved. □

Exercise 2.7.8.

(a) Let R and S be two rings. Let $f : R \to S$ and $g : R \to S$ be two ring morphisms. Let $\operatorname{Eq}(f, g)$ be the subset

$$\{r \in R \mid f(r) = g(r)\}$$

of R. This subset is called the **equalizer** of f and g. Prove that this subset $\operatorname{Eq}(f, g)$ is a subring of R.

(b) Let $\omega : \mathbb{C} \to \mathbb{C}$ be the map sending each complex number $z = a + bi$ to its complex conjugate $\overline{z} = a - bi$. (Recall that this is a ring morphism.) Prove that the equalizer $\operatorname{Eq}(\mathrm{id}_{\mathbb{C}}, \omega)$ is $\mathbb{R}$.

(c) Find a specific example where the equalizer subring $\operatorname{Eq}(f, g)$ is interesting (i.e., ideally a ring you have not seen before).

[33] "LTTR" means "left to the reader".

[**Hint:** There are many good examples for part **(c)**. For instance, using the notation $R^{n\leq n}$ from Subsection 2.3.2, consider the two ring morphisms

$$f : \mathbb{Q}^{3\leq 3} \to \mathbb{Q}^{2\leq 2}, \qquad \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & h \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \qquad \text{and}$$

$$g : \mathbb{Q}^{3\leq 3} \to \mathbb{Q}^{2\leq 2}, \qquad \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & h \end{pmatrix} \mapsto \begin{pmatrix} d & e \\ 0 & h \end{pmatrix}.$$

What is their equalizer?]

2.7.4. Basic properties of ring isomorphisms

We shall now show some fundamental facts about ring isomorphisms.

First, let us give a somewhat simplified characterization of ring isomorphisms. According to Definition 2.7.1 **(b)**, if you want to prove that a map f is a ring isomorphism, you have to check (1) that f is a ring morphism, (2) that f has an inverse, and (3) that this inverse f^{-1} is a ring morphism. However, it turns out that step (3) is unnecessary, since it follows from steps (1) and (2). Let us state this fact and prove it:

Proposition 2.7.7. Let R and S be two rings. Let $f : R \to S$ be an invertible ring morphism. Then, f is a ring isomorphism.

Proof. This is proved using the same reasoning as for groups (but not for topological spaces): You need to show that f^{-1} is a ring morphism. Let me just show that f^{-1} respects addition (the proofs of the other axioms are similar). So let $c, d \in S$; we must show that $f^{-1}(c+d) = f^{-1}(c) + f^{-1}(d)$.

It is clearly sufficient to check that $f\left(f^{-1}(c+d)\right) = f\left(f^{-1}(c) + f^{-1}(d)\right)$. Indeed, if we can show this equality, then we can apply f^{-1} to it and obtain $f^{-1}(c+d) = f^{-1}(c) + f^{-1}(d)$, which is what we want to prove.

Recall that f respects addition. Thus,

$$f\left(f^{-1}(c) + f^{-1}(d)\right) = f\left(f^{-1}(c)\right) + f\left(f^{-1}(d)\right) = c + d = f\left(f^{-1}(c+d)\right).$$

Hence, $f\left(f^{-1}(c+d)\right) = f\left(f^{-1}(c) + f^{-1}(d)\right)$ is proved. □

Incidentally, [DumFoo04] defines ring isomorphisms as invertible ring morphisms. Proposition 2.7.7 shows that this is equivalent to our definition.

We continue with some more straightforward results:

Proposition 2.7.8. Let R, S and T be three rings. Let $f : S \to T$ and $g : R \to S$ be two ring isomorphisms. Then, $f \circ g : R \to T$ is a ring isomorphism.

Proof. This is proved in the same way as for groups. □

Proposition 2.7.9. Let R and S be two rings. Let $f : R \to S$ be a ring isomorphism. Then, $f^{-1} : S \to R$ is a ring isomorphism.

Proof. This is proved in the same way as for groups. □

Corollary 2.7.10. The relation $\cong$ for rings is an equivalence relation.

Proof. Transitivity follows from Proposition 2.7.8. Reflexivity follows from the obvious fact that $\mathrm{id} : R \to R$ is a ring isomorphism whenever R is a ring. Symmetry follows from Proposition 2.7.9. □

The most useful property of ring isomorphisms is the following "meta-theorem":

> **Isomorphism principle for rings:** Let R and S be two isomorphic rings. Then, any "ring-theoretic" property of R (that is, any property that does not refer to what the elements of R are, but can be stated entirely in terms of how they "interact" via the ring operations) that holds for R must hold for S as well.

This is somewhat nebulous: What exactly makes a property of a ring "ring-theoretic"? In lieu of a formal definition, let us give some examples of "ring-theoretic" properties of R (which may or may not hold):

- The ring R has 15 elements.
- The ring R is commutative.
- The ring R is a field.
- For any $a, b, c \in R$, we have $3abc\,(a+b+c) = 0_R$ (where the "3" is the integer 3).
- The center of R has 10 elements.
- There exist two nonzero elements $a, b \in R$ satisfying $a^2 + b^2 = 0_R$.

Thus, all of these properties can be automatically transferred from any ring to any isomorphic ring.

In contrast, here are some examples of properties of R that are **not** "ring-theoretic":

- The elements of R are matrices.
- The ring R is a subset of $\mathbb{R}$.
- The ring R is a subring of $\mathbb{R}$. (**But** the more professional variant "there is an injective ring morphism from R to $\mathbb{R}$" would be ring-theoretic!)

- The set R is disjoint from $\mathbb{C}$.
- There exist two nonzero elements $a, b \in R$ satisfying $a^2 + b^2 = 0_{\mathbb{Z}}$ (the zero of $\mathbb{Z}$).
- The set R contains the complex number $i = \sqrt{-1}$.

Clearly, an isomorphism can destroy these properties, since it can send elements to different elements.

To make sure you understand the meaning of ring isomorphisms, pick any of the above "ring-theoretic" properties of R, and show that it is preserved by isomorphisms (i.e., if it holds for a ring R, then it holds for any ring S isomorphic to R). The proof is analogous to the similar argument for groups.

The following exercise shows an example of a non-obvious ring isomorphism:

Exercise 2.7.9. Define a subring $\mathcal{M}$ of $\mathbb{R}^{2\times 2}$ as in Exercise 2.4.1. Consider the map

$$\begin{aligned} f : \mathbb{C} &\to \mathcal{M}, \\ a + bi &\mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad (\text{for } a, b \in \mathbb{R}). \end{aligned}$$

(a) Prove that f is a ring isomorphism.

(b) Use this to solve Exercise 2.4.1 **(c)** again.

2.7.5. Injective morphisms and their images

If $f : R \to S$ is an injective map from some set R to some set S, then its image $f(R)$ is in one-to-one correspondence with its domain R (via the map $R \to f(R)$ that sends each r to $f(r)$). The same holds for ring morphisms, except that the one-to-one correspondence is now a ring isomorphism:

Proposition 2.7.11. Let R and S be two rings. Let $f : R \to S$ be an injective ring morphism. Then:

(a) The subring $f(R)$ of S (known from Proposition 2.7.6) is isomorphic to R.

(b) More specifically: The map

$$\begin{aligned} R &\to f(R), \\ r &\mapsto f(r) \end{aligned}$$

is a ring isomorphism.

Proof. The map

$$R \to f(R), \\ r \mapsto f(r)$$

is clearly well-defined (since $f(r) \in f(R)$ for each $r \in R$). Let us denote it by f'. This map f' differs from the map f only in that it goes to $f(R)$ rather than to S. Hence, this map f' is injective (since f is injective) and surjective (since each element of $f(R)$ has the form $f(r)$ for some $r \in R$ by definition, and thus equals $f'(r)$ for the same $r \in R$). Hence, it is bijective, i.e., invertible.

Moreover, $f(R)$ is a subring of S, so that its addition, multiplication, zero and unity are inherited from S. Hence, from the fact that f is a ring morphism, we conclude immediately that the map f' (which differs from f only in that it goes to $f(R)$ rather than to S) is a ring morphism as well. Thus, f' is an invertible ring morphism, hence (by Proposition 2.7.7) a ring isomorphism. In other words, the map

$$R \to f(R), \\ r \mapsto f(r)$$

is a ring isomorphism (since this map is f'). Hence, $f(R)$ is isomorphic to R. This proves Proposition 2.7.11. □

2.7.6. Advanced exercises on ring isomorphisms

Here are some further exercises on ring isomorphisms.

Exercise 2.7.10. Let F be a commutative ring. Let R be the set of all 3×3-matrices of the form $\begin{pmatrix} a & b & c \\ 0 & d & 0 \\ 0 & 0 & e \end{pmatrix} \in F^{3\times 3}$ with $a, b, c, d, e \in F$. It is not hard to see that R is a subring of $F^{3\times 3}$.

(a) Prove that if $A, B, C \in R$ are any three matrices in R, then the matrix $C(AB - BA) \in R$ is a scalar multiple of the matrix $AB - BA$. (A "scalar multiple" of a matrix M means a matrix of the form λM with $\lambda \in F$.)

(b) Prove that it is not always true that if $A, B, C \in R$ are any three matrices in R, then the matrix $(BA - AB)C \in R$ is a scalar multiple of the matrix $BA - AB$.

(c) Conclude that R is not isomorphic to R^{op} when $F = \mathbb{Z}$ or $F = \mathbb{Z}/2$.

The next two exercises characterize rings of certain small sizes:

Exercise 2.7.11. Let p be a prime. Let R be a ring of size $|R| = p$. Prove that R is isomorphic to the ring $\mathbb{Z}/p$.

[**Hint:** Prove that the additive group $(R, +, 0)$ must be generated by 1. Argue that this uniquely determines the multiplication of R.]

Exercise 2.7.12. Let R be a ring of size $|R| = 4$. Prove that R is isomorphic to one of the four rings $\mathbb{Z}/4$, F_4, D_4 and B_4 we have seen in Subsection 2.1.2.

[**Hint:** As in Exercise 2.3.4, consider the subgroup $\langle 1 \rangle$ of $(R, +, 0)$. If this subgroup is the whole R, then argue that $R \cong \mathbb{Z}/4$. If not, choose an arbitrary $x \in R \setminus \langle 1 \rangle$, and distinguish cases based on what x^2 is.]

2.8. Ideals and kernels ([DumFoo04, §7.1])

2.8.1. Kernels

In linear algebra, the kernel (aka nullspace) of a linear map "measures how non-injective it is". The same can be done for ring morphisms:

Definition 2.8.1. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then, the **kernel** of f (denoted $\ker f$ or $\operatorname{Ker} f$) is defined to be the subset

$$\operatorname{Ker} f := \{a \in R \mid f(a) = 0_S\}$$

of R.

Some examples:

- Let $n \in \mathbb{Z}$. The kernel of the ring morphism $\pi : \mathbb{Z} \to \mathbb{Z}/n,\ a \mapsto \overline{a}$ is $n\mathbb{Z} = \{\text{all multiples of } n\}$.
- Let R be a ring. Let S be any set. Recall the ring R^S of all functions from S to R. Fix an element $s \in S$. Then, the kernel of the ring morphism $R^S \to R,\ f \mapsto f(s)$ is the set of all functions $f \in R^S$ that vanish on s.
- The kernel of an injective ring morphism $f : R \to S$ is always $\{0_R\}$. Indeed, if $f : R \to S$ is an injective ring morphism, then f sends 0_R to 0_S (since f is a ring morphism), and therefore f cannot send any other element to 0_S (since f is injective).

2.8.2. Ideals

As we saw in the above example, the kernel of a ring morphism is not usually a subring of R, since it normally does not contain 1_R. However, it satisfies all the other axioms for a subring (which is why [DumFoo04] considers it a subring of R). We can say more, however. The type of a subset that kernels of ring morphisms are has its own name:

Definition 2.8.2. Let R be a ring. An **ideal** of R is a subset I of R such that

- we have $a + b \in I$ for any $a, b \in I$;
- we have $ab \in I$ and $ba \in I$ for any $a \in R$ and $b \in I$;
- we have $0 \in I$ (where the 0 means the zero of R).

When R is commutative, of course, the "$ab \in I$" and "$ba \in I$" conditions are equivalent.

The three conditions in Definition 2.8.2 are called the "**ideal axioms**". The first and the third of them are familiar (they already appeared in the definition of a subring). The second is new – it is saying that if a factor in a product belongs to I, then the whole product belongs to I, no matter what the other factors are.[34]

Here are some easy consequences of Definition 2.8.2:

Proposition 2.8.3. Let R be a ring. Let I be an ideal of R. Then, I is a subgroup of the additive group $(R, +, 0)$.

Proof. The first and third "ideal axioms" reveal that I is closed under addition and contains 0. It remains to show that I is closed under negation – i.e., that we have $-b \in I$ for each $b \in I$. But this is easy: If $b \in I$, then the second "ideal axiom" (applied to $a = -1$) yields $(-1)\, b \in I$ and $b\,(-1) \in I$. But this rewrites as $-b \in I$, qed. □

Theorem 2.8.4. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then, the kernel $\operatorname{Ker} f$ of f is an ideal of R.

Proof. We need to prove the three "ideal axioms". Let me only show the second, as the other two are similar. So let $a \in R$ and $b \in \operatorname{Ker} f$. We must prove that $ab \in \operatorname{Ker} f$ and $ba \in \operatorname{Ker} f$.

We have $b \in \operatorname{Ker} f$, so that $f(b) = 0$ (by the definition of $\operatorname{Ker} f$). Now, the map f is a ring morphism and thus respects multiplication. Hence, $f(ab) = f(a) \cdot \underbrace{f(b)}_{=0} = f(a) \cdot 0 = 0$, so that $ab \in \operatorname{Ker} f$ (by the definition of $\operatorname{Ker} f$). Similarly, $ba \in \operatorname{Ker} f$. Thus we have shown the second ideal axiom. □

We will soon see a converse of this theorem: Every ideal of a ring R is the kernel of some ring morphism from R. (Namely, this follows from Theorem 2.9.3 below.)

[34] This second axiom is sometimes called the "**absorption axiom**", referring to the idea that the ideal I "absorbs" every product as long as even one factor of the product is in the ideal. I prefer to think of it as "contagiousness". Another picture in my mind is that I is some kind of ditch which you can enter but never escape through multiplication with elements of R.

2.8.3. Principal ideals

The simplest way to construct ideals of a commutative ring is by fixing an element and taking all its multiples:

Proposition 2.8.5. Let R be a commutative ring.

(a) Let $u \in R$. We define uR to be the set $\{ur \mid r \in R\}$. The elements of this set uR are called the **multiples** of u (in R).

Then, uR is an ideal of R. This ideal is known as a **principal ideal** of R.

(b) In particular, $0R = \{0_R\}$ and $1R = R$ are therefore principal ideals of R.

Proof. **(a)** The only thing to prove is that uR is an ideal of R. But this can be easily achieved by checking that it satisfies all three ideal axioms:

- We have $a + b \in uR$ for any $a \in uR$ and $b \in uR$. (Indeed, if $a \in uR$ and $b \in uR$, then there exist $x, y \in R$ satisfying $a = ux$ and $b = uy$ (since $a \in uR$ and $b \in uR$), and therefore we have $a + b = ux + uy = u(x + y) \in uR$.)
- We have $ab \in uR$ and $ba \in uR$ for any $a \in R$ and $b \in uR$. (Indeed, if $a \in R$ and $b \in uR$, then there exists an $r \in R$ satisfying $b = ur$ (since $b \in uR$), and thus we have $ab = aur = u(ar) \in uR$ and therefore $ba = ab \in uR$.)
- We have $0 \in uR$ (since $0 = u \cdot 0$).

Thus, Proposition 2.8.5 **(a)** is proved.

(b) The equalities $0R = \{0_R\}$ and $1R = R$ are obvious (since each $r \in R$ satisfies $0r = 0$ and $1r = r$). The rest follows from part **(a)**. □

For example, $2\mathbb{Z} = \{\text{all even integers}\}$ is an ideal of $\mathbb{Z}$.

Exercise 2.8.1.

(a) Let F be a field. Prove that the only ideals of F are $0F = \{0_F\}$ and $1F = F$.

(b) Conversely, let R be a nontrivial commutative ring that has only two ideals. Prove that R is a field.

The requirement that R be commutative in Proposition 2.8.5 was not gratuitous; the set uR is not always an ideal when R is not commutative. Nevertheless, principal ideals can also be defined for noncommutative rings, but this is more complicated[35]. However, we don't need all of R to be commutative in order for uR to be an ideal; we can get by with a more local assumption:

[35]Some details:

Exercise 2.8.2. Let R be a ring (not necessarily commutative). Let u be a central element of R. (See Definition 2.3.7 **(a)** for the meaning of "central".)

Prove that the set uR (as defined in Proposition 2.8.5) is an ideal of R.

2.8.4. Other examples of ideals

In general, not all ideals of a ring need to be principal. However, in order to find non-principal ideals, we need to venture beyond the classical number rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, because the latter rings have the property that all their ideals are principal (this will follow from Proposition 2.13.3 further below). One way to construct non-principal ideals is to work with polynomials in several variables over a field, or even with univariate polynomials over $\mathbb{Z}$. For example:

- The set of all polynomials $f \in \mathbb{Q}[x, y]$ that have constant term 0 is an ideal of $\mathbb{Q}[x, y]$ that is not principal.
- The set of all polynomials $f \in \mathbb{Z}[x]$ whose constant term is even is an ideal of $\mathbb{Z}[x]$ that is not principal.

We will come back to this later when we actually have defined polynomials.

For further examples of ideals, one might look into noncommutative rings. However, matrix rings like $\mathbb{R}^{n\times n}$ are rather disappointing in this regard:

Exercise 2.8.3. Let F be a field. Let $n \in \mathbb{N}$. Prove that the matrix ring $F^{n\times n}$ has only two ideals, namely $\{0\}$ and the whole $F^{n\times n}$ (where 0 stands for the zero matrix).

[**Hint:** For each $i, j \in \{1, 2, \ldots, n\}$, let $E_{i,j} \in F^{n\times n}$ be the (i, j)**-th elementary matrix** – i.e., the $n \times n$-matrix whose (i, j)-th entry is 1 and whose all remaining entries are 0. What happens when you multiply a given matrix $A \in F^{n\times n}$ by $E_{i,j}$ from the left or from the right? I.e., how can you describe the matrices $E_{i,j}A$ and $AE_{i,j}$?]

Considering matrix rings over a ring R (instead of over a field F) ameliorates the lack of ideals only slightly – namely, to the extent that R itself has interesting ideals. For example, for each integer m, the matrix ring $\mathbb{Z}^{2\times 2}$ has an ideal consisting of all the matrices whose entries are divisible by m. More generally, any ideal of a ring R yields an ideal of the matrix $R^{n\times n}$:

If R is a noncommutative ring, then **in general** neither $uR = \{ur \mid r \in R\}$ nor its mirror analogue $Ru = \{ru \mid r \in R\}$ are ideals of R. (For example, uR may fail the "$ab \in uR$ for any $a \in R$ and $b \in uR$" requirement, because there is no way to move the u to the left of the a.) This suggests considering the set $\{rus \mid r, s \in R\}$, but this is still not an ideal (in general), since it is not always closed under addition.

However, one can define the "principal ideal" RuR to be

$$\{\text{all finite sums of the form } r_1us_1 + r_2us_2 + \cdots + r_nus_n \text{ with } r_i, s_i \in R\}.$$

This is always an ideal of R.

Exercise 2.8.4. Let R be a ring. Let $n \in \mathbb{N}$.

For each subset I of R, let $I^{n\times n}$ be the subset

$$\left\{A \in R^{n\times n} \mid \text{all entries of } A \text{ belong to } I\right\}$$

of the matrix ring $R^{n\times n}$. Prove the following:

(a) If I is an ideal of R, then $I^{n\times n}$ is an ideal of the matrix ring $R^{n\times n}$.

(b) Any ideal of $R^{n\times n}$ has the form $I^{n\times n}$ for some ideal I of R.

But we can go beyond matrix rings in search of interesting ideals. Going beyond matrix rings doesn't mean extending matrix rings; instead, it suffices to consider some of their subrings. As we know, the upper-triangular matrices form a subring of the matrix ring, as do the lower-triangular ones. Here, a plethora of ideals appears. Some examples follow:

Exercise 2.8.5. Let R be any ring. Recall that $R^{n\leq n}$ denotes the ring of all upper-triangular $n \times n$-matrices with entries in R. In particular,

$$R^{2\leq 2} = \left\{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in R\right\}.$$

(a) Define four subsets I, J, K, L of $R^{2\leq 2}$ by

$$I := \left\{\begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \mid b, d \in R\right\};$$

$$J := \left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in R\right\};$$

$$K := \left\{\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in R\right\};$$

$$L := \left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in R\right\}.$$

Prove that I, J and K are ideals of $R^{2\leq 2}$, but L is not (unless R is trivial).

(b) For any $n \in \mathbb{N}$, prove that the subset

$$\left\{A \in R^{n\times n} \mid \text{all nonzero entries of } A \text{ lie in the first row}\right\}$$
$$= \left\{\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} \mid a_{1,1}, a_{1,2}, \ldots, a_{1,n} \in R\right\}$$

is an ideal of $R^{n\leq n}$, but the subset

$$\left\{A \in R^{n\leq n} \mid \text{all nonzero entries of } A \text{ lie in the second row}\right\}$$

is not (for R nontrivial and $n \geq 2$).

(c) For any $n \in \mathbb{N}$, prove that the subset

$$\begin{aligned}&\left\{A \in R^{n\times n} \;\mid\; \text{all nonzero entries of } A \text{ lie in the first row or the last column}\right\}\\ &= \left\{ \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ 0 & 0 & 0 & \cdots & a_{2,n} \\ 0 & 0 & 0 & \cdots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_{n,n} \end{pmatrix} \;\mid\; a_{1,1}, a_{1,2}, \ldots, a_{1,n}, a_{2,n}, a_{3,n}, \ldots, a_{n,n} \in R \right\}\end{aligned}$$

is an ideal of $R^{n\leq n}$.

(d) For any $n \in \mathbb{N}$, prove that the subset

$$\begin{aligned}&R^{n<n}\\ &:= \left\{A \in R^{n\leq n} \;\mid\; \text{all diagonal entries of } A \text{ equal } 0\right\}\\ &= \left\{A \in R^{n\times n} \;\mid\; \text{all nonzero entries of } A \text{ lie above the main diagonal}\right\}\\ &= \left\{ \begin{pmatrix} 0 & a_{1,2} & a_{1,3} & \cdots & a_{1,n} \\ 0 & 0 & a_{2,3} & \cdots & a_{2,n} \\ 0 & 0 & 0 & \cdots & a_{3,n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix} \;\mid\; a_{i,j} \in R \text{ for all } i < j \right\}\end{aligned}$$

is an ideal of $R^{n\leq n}$. This subset $R^{n<n}$ is called the set of **strictly upper-triangular** $n \times n$-matrices over R.

(e) (For combinatorialists familiar with partially ordered sets:) Consider an $n \in \mathbb{N}$. Assume that some cells of an (unfilled) $n \times n$-matrix are colored red. What combinatorial properties must our coloring satisfy in order for the set

$$\left\{A \in R^{n\times n} \;\mid\; \text{all nonzero entries of } A \text{ lie in red cells}\right\}$$

to be an ideal of $R^{n\leq n}$?

The next exercise assigns a certain important ideal to every commutative ring R:

Exercise 2.8.6. Let R be a ring. An element $a \in R$ is said to be **nilpotent** if there exists an $n \in \mathbb{N}$ such that $a^n = 0$. (For example, the residue class $\overline{6}$ in $\mathbb{Z}/8\mathbb{Z}$ is nilpotent, since its 3-rd power is $\overline{0}$.)

(a) If a and b are two nilpotent elements of R satisfying $ab = ba$, then prove that $a + b$ is nilpotent as well.

(b) Find a counterexample to part **(a)** if we don't assume $ab = ba$.

(c) Assume that the ring R is commutative. Let N be the set of all nilpotent elements of R. Prove that N is an ideal of R.

The ideal N in Exercise 2.8.6 **(c)** is known as the **nilradical** of R.

Exercise 2.8.7. Let n be a positive integer with prime factorization $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and $a_1, a_2, \ldots, a_k$ are positive integers. Let R be the ring $\mathbb{Z}/n$. Prove that the nilradical of R is the principal ideal $\overline{p_1 p_2 \cdots p_k} R$.

Exercise 2.8.8. Recall the set N defined in Exercise 2.8.6 **(c)**. Describe this set N

(a) in the case when R is the matrix ring $\mathbb{Q}^{2\times 2}$;

(b) in the case when R is the upper-triangular matrix ring $\mathbb{Q}^{2\leq 2}$ (see Section 2.3 for its definition).

Both of these rings R are noncommutative, so that Exercise 2.8.6 **(c)** does not apply. Nevertheless, is N an ideal of R in one of these two cases?

Exercise 2.8.9. Let R be a ring. If A, B, C, D are four subsets of R, then the notation $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ shall denote the set of all 2×2-matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R^{2\times 2}$ with $a \in A$, $b \in B$, $c \in C$ and $d \in D$. (For instance, $\begin{pmatrix} \mathbb{N} & 2\mathbb{Z} \\ 2\mathbb{Z} & \mathbb{N} \end{pmatrix}$ is the set of all 2×2-matrices whose diagonal entries are nonnegative integers and whose off-diagonal entries are even integers.)

(a) Let I be a subset of R. Prove that I is an ideal of R if and only if $\begin{pmatrix} R & I \\ \{0\} & R \end{pmatrix}$ is a subring of $R^{2\times 2}$.

(b) Does the same claim hold for $\begin{pmatrix} R & I \\ I & R \end{pmatrix}$ instead of $\begin{pmatrix} R & I \\ \{0\} & R \end{pmatrix}$?

(c) Does the same claim hold for $\begin{pmatrix} R & I \\ R & R \end{pmatrix}$ instead of $\begin{pmatrix} R & I \\ \{0\} & R \end{pmatrix}$?

(d) Does the same claim hold for $\begin{pmatrix} R & R \\ R & I \end{pmatrix}$ instead of $\begin{pmatrix} R & I \\ \{0\} & R \end{pmatrix}$?

The following exercise gives some examples of principal and non-principal ideals:

Exercise 2.8.10. Let R be a ring, and let S be a set. Let R^S be the ring of all functions from S to R (with pointwise addition and multiplication).

The **support** of a function $f : S \to R$ is defined to be the set of all $x \in S$ such that $f(x) \neq 0$. This support is denoted by $\operatorname{Supp} f$.

(a) Let T be any subset of S. Prove that the set

$$R_T^S := \{f : S \to R \mid \operatorname{Supp} f \subseteq T\}$$

is an ideal of R^S, and is in fact a principal ideal if R is commutative.

(b) Prove that the set

$$R^S_{\text{fin}} := \{f : S \to R \mid \text{Supp } f \text{ is a finite set}\}$$

is an ideal of R^S.

(c) Now, assume that $R = \mathbb{Q}$ and $S = \mathbb{Q}$. Prove that R^S_{fin} is not a principal ideal of R^S.

Another example of a non-principal ideal comes from real analysis:

Exercise 2.8.11. Let R be the ring of all functions from $\mathbb{R}$ to $\mathbb{R}$ (with pointwise addition and pointwise multiplication).

The **support** of a function $f : \mathbb{R} \to \mathbb{R}$ is defined to be the set of all $x \in \mathbb{R}$ such that $f(x) \neq 0$.

A subset S of $\mathbb{R}$ is said to be **null** (or to have **Lebesgue measure zero**) if for every positive real ε, there exists a countable union of intervals $I_1 \cup I_2 \cup I_3 \cup \cdots$ in $\mathbb{R}$ such that $S \subseteq I_1 \cup I_2 \cup I_3 \cup \cdots$ and such that the sum of the lengths of these intervals $I_1, I_2, I_3, \ldots$ is smaller than ε. (In particular, any finite or countable subset of $\mathbb{R}$ is null.)

We let I be the set of all functions $f : \mathbb{R} \to \mathbb{R}$ whose support is null. (For example, the function that sends every rational number to 1 and every irrational number to 0 belongs to I, since its support is $\mathbb{Q}$, which is null.)

(a) Prove that I is an ideal of R.

(b) Prove that this ideal I is not principal.

2.9. Quotient rings ([DumFoo04, §7.3])

We now come to one of the most abstract sections of this course: the definition and the basic properties of quotient rings.

Before we define this notion rigorously, let me outline what it is meant to achieve.

Recall the idea behind modular arithmetic (Section 1.4): By passing from the integers to their residue classes modulo a given integer n, we are essentially equating n with 0 (so that two integers become "equal" if they differ by a multiple of n). Thus, these residue classes are "what remains" of the integers if we equate n with 0.

The same passage can be made in greater generality: We can start with any ring R and any ideal I of R, and we can equate all elements of I with 0 (so that two elements of R become "equal" if they differ by an element of I). What remains is again called "residue classes" (now modulo I instead of modulo n),

and we can again define addition and multiplication on these residue classes. The result is a new ring, which is called the **quotient ring** of R by the ideal I, and is denoted by R/I. Working in this quotient ring is a natural generalization of modular arithmetic to things that aren't integers. For instance, we can start with the Gaussian integers and equate 5 with 0, or we can start with the upper-triangular 2×2-matrices[36] and equate the strictly upper-triangular 2×2-matrices[37] with zero. This gives us a new way to build new rings from old.[38]

So much for the idea; let us now define the quotient ring R/I formally.

In rigorous mathematics, you cannot just take two distinct elements and declare them to be equal. Thus, "equating" two elements of R is easier said than done. The right way to do it is by passing from elements to equivalence classes (just as we did in modular arithmetic, back in Section 1.4). Let us see how this can be done.

2.9.1. Quotient groups

It turns out that we don't need to reinvent the wheel: You have already seen these equivalence classes in group theory, under the name "**cosets**". Let me recall how these were defined and used:

- If H is a subgroup of a group G, then the **left cosets** of H in G are the subsets $gH := \{gh \mid h \in H\}$ for all $g \in G$. There is one left coset gH for each $g \in G$; but different $g \in G$ often lead to the same left coset gH, so there are usually fewer left cosets than elements of G. The set of all left cosets of H is denoted by G/H.

- If H is merely a subgroup of a group G, then G/H is merely a "G-set" (i.e., a set with an action of G). However, when H is a **normal** subgroup of G (that is, a subgroup of G satisfying $gng^{-1} \in H$ for each $g \in G$ and $n \in H$), then G/H becomes a **group** as well, with group operation defined by
$$(g_1H)\,(g_2H) = g_1g_2H \qquad \text{for all } g_1, g_2 \in G. \tag{7}$$
This group G/H is called the **quotient group** of G by H. The left cosets of H in G are just called the **cosets** of H in G in this case.

- If G is an abelian group, then any subgroup H of G is normal, so G/H always is a group.

[36] i.e., the matrices of the form $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$

[37] i.e., the matrices of the form $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$

[38] For comparison: When you take a subring of a ring R, you are throwing away some elements of R. In contrast, when you take a quotient ring of R, you are equating some elements of R with one another. In either case, you end up with a ring smaller than R.

- Now, assume that G is an **additive** group (which means that its binary operation is written as $+$ rather than as $\cdot$). This presupposes that G is abelian, as it is considered gauche to write a non-abelian group additively. Let H be a subgroup of G. Then, the cosets of H in G are denoted by $g+H$ instead of gH (in order to match the additive notation for the group operation). Likewise, we write $+$ instead of $\cdot$ for the binary operation of the quotient group G/H. The equality (7) therefore rewrites as

$$(g_1+H)+(g_2+H)=(g_1+g_2)+H \qquad \text{for all } g_1,g_2\in G.$$

  Note that the quotient group G/H is an abelian group.

- The most famous example of quotient groups is when $G=\mathbb{Z}$ and $H=n\mathbb{Z}=\{\text{all multiples of } n\}$ for some fixed integer n. (Here, the group operation on G is addition of integers.) In this case, the quotient group $\mathbb{Z}/n\mathbb{Z}$ is the cyclic group $\mathbb{Z}/n$, also known as Z_n. See [Siksek20, Chapter XII] for this and other examples.

2.9.2. Quotient rings

Now, piggybacking on the construction of quotient groups we just recalled, we shall define a similar quotient structure for rings instead of groups. Instead of normal subgroups, we will use ideals this time:

Definition 2.9.1. Let I be an ideal of a ring R. Thus, I is a subgroup of the additive group $(R,+,0)$, hence a normal subgroup (since $(R,+,0)$ is abelian). Therefore, the quotient group R/I is a well-defined abelian group. Its elements are the cosets $r+I$ of I in R. (Note that, since our groups are additive, we are writing $r+I$ for what would normally be written rI in group theory.)

Note that the addition on R/I is given by

$$(a+I)+(b+I)=(a+b)+I \qquad \text{for all } a,b\in R. \tag{8}$$

We now define a multiplication operation on R/I by setting

$$(a+I)\,(b+I)=ab+I \qquad \text{for all } a,b\in R. \tag{9}$$

(See below for a proof that this is well-defined.)

The set R/I, equipped with the addition and the multiplication we just defined and with the elements $0+I$ and $1+I$ (as zero and unity), is a ring (as we will show in a moment). This ring is called the **quotient ring** of R by the ideal I; it is also pronounced "R **modulo** I". It is denoted R/I (so when you hear "the ring R/I", it always means the set R/I equipped with the structure just mentioned).

The cosets $r+I$ are called **residue classes** modulo I, and are often denoted $r \bmod I$ or $[r]_I$ or $[r]$ or $\overline{r}$. (The last two notations are used when I is clear

from the context. We will mostly be using the notations $r + I$ and $\overline{r}$.) Thus, the equalities (8) and (9) can be restated as

$$\overline{a} + \overline{b} = \overline{a + b} \qquad \text{for all } a, b \in R \tag{10}$$

and

$$\overline{a} \cdot \overline{b} = \overline{ab} \qquad \text{for all } a, b \in R, \tag{11}$$

respectively.

Theorem 2.9.2. Let R and I be as in Definition 2.9.1. Then, the multiplication on R/I is well-defined, and R/I does indeed become a ring when endowed with the operations and elements just described.

Before we prove this theorem, let us see some examples:

- Let $n \in \mathbb{Z}$. The set $n\mathbb{Z} = \{\text{all multiples of } n\}$ is a principal ideal of $\mathbb{Z}$. The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is precisely the ring $\mathbb{Z}/n$ we discussed above. Its elements $r + n\mathbb{Z}$ are precisely the residue classes $\overline{r}$ defined in Section 1.4. The equalities (10) and (11) are precisely the standard definitions of addition and multiplication in $\mathbb{Z}/n$.

  Thus, the notion of a quotient ring generalizes the familiar concept of modular arithmetic. (More precisely, modular arithmetic is arithmetic in R/I where $R = \mathbb{Z}$ and $I = n\mathbb{Z}$.)

- Each ring R has two obvious ideals $\{0_R\}$ and R. The corresponding quotient rings $R/\{0_R\}$ and R/R are fairly boring:
  - The quotient ring $R/\{0_R\}$ is isomorphic to R (since each coset $r + \{0_R\}$ is just a 1-element set $\{r\}$, and thus the elements of $R/\{0_R\}$ are just the elements of R "clothed in set braces").
  - The quotient ring R/R is trivial (since there is only one coset, $r + R = 0 + R = 1 + R = R$, and it contains all elements of R).

  This generalizes the facts that $\mathbb{Z}/0 \cong \mathbb{Z}$ and that $\mathbb{Z}/1$ is trivial.

- Let R be the ring $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ of Gaussian integers. Consider its principal ideal

$$\begin{aligned} 3R &= \{3r \mid r \in R\} = \{3r \mid r \in \mathbb{Z}[i]\} \\ &= \{3a + 3bi \mid a, b \in \mathbb{Z}\} \\ &= \{c + di \mid c, d \in \mathbb{Z} \text{ are multiples of } 3\}. \end{aligned}$$

What is the quotient ring $R/(3R)$? Each element of this quotient ring can be written in the form[39]

$$\overline{a+bi} \qquad \text{with } a,b \in \{0,1,2\}$$

(since any Gaussian integer can be reduced to an $a+bi$ with $a,b \in \{0,1,2\}$ by subtracting an appropriate Gaussian-integer multiple of 3 [40]). In other words,

$$R/(3R) = \left\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{i},\ \overline{1+i},\ \overline{2+i},\ \overline{2i},\ \overline{1+2i},\ \overline{2+2i}\right\}.$$

It is easy to see that this is a 9-element ring (i.e., the residue classes $\overline{0},\ \overline{1},\ \overline{2},\ \overline{i},\ \overline{1+i},\ \overline{2+i},\ \overline{2i},\ \overline{1+2i},\ \overline{2+2i}$ are distinct[41]), and a field (i.e., all the nonzero residue classes are invertible[42]). So we have found a finite field with 9 elements.

Let us do some computations in this field: We have

$$\overline{2+i}+\overline{2+2i} = \overline{(2+i)+(2+2i)} = \overline{4+3i} = \overline{1}$$

(since $4+3i$ and 1 belong to the same coset of the ideal $3R$, as the difference $(4+3i)-1 = 3(1+i)$ lies in this ideal). We also have

$$\overline{2+i}\cdot\overline{2+2i} = \overline{(2+i)\cdot(2+2i)} = \overline{2+6i} = \overline{2}$$

(since $2+6i$ and 2 belong to the same coset of the ideal $3R$). A similar computation proves that

$$\overline{2+i}\cdot\overline{1+i} = \overline{1},$$

which reveals that the elements $\overline{2+i}$ and $\overline{1+i}$ of the ring $R/(3R)$ are inverses of each other (and thus are units of this ring).

[39] We are using $\overline{z}$ to denote the residue class of a Gaussian integer $z \in R$. This should not be confused with the complex conjugate of z (which is commonly denoted $\overline{z}$ as well). Fortunately, this confusion will be avoided in this example, since we will not use complex conjugates.

[40] *Proof.* Let $c+di$ be any Gaussian integer (with $c,d \in \mathbb{Z}$). Let q_c and r_c be the quotient and the remainder obtained when we divide c by 3. Let q_d and r_d be the quotient and the remainder obtained when we divide d by 3. Then, $c = 3q_c + r_c$ and $r_c \in \{0,1,2\}$ and $d = 3q_d + r_d$ and $r_d \in \{0,1,2\}$. Hence,

$$c+di = (3q_c+r_c)+(3q_d+r_d)\,i = 3\left(q_c+q_di\right)+\left(r_c+r_di\right).$$

Thus, by subtracting $3\left(q_c+q_di\right)$ (which is a Gaussian-integer multiple of 3), we can reduce $c+di$ to the Gaussian integer r_c+r_di, which has the form $a+bi$ with $a,b \in \{0,1,2\}$.

For example, $5+7i$ can be reduced to $2+i$ by subtracting $3(1+2i)$. Thus, $\overline{5+7i} = \overline{2+i}$.

[41] In order to verify this, you must show that no two of the Gaussian integers $0,\ 1,\ 2,\ i,\ 1+i,\ 2+i,\ 2i,\ 1+2i,\ 2+2i$ differ by a Gaussian-integer multiple of 3 (so that their residue classes are distinct).

[42] Checking this is Exercise 2.9.1 **(a)**.

For the curious: If we replace 3 by any other positive integer n, then $R/(nR)$ will be a finite ring with n^2 elements, but not always a field. Understanding when it will be a field is a fruitful question in elementary number theory. (It is a field for some, but not for all, primes n.)

We can also consider quotient rings of the form $R/(zR)$ for non-real $z \in R$. For example, one such quotient ring is $R/((1+i)R)$. It is much less obvious how many elements this quotient ring has! (See Exercise 2.9.2 below for the answer.)

Exercise 2.9.1. Let $R = \mathbb{Z}[i]$, as in the example we just did.

(a) Confirm that the quotient ring $R/(3R)$ is a field by finding inverses for all its eight nonzero elements.

(b) Confirm that the quotient ring $R/(5R)$ is not a field by checking that $\overline{1+2i} \cdot \overline{1-2i} = \overline{0}$ in this ring.

(c) Confirm that the quotient ring $R/(17R)$ is not a field either.

[**Hint:** For part **(c)**, find a similar equality as in part **(b)**.]

Exercise 2.9.2. Let $R = \mathbb{Z}[i]$, as in the above example. Prove that the quotient ring $R/((1+i)R)$ has just 2 elements, and in fact is isomorphic to $\mathbb{Z}/2$.

[**Hint:** First, show that both 2 and $2i$ belong to the principal ideal $(1+i)R$. Hence, each element of R can be reduced to the form $a+bi$ with $a, b \in \{0,1\}$ by subtracting an appropriate element of this ideal. Thus, the only possible residue classes in $R/((1+i)R)$ are $\overline{0}$, $\overline{1}$, $\overline{i}$ and $\overline{1+i}$. But the difference $i-1$ also lies in the principal ideal $(1+i)R$ (why?), and thus the classes $\overline{i}$ and $\overline{1}$ are actually identical. So are the classes $\overline{1+i}$ and $\overline{0}$. We are left with the two classes $\overline{0}$ and $\overline{1}$, which may or may not be actually distinct. Prove that they are distinct by arguing that 1 is not a multiple of $1+i$ in R. This shows that $R/((1+i)R)$ has exactly 2 elements.]

Exercise 2.9.3. Let R be the ring of all real numbers of the form $a+b\sqrt{5}$ with $a, b \in \mathbb{Z}$. (This is a ring for the same reasons that the S in Subsection 2.1.2 was a ring; the only difference is that we now require $a, b \in \mathbb{Z}$ instead of $a, b \in \mathbb{Q}$.)

(a) Is the quotient ring $R/(2R)$ a field?

(b) Is the quotient ring $R/(3R)$ a field?

(c) Prove that the quotient ring $R/(5R)$ is not a field, and in fact the residue class $\overline{\sqrt{5}}$ in this quotient is nilpotent. (See Exercise 2.8.6 for the meaning of "nilpotent".)

We will see more examples of quotient rings soon (and even more in later

chapters, after we introduce polynomial rings). For now, however, let us make good on our debts and prove Theorem 2.9.2:

Proof of Theorem 2.9.2. To see that the multiplication on R/I is well-defined (by the equation (9)), we must prove that a product xy with $x, y \in R/I$ does not depend on how exactly we write x and y as $x = a + I$ and $y = b + I$. In other words, we must show that if four elements a, a', b, b' of R satisfy $a + I = a' + I$ and $b + I = b' + I$, then $ab + I = a'b' + I$.

So let $a, a', b, b' \in R$ be such that $a + I = a' + I$ and $b + I = b' + I$. From $a + I = a' + I$, we obtain $a - a' \in I$, so that $(a - a')\, b \in I$ (by the second ideal axiom, since I is an ideal). In other words, $ab - a'b \in I$. Hence, $ab + I = a'b + I$. Similarly, we can obtain $a'b + I = a'b' + I$ (from $b + I = b' + I$). Thus, $ab + I = a'b + I = a'b' + I$, which is just what we need.

So we have shown that the multiplication on R/I is well-defined. Now why is R/I a ring? This we leave to the reader – it's a straightforward consequence of the fact that R is a ring.[43] □

Let me mention some more terminology (some of it informal but fairly popular):

When R is a ring, and I is an ideal of R, the quotient ring R/I is often just called the **quotient** of R by I. It is said to be obtained by **quotienting** R by I, or by **quotienting** I **out of** R.

2.9.3. More examples of quotient rings

Let us give two further hands-on examples of quotient rings. These are not strictly necessary for the understanding of what follows, but they give some extra intuition and practice.

- We recall (from Subsection 2.3.2) that $\mathbb{Q}^{3\leq 3}$ denotes the ring of all upper-triangular 3×3-matrices with rational entries. Thus,

$$\mathbb{Q}^{3\leq 3} = \left\{ \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \mid a, b, c, d, e, f \in \mathbb{Q} \right\}.$$

  The addition and the multiplication of this ring are matrix addition and matrix multiplication; its zero is the zero matrix $0_{3\times 3}$; its unity is the identity matrix I_3.

[43] For example, in order to prove that the multiplication on R/I is associative, we must show that $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for any three elements $x, y, z \in R/I$. But this is straightforward: If we write these three elements x, y, z as $x = a + I$ and $y = b + I$ and $z = c + I$, then this boils down to proving that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, which follows from associativity in R.

There is also a ring $\mathbb{Q}^{3=3}$ of all diagonal 3×3-matrices with rational entries. That is,

$$\mathbb{Q}^{3=3} = \left\{ \begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{pmatrix} \mid a, d, f \in \mathbb{Q} \right\}.$$

This is a subring of $\mathbb{Q}^{3\leq 3}$.

As in Exercise 2.8.5 **(d)**, we furthermore define $\mathbb{Q}^{3<3}$ to be the set of all matrices in $\mathbb{Q}^{3\leq 3}$ whose diagonal entries are 0. Thus,

$$\mathbb{Q}^{3<3} = \left\{ \begin{pmatrix} 0 & b & c \\ 0 & 0 & e \\ 0 & 0 & 0 \end{pmatrix} \mid b, c, e \in \mathbb{Q} \right\}.$$

The matrices in $\mathbb{Q}^{3<3}$ are known as "strictly upper-triangular 3×3-matrices".

We know from Exercise 2.8.5 **(d)** that $\mathbb{Q}^{3<3}$ is an ideal of $\mathbb{Q}^{3\leq 3}$ (and of course, we can also check this directly[44]). What is the quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3}$?

Any element of this quotient ring is a residue class of the form

$$\overline{A} = A + \mathbb{Q}^{3<3} \qquad \text{for some } A \in \mathbb{Q}^{3\leq 3}.$$

In other words, it is a set that consists of some given matrix $A \in \mathbb{Q}^{3\leq 3}$ and all matrices that can be obtained from A by adding a strictly upper-

[44]The only interesting part is to check the second ideal axiom, i.e., to show that if $A \in \mathbb{Q}^{3<3}$ and $B \in \mathbb{Q}^{3\leq 3}$, then AB and BA belong to $\mathbb{Q}^{3<3}$. Still, we can do this by direct computation:

$$\text{If } A = \begin{pmatrix} 0 & x & y \\ 0 & 0 & z \\ 0 & 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix},$$

$$\text{then } AB = \begin{pmatrix} 0 & dx & ex+fy \\ 0 & 0 & fz \\ 0 & 0 & 0 \end{pmatrix} \text{ and } BA = \begin{pmatrix} 0 & ax & ay+bz \\ 0 & 0 & dz \\ 0 & 0 & 0 \end{pmatrix}.$$

triangular 3×3-matrix. For example, if $A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix}$, then

$$\begin{aligned}
\overline{A} = A + \mathbb{Q}^{3<3} &= \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix} + \left\{ \begin{pmatrix} 0 & b & c \\ 0 & 0 & e \\ 0 & 0 & 0 \end{pmatrix} \mid b, c, e \in \mathbb{Q} \right\} \\
&= \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 0 & 6 \end{pmatrix} + \begin{pmatrix} 0 & b & c \\ 0 & 0 & e \\ 0 & 0 & 0 \end{pmatrix} \mid b, c, e \in \mathbb{Q} \right\} \\
&= \left\{ \begin{pmatrix} 1 & 2+b & 3+c \\ 0 & 4 & 5+e \\ 0 & 0 & 6 \end{pmatrix} \mid b, c, e \in \mathbb{Q} \right\} \\
&= \left\{ \begin{pmatrix} 1 & x & y \\ 0 & 4 & z \\ 0 & 0 & 6 \end{pmatrix} \mid x, y, z \in \mathbb{Q} \right\}
\end{aligned}$$

(here, we have substituted x, y, z for $2+b, 3+c, 5+e$, because when b ranges over $\mathbb{Q}$, so does $2+b$, etc.). So this set $\overline{A}$ consists of all upper-triangular 3×3-matrices whose diagonal entries are $1, 4, 6$ and whose above-diagonal entries are arbitrary rational numbers. We can thus view this set $\overline{A}$ as a "partly undetermined matrix", in the sense that it is "a matrix in which some of the entries can be filled in arbitrarily" (although, of course, formally speaking, it is not a matrix but a set of matrices). From this point of view, it makes sense to write $\overline{A}$ as follows:

$$\overline{A} = \begin{pmatrix} 1 & ? & ? \\ 0 & 4 & ? \\ 0 & 0 & 6 \end{pmatrix},$$

where each question mark stands for an undetermined entry (noting that different question marks are independent, i.e., there are three degrees of freedom). Formally, such a "partly undetermined matrix" is meant to be a set of matrices, where each question mark is a variable that can take any element of $\mathbb{Q}$ as value.

More generally, for any matrix $A = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \in \mathbb{Q}^{3 \leq 3}$, the residue class $\overline{A} \in \mathbb{Q}^{3 \leq 3} / \mathbb{Q}^{3<3}$ is

$$\overline{A} = \overline{\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}} = \begin{pmatrix} a & ? & ? \\ 0 & d & ? \\ 0 & 0 & f \end{pmatrix} \tag{12}$$

(written as a "partly undetermined matrix"). Thus, this class $\overline{A}$ does not depend on the above-diagonal entries of A. (This is not surprising: After

all, when we quotient out the ideal $\mathbb{Q}^{3<3}$, we are equating the strictly upper-triangular matrices with 0, which amounts to ignoring the above-diagonal entries.)

Thus, the quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3}$ is the set of "partly undetermined matrices" of the form $\begin{pmatrix} a & ? & ? \\ 0 & d & ? \\ 0 & 0 & f \end{pmatrix}$ (that is, upper-triangular 3×3-matrices with fixed entries on the main diagonal and question marks above it).

According to the formula (11), the multiplication on this quotient ring is given by

$$\begin{aligned} \overline{\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}} \cdot \overline{\begin{pmatrix} x & y & z \\ 0 & u & v \\ 0 & 0 & w \end{pmatrix}} &= \overline{\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \cdot \begin{pmatrix} x & y & z \\ 0 & u & v \\ 0 & 0 & w \end{pmatrix}} \\ &= \overline{\begin{pmatrix} ax & bu+ay & az+bv+cw \\ 0 & du & dv+ew \\ 0 & 0 & fw \end{pmatrix}}. \end{aligned}$$

In terms of "partly undetermined matrices", this can be rewritten in the following simpler form:

$$\begin{pmatrix} a & ? & ? \\ 0 & d & ? \\ 0 & 0 & f \end{pmatrix} \cdot \begin{pmatrix} x & ? & ? \\ 0 & u & ? \\ 0 & 0 & w \end{pmatrix} = \begin{pmatrix} ax & ? & ? \\ 0 & du & ? \\ 0 & 0 & fw \end{pmatrix}. \tag{13}$$

(As we said, the above-diagonal entries don't matter, so we don't need to even bother computing them.)

Similarly to (13), addition in $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3}$ is given by the formula

$$\begin{pmatrix} a & ? & ? \\ 0 & d & ? \\ 0 & 0 & f \end{pmatrix} + \begin{pmatrix} x & ? & ? \\ 0 & u & ? \\ 0 & 0 & w \end{pmatrix} = \begin{pmatrix} a+x & ? & ? \\ 0 & d+u & ? \\ 0 & 0 & f+w \end{pmatrix}. \tag{14}$$

I hope you are disappointed by the formulas (14) and (13). After all, what is happening in these formulas is just entrywise addition and entrywise multiplication of the diagonal entries. In other words, the "partly undetermined matrices" $\begin{pmatrix} a & ? & ? \\ 0 & d & ? \\ 0 & 0 & f \end{pmatrix}$ in our quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3}$ are behaving (under addition and multiplication) just like the diagonal matrices $\begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{pmatrix}$ in the ring $\mathbb{Q}^{3=3}$ (since the latter diagonal matrices, too,

are added and multiplied entrywise[45]). To state this more precisely, our quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3}$ turns out to be isomorphic to the ring $\mathbb{Q}^{3=3}$ of diagonal 3×3-matrices, and the isomorphism is just the map

$$\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3} \to \mathbb{Q}^{3=3},$$
$$\begin{pmatrix} a & ? & ? \\ 0 & d & ? \\ 0 & 0 & f \end{pmatrix} \mapsto \begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{pmatrix}$$

that replaces all question marks by zeroes. Thus, our "partly undetermined matrices" are just diagonal matrices in a complicated guise, and our quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<3}$ is just an isomorphic copy of the subring $\mathbb{Q}^{3=3}$. This doesn't feel worth the trouble of defining quotient rings!

If all quotient rings were as boring as this one, then the whole concept wouldn't be of much use. Fortunately, this is not the case: Not all quotient rings are subrings in disguise, and not all question marks can just be replaced by zeroes. We will see this in the next example.

- We again consider a quotient ring of $\mathbb{Q}^{3\leq 3}$, but this time we quotient out a smaller ideal. Namely, we define the subset

$$\mathbb{Q}^{3<<3} := \left\{ \begin{pmatrix} 0 & 0 & c \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \mid c \in \mathbb{Q} \right\}$$

of $\mathbb{Q}^{3\leq 3}$. This set $\mathbb{Q}^{3<<3}$ is an ideal of $\mathbb{Q}^{3\leq 3}$ (again, this can be checked directly[46]), and thus there is a quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<<3}$. In this quotient

[45] Indeed, addition and multiplication of diagonal matrices are given by the formulas

$$\begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{pmatrix} + \begin{pmatrix} x & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & w \end{pmatrix} = \begin{pmatrix} a+x & 0 & 0 \\ 0 & d+u & 0 \\ 0 & 0 & f+w \end{pmatrix}$$

and

$$\begin{pmatrix} a & 0 & 0 \\ 0 & d & 0 \\ 0 & 0 & f \end{pmatrix} \cdot \begin{pmatrix} x & 0 & 0 \\ 0 & u & 0 \\ 0 & 0 & w \end{pmatrix} = \begin{pmatrix} ax & 0 & 0 \\ 0 & du & 0 \\ 0 & 0 & fw \end{pmatrix}.$$

These look exactly like the formulas (14) and (13) for our "partly undetermined matrices", except that all question marks are replaced by zeroes.

[46] The only interesting part is to check the second ideal axiom, i.e., to show that if $A \in \mathbb{Q}^{3<<3}$

ring, the residue class $\overline{A}$ of a matrix $A = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \in \mathbb{Q}^{3\leq 3}$ is

$$\overline{A} = \overline{\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}} = \begin{pmatrix} a & b & ? \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$$
$$= \left\{ \begin{pmatrix} a & b & x \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \mid x \in \mathbb{Q} \right\}.$$

This is a "partly undetermined matrix" like those in the previous example, but this time only the northeasternmost entry is a question mark, since that entry is the only one that can be changed by adding a matrix in $\mathbb{Q}^{3<<3}$.

According to the formula (11), the multiplication on the quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<<3}$ is given by

$$\begin{pmatrix} a & b & ? \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \cdot \begin{pmatrix} x & y & ? \\ 0 & u & v \\ 0 & 0 & w \end{pmatrix} = \begin{pmatrix} ax & bu+ay & ? \\ 0 & du & dv+ew \\ 0 & 0 & fw \end{pmatrix}.$$

Again, the question-mark entry needs not be computed. What is new this time is that **we cannot replace the question marks by zeroes**. Indeed, the product

$$\begin{pmatrix} a & b & 0 \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix} \cdot \begin{pmatrix} x & y & 0 \\ 0 & u & v \\ 0 & 0 & w \end{pmatrix} = \begin{pmatrix} ax & bu+ay & bv \\ 0 & du & dv+ew \\ 0 & 0 & fw \end{pmatrix}$$

does not usually have a 0 in the northeasternmost position, so that the matrices of the form $\begin{pmatrix} a & b & 0 \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$ do not form a subring of $\mathbb{Q}^{3\leq 3}$. Thus, the multiplication of our "partly undetermined matrices" does not just reduce to the multiplication of regular matrices in a subring (like it did

and $B \in \mathbb{Q}^{3\leq 3}$, then AB and BA belong to $\mathbb{Q}^{3<<3}$. Still, we can do this by direct computation:

$$\text{If } A = \begin{pmatrix} 0 & 0 & y \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix},$$
$$\text{then } AB = \begin{pmatrix} 0 & 0 & fy \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } BA = \begin{pmatrix} 0 & 0 & ay \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

in the previous example). In other words, $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<<3}$ is not isomorphic to a subring of $\mathbb{Q}^{3\leq 3}$ (at least not in an obvious way as in the previous example), but is a genuinely new ring.

The first of the above two examples can be generalized from 3×3-matrices to $n \times n$-matrices (and from rational entries to entries in an arbitrary ring R):

Exercise 2.9.4. Let R be any ring. Let $n \in \mathbb{N}$. Recall that $R^{n\leq n}$ denotes the ring of all upper-triangular $n \times n$-matrices with entries in R. In Exercise 2.8.5 **(d)**, we have seen that

$$R^{n<n} = \left\{A \in R^{n\leq n} \mid \text{all diagonal entries of } A \text{ equal } 0\right\}$$

is an ideal of this ring $R^{n\leq n}$. The elements of $R^{n<n}$ are called the strictly upper-triangular matrices.

Let furthermore $R^{n=n}$ denote the set of all diagonal $n \times n$-matrices in $R^{n\times n}$. That is,

$$\begin{aligned} R^{n=n} &:= \left\{A \in R^{n\times n} \mid \text{all off-diagonal entries of } A \text{ equal } 0\right\} \\ &= \left\{ \begin{pmatrix} a_1 & 0 & 0 & \cdots & 0 \\ 0 & a_2 & 0 & \cdots & 0 \\ 0 & 0 & a_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & a_n \end{pmatrix} \mid a_1, a_2, \ldots, a_n \in R \right\}. \end{aligned}$$

It is easy to see that $R^{n=n}$ is a subring of $R^{n\times n}$.

We claim that the quotient ring $R^{n\leq n}/R^{n<n}$ is isomorphic to $R^{n=n}$. Intuitively, this is reasonable: When you start with all upper-triangular matrices but "equate" all the strictly upper-triangular matrices to zero, then you should be left with the diagonal matrices, since all the off-diagonal entries are "being ignored". Let us make this rigorous.

Define the map $\delta : R^{n\times n} \to R^{n\times n}$ as in Exercise 2.7.4. Note that the actual image of this map δ is $R^{n=n}$.

(a) Prove that the map

$$\begin{aligned} R^{n\leq n}/R^{n<n} &\to R^{n=n}, \\ \overline{A} &\mapsto \delta(A) \end{aligned}$$

is well-defined – i.e., the value $\delta(A)$ depends not on the matrix $A \in R^{n\leq n}$ but only on its residue class $\overline{A} \in R^{n\leq n}/R^{n<n}$. (In other words, prove that if two matrices $A, B \in R^{n\leq n}$ have the same residue class $\overline{A} = \overline{B}$ in $R^{n\leq n}/R^{n<n}$, then $\delta(A) = \delta(B)$.)

(b) Prove that this map is furthermore a ring morphism.

(c) Prove that this map is invertible.

This shows that the map is a ring isomorphism, and therefore we have $R^{n\leq n}/R^{n<n} \cong R^{n=n}$ as rings.

The ideal $\mathbb{Q}^{3<<3}$ of the second example can also be generalized:

Exercise 2.9.5. Let R be any ring. Let $n \in \mathbb{N}$. Let $k \in \mathbb{N}$. Recall that $R^{n\leq n}$ denotes the ring of all upper-triangular $n \times n$-matrices with entries in R.

A matrix $A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \in R^{n\times n}$ will be called **k-upper-triangular** if all its entries $a_{i,j}$ with $i > j + k$ are zero (i.e., if it satisfies $a_{i,j} = 0$ for all $i, j \in \{1, 2, \ldots, n\}$ satisfying $i > j + k$).

Let $R_k^{n\leq n}$ denote the set of all k-upper-triangular $n \times n$-matrices in $R^{n\times n}$. Prove that $R_k^{n\leq n}$ is an ideal of $R^{n\leq n}$.

[The ideals $\mathbb{Q}^{3<3}$ and $\mathbb{Q}^{3<<3}$ from the above two examples are $\mathbb{Q}_1^{3\leq 3}$ and $\mathbb{Q}_2^{3\leq 3}$, respectively.]

2.9.4. The canonical projection

Ideals of rings are somewhat like normal subgroups of groups: You can "quotient them out" (this is slang for "take a quotient by them") and get a ring again (by Theorem 2.9.2).

Now, we are ready to show that any ideal of a ring is the kernel of a ring morphism:

Theorem 2.9.3. Let R be a ring. Let I be an ideal of R. Consider the map

$$\begin{aligned} \pi : R &\to R/I, \\ r &\mapsto r + I. \end{aligned}$$

Then, π is a surjective ring morphism with kernel I.

Definition 2.9.4. This morphism π is called the **canonical projection** from R onto R/I.

Proof of Theorem 2.9.3. To prove that π is a ring morphism, we need to check that π respects addition, multiplication, zero and unity. All of this is straightforward. For example, in order to see that π respects multiplication, we must show that $\pi(rs) = \pi(r) \cdot \pi(s)$ for all $r, s \in R$; but this follows from

$$\begin{aligned} \pi(r) \cdot \pi(s) &= (r + I) \cdot (s + I) && \text{(by the definition of } \pi) \\ &= rs + I && \left(\begin{array}{c} \text{by the definition of the} \\ \text{multiplication in } R/I \end{array} \right) \\ &= \pi(rs) && \text{(by the definition of } \pi). \end{aligned}$$

Thus, we can show that π is a ring morphism.

The surjectivity of π is clear, since any element of R/I has the form $r + I = \pi(r)$ for some $r \in R$.

Finally, we need to show that π has kernel I. But this, too, is easy: The kernel of π consists of those elements $r \in R$ that satisfy $\pi(r) = 0_{R/I}$. But $\pi(r) = 0_{R/I}$ is equivalent to $r + I = 0 + I$ (since $\pi(r)$ is the coset $r + I$, whereas $0_{R/I}$ is the coset $0 + I$), which is tantamount to $r \in I$. Thus, the kernel of π is I. □

The canonical projection π in Theorem 2.9.3 can be viewed as "putting a bar on each element", since it sends each $r \in R$ to the residue class $\overline{r} \in R/I$.

For example, if we take $R = \mathbb{Z}$ and $I = 2\mathbb{Z}$ in Theorem 2.9.3, then the canonical projection π is the map

$$\begin{aligned} \pi : \mathbb{Z} &\to \mathbb{Z}/2, \\ r &\mapsto r + 2\mathbb{Z} = \overline{r}. \end{aligned}$$

This map π sends each even integer to $\overline{0}$ and each odd integer to $\overline{1}$. In other words, π assigns to each integer its parity (as an element of $\mathbb{Z}/2$).

The following two exercises ([21w, homework set #2, Exercise 10 **(a)** and **(b)**]) illustrate one of many uses of quotient rings:

Exercise 2.9.6. Let R be a commutative ring, and let u and n be two nonnegative integers. Let $x, y \in R$ be two elements such that $x - y \in uR$. (Here, $uR := \{ur \mid r \in R\}$; this is a principal ideal of R, since $uR = (u1_R) R$.)

Prove that

$$x^n - y^n \in guR, \qquad \text{where } g = \gcd(n, u).$$

[**Hint:** Write $x^n - y^n$ as $(x - y)\left(x^{n-1} + x^{n-2}y + \cdots + y^{n-1}\right)$, and show that the second factor belongs to gR. The latter is easiest to do by working in the quotient ring R/gR.]

Exercise 2.9.7. Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence, defined as in Definition 2.3.4. Prove that

$$\gcd(n, f_d) \cdot f_d \mid f_{dn} \qquad \text{for any } d, n \in \mathbb{N}.$$

[**Hint:** Define the matrices A and B and the commutative ring $\mathcal{F}$ as in Exercise 2.3.6, and apply Exercise 2.9.6 to $R = \mathcal{F}$ and $x = A^d$ and $y = B^d$ and $u = f_d$.]

2.9.5. The universal property of quotient rings: elementwise form

When trying to understand a quotient ring, it is important to construct ring morphisms into and out of it. (In the best case scenario, you can find mutually inverse maps in both directions, and thus obtain an isomorphism to another ring.)

Constructing morphisms $\alpha : S \to R/I$ into a quotient ring R/I is pretty easy (see Theorem 2.9.3 for an example).

Constructing morphisms $\beta : R/I \to S$ out of a quotient ring R/I is trickier. The main problem is to establish that β is well-defined: An element of a

quotient ring R/I can be written as $\overline{r}$ for many different elements $r \in R$, and therefore, when assigning an output value $\beta(\overline{r})$ for this element, we need to ensure that this value depends not on the r but only on the $\overline{r}$. This can be done by hand (see Exercise 2.9.4 **(a)** for an easy example of this), but gets tedious fairly soon. Is there a more comfortable method?

Yes, and such a method is provided by a theorem known as the "**universal property of quotient rings**". This theorem may appear technical, abstract and pointless at first sight, but it reveals its usefulness soon after you tire of manually constructing morphisms out of quotient rings. It provides a mechanical way of constructing a ring morphism $f' : R/I \to S$ out of a ring morphism $f : R \to S$, as soon as you can show that f sends all elements of the ideal I to 0. The well-definedness of f' and the fact that f' is a ring morphism are automatic consequences of the theorem, once its assumptions have been satisfied. Here is the precise statement of the theorem (in one of its forms):

Theorem 2.9.5 (Universal property of quotient rings, elementwise form)**.** Let R be a ring. Let I be an ideal of R.

Let S be a ring. Let $f : R \to S$ be a ring morphism. Assume that $f(I) = 0$ (this is shorthand for saying that $f(a) = 0$ for all $a \in I$). Then, the map

$$\begin{aligned} f' : R/I &\to S, \\ \overline{r} &\mapsto f(r) \qquad \text{(for all } r \in R\text{)} \end{aligned}$$

[47] is well-defined (i.e., the value $f(r)$ depends only on the residue class $\overline{r}$, not on r itself) and is a ring morphism.

Before we prove Theorem 2.9.5, let us give an example:

- Consider the canonical projections

$$\begin{aligned} \pi_6 : \mathbb{Z} &\to \mathbb{Z}/6, \\ r &\mapsto r + 6\mathbb{Z} \end{aligned}$$

and

$$\begin{aligned} \pi_3 : \mathbb{Z} &\to \mathbb{Z}/3, \\ r &\mapsto r + 3\mathbb{Z}. \end{aligned}$$

[47] Recall that $\overline{r}$ means the residue class of r in R/I, that is, the coset $r + I$. Thus, the definition of f' can be rewritten as follows:

$$\begin{aligned} f' : R/I &\to S, \\ r + I &\mapsto f(r) \qquad \text{(for all } r \in R\text{)}. \end{aligned}$$

Roughly speaking, the definition of f' says that f' sends a residue class where f would send any element of this residue class. The (slightly) nontrivial part here is to prove that this is well-defined, i.e., that f takes all elements of the given residue class to the same output value.

(Each of these two projections sends each integer r to its residue class $\overline{r}$, but the residue class is a modulo-6 class for π_6 and a modulo-3 class for π_3. The notation $\overline{r}$ can mean either $r+6\mathbb{Z}$ or $r+3\mathbb{Z}$ depending on the context. Thus, pay attention to the sets to which the elements belong!)

The ideal $6\mathbb{Z}$ of $\mathbb{Z}$ satisfies $\pi_3(6\mathbb{Z}) = 0$ (because any $j \in 6\mathbb{Z}$ is a multiple of 6, thus a multiple of 3, and therefore its residue class $j+3\mathbb{Z}$ is $\overline{0}$, and thus $\pi_3(j) = j+3\mathbb{Z} = \overline{0} = 0_{\mathbb{Z}/3}$). Thus, by Theorem 2.9.5 (applied to $R=\mathbb{Z}$, $I=6\mathbb{Z}$, $S=\mathbb{Z}/3$ and $f=\pi_3$), we see that the map

$$\begin{aligned} &\pi_3' : \mathbb{Z}/6 \to \mathbb{Z}/3, \\ &\qquad \overline{r} \mapsto \pi_3(r) \qquad \text{(that is, } r+6\mathbb{Z} \mapsto r+3\mathbb{Z}\text{)} \end{aligned} \tag{15}$$

is well-defined and is a ring morphism. Explicitly, this morphism π_3' sends[48]

$$\begin{aligned} &\text{the modulo-6 residue classes } \overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5} \\ &\text{to the modulo-3 residue classes } \overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}. \end{aligned}$$

In other words, it sends

$$\begin{aligned} &\text{the modulo-6 residue classes } \overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5} \\ &\text{to the modulo-3 residue classes } \overline{0},\ \overline{1},\ \overline{2},\ \overline{0},\ \overline{1},\ \overline{2} \end{aligned}$$

(because in $\mathbb{Z}/3$, we have $\overline{3} = \overline{0}$ and $\overline{4} = \overline{1}$ and $\overline{5} = \overline{2}$). If you don't believe in Theorem 2.9.5 yet, you can easily check by hand that this is a ring morphism.

More generally, if n and m are two integers such that $m \mid n$, then the map

$$\begin{aligned} &\mathbb{Z}/n \to \mathbb{Z}/m, \\ &\qquad \overline{r} \mapsto \overline{r} \qquad \text{(that is, } r+n\mathbb{Z} \mapsto r+m\mathbb{Z}\text{)} \end{aligned} \tag{16}$$

is well-defined and is a ring morphism. This follows from Theorem 2.9.5, applied to $R=\mathbb{Z}$, $I=n\mathbb{Z}$, $S=\mathbb{Z}/m$ and $f=\pi_m$ (the canonical projection from $\mathbb{Z}$ to $\mathbb{Z}/m$), because the condition $m \mid n$ yields $\pi_m(n\mathbb{Z}) = 0$. The morphism (16) can be regarded as reducing a modulo-n residue class "further" to a modulo-m residue class.

Incidentally, this accounts for all ring morphisms that go between two quotient rings of $\mathbb{Z}$. That is:

- If m and n are two integers such that $m \mid n$, then there is only one ring morphism $\mathbb{Z}/n \to \mathbb{Z}/m$, and it is the morphism (16).

[48] A "modulo-6 residue class" $\overline{r}$ means the residue class $r+6\mathbb{Z}$, whereas a "modulo-3 residue class" $\overline{r}$ means the residue class $r+3\mathbb{Z}$.

- If m and n are two integers such that $m \nmid n$, then there is no ring morphism $\mathbb{Z}/n \to \mathbb{Z}/m$.

Proving this is a nice (and easy) exercise (Exercise 2.9.11).

Let us now prove the universal property of quotient rings:

Proof of Theorem 2.9.5. We must prove the following two facts:

1. The map
$$f' : R/I \to S, \quad \overline{r} \mapsto f(r) \qquad (\text{for all } r \in R)$$
is well-defined – i.e., the value $f(r)$ depends only on the residue class $\overline{r}$ but not on the specific choice of r. (This will ensure that its definition does not give two conflicting output values $f'(x)$ for one and the same residue class $x \in R/I$, which would spell doom for the map f'.)

2. The map f' is a ring morphism.

Let us prove Fact 1 first. So let $r, r' \in R$ be such that $\overline{r} = \overline{r'}$. We must show that $f(r) = f(r')$.

We do what we can: From $\overline{r} = \overline{r'}$, we obtain $r - r' \in I$, so that $f(r - r') = 0$ because $f(I) = 0$. However, f is a ring morphism and thus respects differences; hence, $f(r - r') = f(r) - f(r')$. Thus, $f(r) - f(r') = f(r - r') = 0$, so that $f(r) = f(r')$. This proves Fact 1.

Let us now prove Fact 2. We need to show that f' is a ring morphism. There are four axioms to check, but we shall only show one of them (since the proofs of the other three axioms follow the same mold). Namely, we shall show that f' respects multiplication.

So let $a, b \in R/I$. We must show that $f'(ab) = f'(a) \cdot f'(b)$.

Write the residue classes $a, b \in R/I$ as $a = \overline{r}$ and $b = \overline{s}$ for some $r, s \in R$. Then, $ab = \overline{r} \cdot \overline{s} = \overline{rs}$ by the formula (11). Hence, $f'(ab) = f'(\overline{rs}) = f(rs)$ (by the definition of f'). On the other hand, $a = \overline{r}$ and thus $f'(a) = f'(\overline{r}) = f(r)$ (by the definition of f'). Similarly, $f'(b) = f(s)$. Thus,

$$\begin{aligned} f'(ab) = f(rs) &= \underbrace{f(r)}_{=f'(a)} \cdot \underbrace{f(s)}_{=f'(b)} \qquad (\text{since } f \text{ is a ring morphism}) \\ &= f'(a) \cdot f'(b), \end{aligned}$$

which is precisely what we wanted to prove. Thus, Fact 2 is proved as well.

So we have shown that our map $f' : R/I \to S$ is well-defined and is a ring morphism. Thus, Theorem 2.9.5 is proven. □

As we said, the universal property of quotient rings provides a comfortable way to construct ring morphisms out of a quotient ring R/I. The following exercises provide some examples of this:

Exercise 2.9.8. Consider the quotient ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<<3}$ studied in Subsection 2.9.3.

(a) Prove that the map

$$f : \mathbb{Q}^{3\leq 3} \to \mathbb{Q}^{2\times 2},$$
$$\begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & g \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

is a ring morphism.

(b) Prove that this morphism f satisfies $f\left(\mathbb{Q}^{3<<3}\right) = 0$.

(c) Use Theorem 2.9.5 to conclude that there is a ring morphism

$$f' : \mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<<3} \to \mathbb{Q}^{2\times 2},$$
$$\begin{pmatrix} a & b & ? \\ 0 & d & e \\ 0 & 0 & g \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

where the question mark stands for an undetermined entry (as explained in Subsection 2.9.3).

(d) Use a similar reasoning to prove the existence of a ring morphism

$$F' : \mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<<3} \to \mathbb{Q}^{4\times 4},$$
$$\begin{pmatrix} a & b & ? \\ 0 & d & e \\ 0 & 0 & g \end{pmatrix} \mapsto \begin{pmatrix} a & b & 0 & 0 \\ 0 & d & 0 & 0 \\ 0 & 0 & d & e \\ 0 & 0 & 0 & g \end{pmatrix},$$

which is furthermore injective.

(e) Conclude that the ring $\mathbb{Q}^{3\leq 3}/\mathbb{Q}^{3<<3}$ is isomorphic to a subring of $\mathbb{Q}^{4\times 4}$.

Exercise 2.9.9. Solve parts **(a)** and **(b)** of Exercise 2.9.4 again using the universal property of quotient rings. (This should be much quicker than the original solutions.)

Exercise 2.9.10. For every integer m, define a subring R_m of $\mathbb{Q}$ as in Exercise 2.3.2. Consider the quotient ring $R_2/3R_2$.

(a) Prove that the map

$$f_2 : \mathbb{Z} \to R_2/3R_2,$$
$$r \mapsto \overline{r}$$

is a ring morphism that satisfies $f_2(3\mathbb{Z}) = 0$.

(b) Use the universal property of quotient rings to obtain a ring morphism

$$f_2' : \mathbb{Z}/3 \to R_2/3R_2,$$
$$\overline{r} \mapsto \overline{r}.$$

(c) Show that this morphism f_2' is injective.

(d) Show that this morphism f_2' is surjective.

(e) Conclude that $\mathbb{Z}/3\mathbb{Z} \cong R_2/3R_2$ as rings.

(f) More generally, let m and n be two coprime integers. Show that there is a ring isomorphism

$$\mathbb{Z}/n \to R_m/nR_m,$$
$$\overline{r} \mapsto \overline{r}.$$

[**Hint:** Parts **(a)** and **(b)** are almost automatic. Part **(c)** requires showing that an integer r that is not divisible by 3 cannot lie in $3R_2$ either. Argue this using the coprimality of 2 and 3. Part **(d)** boils down to showing that the map f_2' takes $\overline{1/2}$ as a value (why?), but this is easy (why?). Part **(f)** requires generalizing the previous parts, using some properties of coprime integers that we have seen before.]

We have also promised another exercise:

Exercise 2.9.11. Let m and n be two integers. Prove the following:

(a) If $m \mid n$, then there is only one ring morphism $\mathbb{Z}/n \to \mathbb{Z}/m$, and it is the morphism (16).

(b) If $m \nmid n$, then there is no ring morphism $\mathbb{Z}/n \to \mathbb{Z}/m$.

[**Hint:** For part **(a)**, show that every ring morphism $g : \mathbb{Z}/n \to \mathbb{Z}/m$ must satisfy $g(\overline{r}) = \overline{r}$ for each $r \in \mathbb{N}$, since $\overline{r} = r \cdot 1_{\mathbb{Z}/n} = \underbrace{1_{\mathbb{Z}/n} + 1_{\mathbb{Z}/n} + \cdots + 1_{\mathbb{Z}/n}}_{r \text{ times}}$. For part **(b)**, argue that the existence of a ring morphism $g : \mathbb{Z}/n \to \mathbb{Z}/m$ forces $n \cdot 1_{\mathbb{Z}/m} = 0$ because $n \cdot 1_{\mathbb{Z}/n} = 0$.]

2.9.6. The universal property of quotient rings: abstract form

For various reasons, it is helpful to have an alternative formulation of Theorem 2.9.5, which does not refer to specific elements $\overline{r}$ but instead "implicitly" describes the morphism f' by an equality:

Theorem 2.9.6 (Universal property of quotient rings, abstract form)**.** Let R be a ring. Let I be an ideal of R. Consider the canonical projection $\pi : R \to R/I$ (as defined in Theorem 2.9.3).

Let S be a ring. Let $f : R \to S$ be a ring morphism. Assume that $f(I) = 0$ (this is shorthand for saying that $f(a) = 0$ for all $a \in I$). Then, there is a unique ring morphism $f' : R/I \to S$ satisfying $f = f' \circ \pi$.

Proof. Theorem 2.9.5 shows that there is a unique ring morphism $f' : R/I \to S$ that satisfies

$$f'(\overline{r}) = f(r) \qquad \text{for all } r \in R. \tag{17}$$

(Indeed, the equality (17) clearly characterizes f' uniquely, since every element of R/I can be written as $\overline{r}$ for some $r \in R$. What Theorem 2.9.5 gives us is the **existence** of such a morphism f'.)

We shall now prove that the equality $f = f' \circ \pi$ is just an equivalent restatement of the condition (17).

Indeed, we have the following chain of equivalences:

$$\begin{aligned}
&\left(f = f' \circ \pi\right) \\
&\iff \left(f(r) = \left(f' \circ \pi\right)(r) \text{ for all } r \in R\right) \qquad \left(\begin{array}{c}\text{since two maps are equal}\\ \text{if and only if they}\\ \text{agree on each input}\end{array}\right) \\
&\iff \left(f(r) = f'(\pi(r)) \text{ for all } r \in R\right) \qquad \left(\text{since } \left(f' \circ \pi\right)(r) = f'(\pi(r)) \text{ for each } r\right) \\
&\iff \left(f(r) = f'(\overline{r}) \text{ for all } r \in R\right) \qquad \left(\text{since } \pi(r) = \overline{r} \text{ for each } r\right) \\
&\iff \left(f'(\overline{r}) = f(r) \text{ for all } r \in R\right).
\end{aligned}$$

In other words, the equality $f = f' \circ \pi$ is equivalent to the condition (17).

Now, recall that there is a unique ring morphism $f' : R/I \to S$ that satisfies the condition (17). In view of the previous sentence, we can reformulate this as follows: There is a unique ring morphism $f' : R/I \to S$ that satisfies $f = f' \circ \pi$. This proves Theorem 2.9.6. □

For example:

- We can recover the ring morphism $\pi'_3 : \mathbb{Z}/6 \to \mathbb{Z}/3$ constructed in (15) using Theorem 2.9.6 instead of Theorem 2.9.5. Indeed, applying Theorem 2.9.6 to $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $\pi = \pi_6$, $S = \mathbb{Z}/3$ and $f = \pi_3$, we see that there is a unique ring morphism $\pi'_3 : \mathbb{Z}/6 \to \mathbb{Z}/3$ such that $\pi_3 = \pi'_3 \circ \pi_6$ (since $\pi_3(6\mathbb{Z}) = 0$). This morphism π'_3 is, of course, the same as the one in (15), since the equality $\pi_3 = \pi'_3 \circ \pi_6$ says precisely that each integer r satisfies $\pi_3(r) = \pi'_3(\pi_6(r))$, that is, $\overline{r} = \pi'_3(\overline{r})$.

A few more remarks are in order.

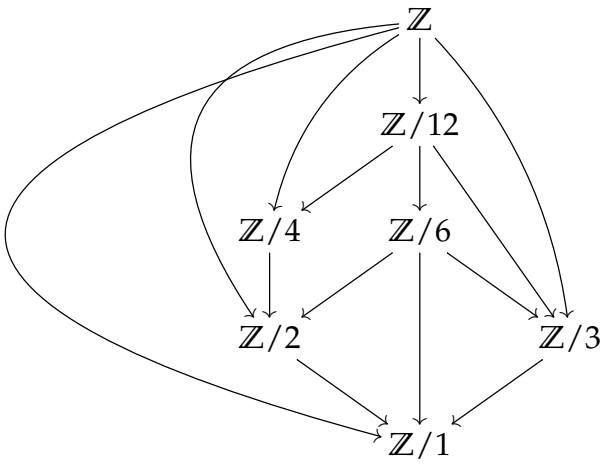
The equality $f = f' \circ \pi$ in Theorem 2.9.6 is oftentimes restated as follows: The diagram

$$\begin{array}{ccc} R & & \\ {\scriptstyle\pi}\downarrow & \searrow^{f} & \\ R/I & \overset{f'}{\dashrightarrow} & S \end{array} \tag{18}$$

commutes. Let me explain what this means: In general, a **diagram** is a bunch of sets and a bunch of maps between them, drawn as nodes and arrows. (Each set is drawn as a node, and each map $g : A \to B$ is drawn as an arrow from the A-node to the B-node.) For instance, the diagram (18) shows the three sets R, R/I and S and the three maps π, f and f'. A diagram is said to **commute** (or **be commutative**) if any two ways of going between two nodes yield the same composed map. In the diagram (18), there are two ways of going from the R-node to the S-node: one direct way (which just uses the f-arrow), and one indirect way via the R/I-mode (using the π-arrow and the f'-arrow). The corresponding composed maps are f (for the direct way) and $f' \circ \pi$ (for the indirect way). This is the only pair of two different ways that go between the same two nodes in the diagram (18); thus, the diagram commutes if and only if $f = f' \circ \pi$.

Note that we have drawn the map f' as a dashed arrow in (18), since this is the map whose existence is claimed, whereas the other two maps are given and thus drawn as regular arrows. This is a common convention and helps you distinguish the things you have from the things you are trying to construct.

In general, diagrams are a good way to visualize situations in which there are several maps going between the same sets. For example, here is a diagram that shows the rings $\mathbb{Z}$, $\mathbb{Z}/12$, $\mathbb{Z}/6$, $\mathbb{Z}/4$, $\mathbb{Z}/3$, $\mathbb{Z}/2$ and $\mathbb{Z}/1$ (the latter ring is trivial) as well as various morphisms between them:



.

In this diagram, all arrows coming out of the $\mathbb{Z}$-node are canonical projections $\mathbb{Z} \to \mathbb{Z}/n$ (sending each $r \in \mathbb{Z}$ to $\overline{r} \in \mathbb{Z}/n$), whereas all the other arrows

are instances of the morphisms (16) constructed above. Note that we have not drawn all possible morphisms (e.g., the morphism $\mathbb{Z}/4 \to \mathbb{Z}/1$ is missing) to avoid crowding the diagram. This diagram commutes, since each of the arrows sends each residue class $\overline{r}$ (or, in the case of $\mathbb{Z}$, each integer r) to the corresponding residue class $\overline{r}$ modulo the respective number.

Commutative diagrams become increasingly useful as you go deeper into algebra (and become ubiquitous when you get to category theory or homological algebra). For us here, they are just convenient visual and mnemonic devices.

2.9.7. Injectivity means zero kernel

Next comes another useful result: a characterization of injectivity in terms of kernels.

Lemma 2.9.7. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then, f is injective if and only if $\operatorname{Ker} f = \{0_R\}$.

Proof. You probably have seen the analogous results for groups or vector spaces. If so, then you can just recall the analogous result for groups, and apply it to the additive groups $(R, +, 0)$ and $(S, +, 0)$ (since the ring morphism f is clearly a group morphism from $(R, +, 0)$ to $(S, +, 0)$).

If not, here is the proof:

$\Longrightarrow$: Assume that f is injective. Then, each $x \in \operatorname{Ker} f$ satisfies $f(x) = 0_S = f(0_R)$ (since f is a ring morphism) and thus $x = 0_R$ because f is injective. In other words, $\operatorname{Ker} f \subseteq \{0_R\}$. But this entails $\operatorname{Ker} f = \{0_R\}$ (since 0_R always lies in $\operatorname{Ker} f$). This proves the "$\Longrightarrow$" direction of Lemma 2.9.7.

$\Longleftarrow$: Assume that $\operatorname{Ker} f = \{0_R\}$. Now, f is a ring morphism and thus respects differences. Hence, if $a, b \in R$ satisfy $f(a) = f(b)$, then $f(a - b) = f(a) - f(b) = 0$ (since $f(a) = f(b)$) and therefore $a - b \in \operatorname{Ker} f = \{0_R\}$, so that $a - b = 0$ and thus $a = b$. But this means that f is injective. This proves the "$\Longleftarrow$" direction of Lemma 2.9.7, and thus completes the proof of the lemma. □

2.9.8. The First Isomorphism Theorem for sets

We now approach another important property of quotient rings: the so-called "first isomorphism theorem".

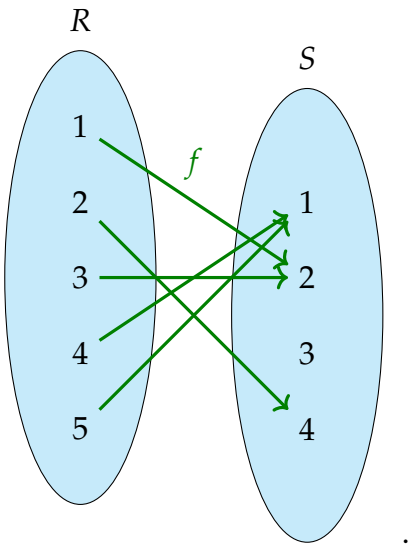
We begin with some basic set theory.

Consider a map $f : R \to S$ from some set R to some set S. Then, I claim that there is a bijection[49] hiding inside f.

What do I mean by this?

[49] "Bijection" means the same as "bijective map" (i.e., a map that is both injective and surjective) and as "1-to-1 correspondence". Also, it is worth recalling that a map is bijective if and only if it is invertible (i.e., has an inverse).

For an example, let $R = \{1,2,3,4,5\}$ and $S = \{1,2,3,4\}$, and let $f : R \to S$ be the map that sends $1,2,3,4,5$ to $2,4,2,1,1$, respectively. Here is an illustration of this map using a standard "blobs and arrows" diagram:



.

As you see, this map f is neither injective nor surjective, thus certainly not bijective. However, I claim that I can **make** it bijective, by appropriately tweaking its domain R and its target S as well as the map f itself. Namely:

- First, I make f surjective. To do so, I replace the target[50] S by the image $f(R) = \{f(r) \mid r \in R\}$ of the map f. This way, I throw away all elements of S that are not taken as values by the map f. The resulting map

$$\begin{aligned} \widetilde{f} : R &\to f(R), \\ r &\mapsto f(r) \end{aligned}$$

  (which differs from f only in its choice of target) is thus surjective.

- Next, I make f (or, more precisely, $\widetilde{f}$) injective. To do so, I equate every pair of elements $a, b \in R$ that satisfy $f(a) = f(b)$. The rigorous way to do so is to replace the elements of R by their equivalence classes with respect to an appropriately chosen equivalence relation. To wit: We define a binary relation $\sim$ on the set R by stipulating that two elements $a, b \in R$ should satisfy $a \sim b$ if and only if $f(a) = f(b)$. This relation $\sim$ is an equivalence relation[51], and its equivalence classes will be called **f-classes**. We will use the notation $\overline{r}$ for the f-class that contains a given element $r \in R$. We let R/f denote the set of all f-classes.

[50] If $g : U \to V$ is a map from a set U to a set V, then V is called the **target** (or **codomain**) of g.

[51] For example, it is transitive because if three elements $a, b, c \in R$ satisfy $f(a) = f(b)$ and $f(b) = f(c)$, then $f(a) = f(b)$.

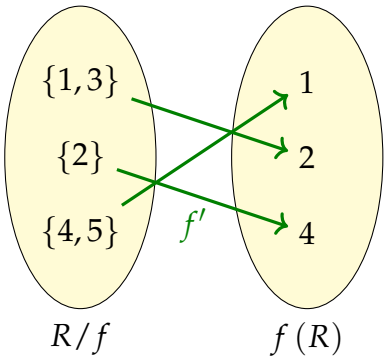
Now, consider the map

$$\begin{aligned} f' : R/f &\to f(R), \\ \overline{r} &\mapsto f(r), \end{aligned}$$

which sends each f-class $\overline{r}$ to the value $f(r)$. This map f' is well-defined, since $f(r)$ depends not on the element r but only on its f-class $\overline{r}$ (because if two elements $a, b \in R/f$ have the same f-class, then $a \sim b$ and thus $f(a) = f(b)$ by the very definition of f).

Just like $\widetilde{f}$, the map f' is surjective (since every element of its target $f(R)$ is taken as a value by f, and thus also by f'). But f' is also injective, since any two elements a, b of R that satisfy $f(a) = f(b)$ have already been merged into the same f-class in R/f. Thus, f' is both injective and surjective, hence bijective.

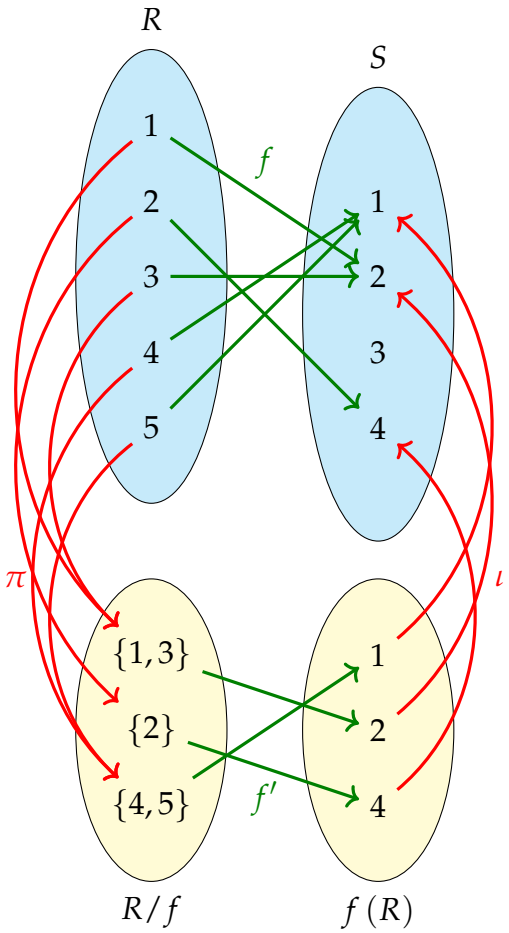
We might call f' the **bijectivization** of f (although there does not seems to be a standard name for f'). In our above example, this map f' looks as follows:



.

Moreover, the maps f and f' fit together into a nice picture with two other

rather natural maps:



.

Here, $\pi : R \to R/f$ is the **canonical projection** (i.e., the map that sends each $r \in R$ to its f-class $\overline{r}$), and $\iota : f(R) \to S$ is the **canonical inclusion** (i.e., the map that sends each $s \in f(R)$ to s). These four maps f, f', π, ι satisfy

$$f = \iota \circ f' \circ \pi,$$

which means (in the language of Subsection 2.9.6) that the diagram

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ R/f & \xrightarrow[f']{} & f(R) \end{array}$$

is commutative.

For the sake of completeness, let us state this all as a theorem:

Theorem 2.9.8 (First Isomorphism Theorem for sets)**.** Let R and S be any two sets, and let $f : R \to S$ be any map.

Let $\sim$ be the binary relation on the set R defined by requiring that two elements $a, b \in R$ satisfy $a \sim b$ if and only if $f(a) = f(b)$.

(a) This relation $\sim$ is an equivalence relation.

Let us refer to the equivalence classes of this equivalence relation $\sim$ as the **f-classes**. Let R/f denote the set of all f-classes. For any $r \in R$, we let $\overline{r}$ denote the f-class that contains r.

(b) The image $f(R) := \{f(r) \mid r \in R\}$ of f is a subset of S.

(c) The map

$$\begin{aligned} f' : R/f &\to f(R), \\ \overline{r} &\mapsto f(r) \end{aligned}$$

is well-defined and bijective.

(d) Let $\pi : R \to R/f$ denote the **canonical projection** (i.e., the map that sends each $r \in R$ to its f-class $\overline{r}$). Let $\iota : f(R) \to S$ denote the **canonical inclusion** (i.e., the map that sends each $s \in f(R)$ to s). Then, the map f' defined in part **(c)** satisfies

$$f = \iota \circ f' \circ \pi.$$

In other words, the diagram

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ R/f & \xrightarrow[f']{} & f(R) \end{array} \tag{19}$$

is commutative.

Proof. Part **(b)** is obvious. We explained the proofs of parts **(a)** and **(c)** before even stating this theorem. Just for the sake of completeness, we shall now repeat the proof of part **(c)**, and then prove part **(d)**:

(c) If $a, b \in R$ are two elements satisfying $\overline{a} = \overline{b}$, then $f(a) = f(b)$ [52]. In other words, for any element $r \in R$, the value $f(r)$ depends only on the f-class

[52] *Proof.* Let $a, b \in R$ be two elements satisfying $\overline{a} = \overline{b}$. The equality $\overline{a} = \overline{b}$ shows that a and b belong to the same f-class (since $\overline{a}$ denotes the f-class that contains a, whereas $\overline{b}$ denotes the f-class that contains b). In other words, a and b belong to the same equivalence class of the

$\overline{r}$ and not on r itself. Hence, the map

$$f' : R/f \to f(R), \\ \overline{r} \mapsto f(r)$$

is well-defined (since each element of R/f can be written as $\overline{r}$ for some $r \in R$). It remains to prove that this map is bijective. To that purpose, we shall now prove that it is injective and surjective.

Injectivity: Let $x, y \in R/f$ be two elements of R/f satisfying $f'(x) = f'(y)$. We shall prove that $x = y$.

We know that x is an element of R/f. In other words, x is an f-class (since R/f is the set of all f-classes). Thus, we can write x in the form $x = \overline{a}$ for some $a \in R$. Likewise, we can write y in the form $y = \overline{b}$ for some $b \in R$. Consider these a and b.

From $x = \overline{a}$, we obtain $f'(x) = f'(\overline{a}) = f(a)$ (by the definition of f'). Similarly, $f'(y) = f(b)$ (since $y = \overline{b}$). Hence, $f(a) = f'(x) = f'(y) = f(b)$. In other words, $a \sim b$ (by the definition of the relation $\sim$). In other words, a and b belong to the same equivalence class of the equivalence relation $\sim$. In other words, a and b belong to the same f-class (since the f-classes are the equivalence classes of this equivalence relation $\sim$). In other words, $\overline{a} = \overline{b}$ (since $\overline{a}$ denotes the f-class that contains a, whereas $\overline{b}$ denotes the f-class that contains b). In other words, $x = y$ (since $x = \overline{a}$ and $y = \overline{b}$).

Forget that we fixed x and y. We thus have shown that if $x, y \in R/f$ are two elements of R/f satisfying $f'(x) = f'(y)$, then $x = y$. In other words, the map f' is injective.

Surjectivity: Let $z \in f(R)$. Thus, $z = f(r)$ for some $r \in R$. Now, the f-class $\overline{r} \in R/f$ satisfies $f'(\overline{r}) = f(r)$ (by the definition of f'). Comparing this with $z = f(r)$, we obtain $z = f'(\overline{r})$. This shows that the map f' takes z as a value.

Forget that we fixed z. We thus have shown that the map f' takes each $z \in f(R)$ as a value. In other words, the map f' is surjective.

We now have proved that f' is injective and surjective. Thus, f' is bijective, and the proof of Theorem 2.9.8 **(c)** is complete.

(d) For each $r \in R$, we have

$$\begin{aligned}
&\left(\iota \circ f' \circ \pi\right)(r) \\
&= \iota\left(f'(\pi(r))\right) \\
&= f'(\pi(r)) \qquad \text{(since the definition of } \iota \text{ yields } \iota(s) = s \text{ for each } s \in f(R)\text{)} \\
&= f'(\overline{r}) \qquad \text{(since the definition of } \pi \text{ yields } \pi(r) = \overline{r}\text{)} \\
&= f(r) \qquad \left(\text{by the definition of } f'\right).
\end{aligned}$$

In other words, $\iota \circ f' \circ \pi = f$. Thus, $f = \iota \circ f' \circ \pi$. In other words, the diagram (19) is commutative. This proves Theorem 2.9.8 **(d)**. □

equivalence relation $\sim$ (since the f-classes are the equivalence classes of this equivalence relation $\sim$). In other words, $a \sim b$. In other words, $f(a) = f(b)$ (by the definition of the relation $\sim$).

2.9.9. The First Isomorphism Theorem for rings

Now, let us extend the First Isomorphism Theorem to rings and ring morphisms instead of arbitrary sets and maps.

Theorem 2.9.9 (First Isomorphism Theorem for rings, elementwise form)**.** Let R and S be two rings, and let $f : R \to S$ be a ring morphism. Then:

(a) The kernel $\operatorname{Ker} f$ is an ideal of R. Thus, $R/\operatorname{Ker} f$ is a quotient ring of R. As a set, $R/\operatorname{Ker} f$ is precisely the set R/f defined in Theorem 2.9.8. The f-classes (as defined in Theorem 2.9.8) are precisely the cosets of $\operatorname{Ker} f$.

(b) The image $f(R) := \{f(r) \mid r \in R\}$ of f is a subring of S.

(c) The map

$$\begin{aligned} f' : R/\operatorname{Ker} f &\to f(R), \\ \overline{r} &\mapsto f(r) \end{aligned}$$

is well-defined and is a ring isomorphism.

(d) This map f' is precisely the map f' defined in Theorem 2.9.8 **(c)**.

(e) Let $\pi : R \to R/\operatorname{Ker} f$ denote the **canonical projection** (i.e., the map that sends each $r \in R$ to its coset $\overline{r}$). Let $\iota : f(R) \to S$ denote the **canonical inclusion** (i.e., the map that sends each $s \in f(R)$ to s). Then, the map f' defined in part **(c)** satisfies

$$f = \iota \circ f' \circ \pi.$$

In other words, the diagram

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ R/\operatorname{Ker} f & \xrightarrow[f']{} & f(R) \end{array} \tag{20}$$

is commutative.

(f) We have $R/\operatorname{Ker} f \cong f(R)$ as rings.

Proof. **(a)** We know that $\operatorname{Ker} f$ is an ideal of R (by Theorem 2.8.4), and therefore $R/\operatorname{Ker} f$ is a quotient ring of R.

Let us next prove that the f-classes (as defined in Theorem 2.9.8) are precisely the cosets of $\operatorname{Ker} f$.

Indeed, let $\sim$ be the equivalence relation on R defined in Theorem 2.9.8. Then, the f-classes are defined as the equivalence classes of this relation $\sim$. For any $a, b \in R$, we have $f(b) - f(a) = f(b-a)$ (since f is a ring morphism and thus respects differences). For any two elements $a, b \in R$, we have the chain of equivalences

$$\begin{aligned}
& (a \sim b) \\
\iff & (f(a) = f(b)) && \text{(by the definition of } \sim\text{)} \\
\iff & (f(b) - f(a) = 0) \\
\iff & (f(b-a) = 0) && \text{(since } f(b) - f(a) = f(b-a)\text{)} \\
\iff & (b - a \in \operatorname{Ker} f) && \text{(by the definition of } \operatorname{Ker} f\text{)}.
\end{aligned}$$

However, if $a \in R$ is arbitrary, then

$$\begin{aligned}
& (\text{the } f\text{-class that contains } a) \\
& = (\text{the equivalence class of the relation } \sim \text{ that contains } a) \\
& \qquad\qquad (\text{since the } f\text{-classes are the equivalence classes of } \sim) \\
& = \{b \in R \mid a \sim b\} \qquad (\text{by the definition of equivalence classes}) \\
& = \{b \in R \mid b - a \in \operatorname{Ker} f\} \\
& \qquad\qquad \left(\begin{array}{c} \text{by the equivalence } (a \sim b) \iff (b - a \in \operatorname{Ker} f) \\ \text{that we proved above} \end{array} \right) \\
& = \{b \in R \mid b \in a + \operatorname{Ker} f\} \\
& = a + \operatorname{Ker} f \\
& = (\text{the coset of } \operatorname{Ker} f \text{ that contains } a)
\end{aligned}$$

(since the coset of $\operatorname{Ker} f$ that contains a is $a + \operatorname{Ker} f$ by definition). Thus, the f-classes are precisely the cosets of $\operatorname{Ker} f$.

In other words, the cosets of $\operatorname{Ker} f$ are precisely the f-classes. Hence, the set $R/\operatorname{Ker} f$ is precisely the set R/f (since the former set consists of the cosets of $\operatorname{Ker} f$, while the latter set consists of the f-classes). This concludes the proof of Theorem 2.9.9 **(a)**.

(b) This is just Proposition 2.7.6.

(c) Theorem 2.9.9 **(a)** yields that $R/f = R/\operatorname{Ker} f$, and that the f-classes are precisely the cosets of $\operatorname{Ker} f$. Hence, the meaning of the notation $\overline{r}$ in Theorem 2.9.8 is identical with the meaning of this notation in Theorem 2.9.9 (indeed, the former denotes the f-class that contains r, whereas the latter denotes the coset of $\operatorname{Ker} f$ that contains r; but as we just said, the f-classes are precisely the cosets of $\operatorname{Ker} f$). Hence, Theorem 2.9.8 **(c)** shows that the map

$$\begin{aligned}
f' : R/f &\to f(R), \\
\overline{r} &\mapsto f(r)
\end{aligned}$$

is well-defined and bijective. Since $R/f = R/\operatorname{Ker} f$ (as sets), we can restate this as follows: The map

$$\begin{aligned} f' : R/\operatorname{Ker} f &\to f(R), \\ \overline{r} &\mapsto f(r) \end{aligned}$$

is well-defined and bijective. It remains to prove that this map f' is a ring isomorphism.

We shall first show that f' is a ring morphism. Indeed, this is an easy consequence of Theorem 2.9.5 (applied to $I = \operatorname{Ker} f$), since we have $f(\operatorname{Ker} f) = 0$ (by the definition of $\operatorname{Ker} f$). Alternatively, we can prove this by hand as follows:

We must show that f' is a ring morphism, i.e., that f' respects addition, multiplication, zero and unity.

To see that f' respects multiplication, we must show that $f'(xy) = f'(x) \cdot f'(y)$ for any $x, y \in R/\operatorname{Ker} f$. So let $x, y \in R/\operatorname{Ker} f$ be arbitrary. Then, we can write x and y as $x = \overline{a}$ and $y = \overline{b}$ for two elements $a, b \in R$. Consider these a, b. From $x = \overline{a}$ and $y = \overline{b}$, we obtain $xy = \overline{a} \cdot \overline{b} = \overline{ab}$ (by the definition of the product on $R/\operatorname{Ker} f$), so that

$$\begin{aligned} f'(xy) &= f'\left(\overline{ab}\right) = f(ab) && \left(\text{by the definition of } f'\right) \\ &= f(a) \cdot f(b) && \left(\text{since } f \text{ is a ring morphism}\right). \end{aligned}$$

Comparing this with

$$f'\left(\underbrace{x}_{=\overline{a}}\right) \cdot f'\left(\underbrace{y}_{=\overline{b}}\right) = \underbrace{f'(\overline{a})}_{\substack{=f(a) \\ \text{(by the} \\ \text{definition of } f')}} \cdot \underbrace{f'\left(\overline{b}\right)}_{\substack{=f(b) \\ \text{(by the} \\ \text{definition of } f')}} = f(a) \cdot f(b),$$

we obtain $f'(xy) = f'(x) \cdot f'(y)$, just as desired. Thus, we have shown that f' respects multiplication. Similarly, f' satisfies all the other axioms in the definition of a ring morphism.

Thus, we know that f' is a ring morphism. Since f' is also invertible (because f' is bijective), we conclude that f' is an invertible ring morphism. Thus, f' is a ring isomorphism (since Proposition 2.7.7 shows that any invertible ring morphism is a ring isomorphism). Thus, the proof of Theorem 2.9.9 **(c)** is finished.

(d) As we have seen in our above proof of Theorem 2.9.9 **(c)**, we have $R/f = R/\operatorname{Ker} f$, and the meaning of the notation $\overline{r}$ in Theorem 2.9.8 is identical with the meaning of this notation in Theorem 2.9.9. Thus, the map f' in Theorem 2.9.9 **(c)** is precisely the map f' defined in Theorem 2.9.8 **(c)**. This proves Theorem 2.9.9 **(d)**.

(e) As we have seen in our above proof of Theorem 2.9.9 **(c)**, we have $R/f = R/\operatorname{Ker} f$, and the meaning of the notation $\overline{r}$ in Theorem 2.9.8 is identical with the meaning of this notation in Theorem 2.9.9. Therefore, the maps π and ι defined in Theorem 2.9.9 **(e)** are precisely the maps π and ι in Theorem 2.9.8 **(e)**. Hence, the claim of Theorem 2.9.9 **(e)** follows immediately from Theorem 2.9.8 **(e)** (since $R/f = R/\operatorname{Ker} f$).

(f) This follows directly from Theorem 2.9.9 **(c)**. □

As our proof has shown, Theorem 2.9.9 **(c)** is merely a partial improvement on the universal property of quotient rings (Theorem 2.9.5): The latter yields a ring morphism, while the former produces a ring **iso**morphism (but in a less general setup: $R/\operatorname{Ker} f$ instead of R/I). Nevertheless, it is a useful result, as it can be used to identify certain quotient rings as (isomorphic copies of) known rings.

Here are some examples for what can be done with the first isomorphism theorem:

- Consider the map[53]

$$f : \mathbb{Q}^{4\leq 4} \to \mathbb{Q}^{2\leq 2},$$
$$\begin{pmatrix} a & b & c & d \\ 0 & u & v & w \\ 0 & 0 & x & y \\ 0 & 0 & 0 & z \end{pmatrix} \mapsto \begin{pmatrix} u & v \\ 0 & x \end{pmatrix},$$

  which removes the "outer shell" (i.e., the first and the fourth rows and columns) from an upper-triangular 4×4-matrix. This map f is a ring morphism[54].

[53] See Subsection 2.3.2 for the meaning of the notation $\mathbb{Q}^{n\leq n}$ (and, more generally, $R^{n\leq n}$ when R is any ring).

[54] Proving this is a nice exercise in matrix multiplication! It is obvious that f respects addition, zero and unity, but you might be skeptical that it respects multiplication. (And indeed, the analogous map

$$F : \mathbb{Q}^{4\times 4} \to \mathbb{Q}^{2\times 2},$$
$$\begin{pmatrix} a & b & c & d \\ a' & b' & c' & d' \\ a'' & b'' & c'' & d'' \\ a''' & b''' & c''' & d''' \end{pmatrix} \mapsto \begin{pmatrix} b' & c' \\ b'' & c'' \end{pmatrix},$$

which removes the "outer shell" from an arbitrary (not upper-triangular) 4×4-matrix, does not respect multiplication.) You can convince yourself of this property of f by a straightfor-

The kernel of this morphism f is

$$\begin{aligned}\operatorname{Ker} f &= \left\{ \begin{pmatrix} a & b & c & d \\ 0 & u & v & w \\ 0 & 0 & x & y \\ 0 & 0 & 0 & z \end{pmatrix} \in \mathbb{Q}^{4\leq 4} \;\mid\; \begin{pmatrix} u & v \\ 0 & x \end{pmatrix} = 0 \right\} \\ &= \left\{ \begin{pmatrix} a & b & c & d \\ 0 & u & v & w \\ 0 & 0 & x & y \\ 0 & 0 & 0 & z \end{pmatrix} \in \mathbb{Q}^{4\leq 4} \;\mid\; u = v = x = 0 \right\} \\ &= \left\{ \begin{pmatrix} a & b & c & d \\ 0 & 0 & 0 & w \\ 0 & 0 & 0 & y \\ 0 & 0 & 0 & z \end{pmatrix} \in \mathbb{Q}^{4\leq 4} \right\}.\end{aligned}$$

So you can conclude right away that $\operatorname{Ker} f$ is an ideal of $\mathbb{Q}^{4\leq 4}$. Moreover, the image $f\left(\mathbb{Q}^{4\leq 4}\right)$ is the whole $\mathbb{Q}^{2\leq 2}$ (that is, the map f is surjective).

The First Isomorphism theorem (Theorem 2.9.9 **(c)**) yields a ring isomorphism

$$\begin{aligned} f' : \mathbb{Q}^{4\leq 4} / \operatorname{Ker} f &\to f\left(\mathbb{Q}^{4\leq 4}\right), \\ \overline{r} &\mapsto f(r). \end{aligned}$$

In other words, it yields a ring isomorphism

$$\begin{aligned} f' : \mathbb{Q}^{4\leq 4} / \operatorname{Ker} f &\to \mathbb{Q}^{2\leq 2}, \\ \overline{\begin{pmatrix} a & b & c & d \\ 0 & u & v & w \\ 0 & 0 & x & y \\ 0 & 0 & 0 & z \end{pmatrix}} &\mapsto \begin{pmatrix} u & v \\ 0 & x \end{pmatrix} \end{aligned}$$

(since $f\left(\mathbb{Q}^{4\leq 4}\right) = \mathbb{Q}^{2\leq 2}$). In particular, $\mathbb{Q}^{4\leq 4} / \operatorname{Ker} f \cong \mathbb{Q}^{2\leq 2}$.

---

ward computation:

$$\begin{pmatrix} a & b & c & d \\ 0 & u & v & w \\ 0 & 0 & x & y \\ 0 & 0 & 0 & z \end{pmatrix} \begin{pmatrix} a' & b' & c' & d' \\ 0 & u' & v' & w' \\ 0 & 0 & x' & y' \\ 0 & 0 & 0 & z' \end{pmatrix} = \begin{pmatrix} aa' & ab'+bu' & ac'+bv'+cx' & ad'+bw'+cy'+dz' \\ 0 & uu' & uv'+vx' & uw'+vy'+wz' \\ 0 & 0 & xx' & xy'+yz' \\ 0 & 0 & 0 & zz' \end{pmatrix}$$

(note the uu', $uv'+vx'$, 0 and xx' entries, which are precisely the entries of $\begin{pmatrix} u & v \\ 0 & x \end{pmatrix} \begin{pmatrix} u' & v' \\ 0 & x' \end{pmatrix}$).

- We have not properly defined polynomials yet, but once we will, you will be inundated with good examples for the First Isomorphism Theorem. Many of these examples will have the form

$$(\text{a polynomial ring}) \,/\, (\text{an ideal}) \cong (\text{a ring of numbers}).$$

For instance, recalling that $\mathbb{R}[x]$ is the ring of all polynomials in one indeterminate x with real coefficients, we have a ring morphism

$$\begin{aligned} f : \mathbb{R}[x] &\to \mathbb{C}, \\ p &\mapsto p(i) \end{aligned}$$

(which sends each polynomial $p \in \mathbb{R}[x]$ to its value at the imaginary unit $i = \sqrt{-1}$). This morphism is surjective (that is, $f(\mathbb{R}[x]) = \mathbb{C}$) and has kernel $\operatorname{Ker} f = \left(x^2+1\right)\mathbb{R}[x]$ (the principal ideal generated by x^2+1), so that the First Isomorphism theorem (Theorem 2.9.9 **(f)**) yields

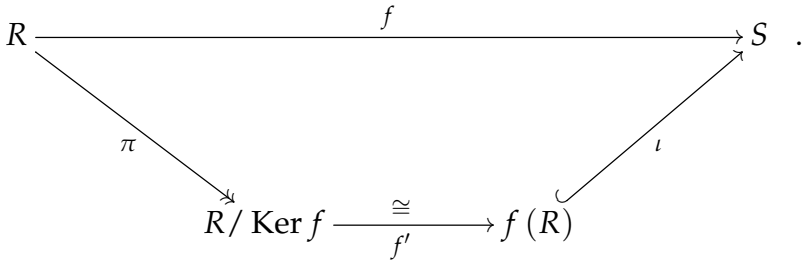
$$\mathbb{R}[x] \,/\, \left(\left(x^2+1\right)\mathbb{R}[x]\right) \cong \mathbb{C}.$$

Informally, this is saying that if you are working with polynomials in an indeterminate x over $\mathbb{R}$, but you equate the polynomial x^2+1 to zero (that is, you pretend that $x^2 = -1$), then you obtain the complex numbers. This is the rigorous concept behind the classical idea that "the complex numbers are what you get if you start with the real numbers and adjoin a root of the polynomial x^2+1". We will make this precise in a later chapter.

2.9.10. A few remarks on the first isomorphism theorem

Theorem 2.9.9 (specifically, its parts **(c)** and **(e)**) is commonly called the **first isomorphism theorem for rings**, and is one of the major sources of ring isomorphisms in some parts of abstract algebra. Due to its importance, a few more comments on it are worth making.

The commutative diagram (20) in Theorem 2.9.9 **(e)** can be rewritten in a somewhat more expressive form:



Let me explain what you are seeing here: On top is the original ring morphism $f : R \to S$. The other four arrows are

- the canonical projection $\pi : R \to R/\operatorname{Ker} f$, sending each $r \in R$ to its residue class $\overline{r} = r + \operatorname{Ker} f \in R/\operatorname{Ker} f$;
- the canonical inclusion $\iota : f(R) \to S$ (which just sends each element to itself);
- the morphism $f' : R/\operatorname{Ker} f \to f(R)$ claimed by Theorem 2.9.9 **(c)**.

The special shapes of the arrows signify certain properties:

- An arrow of shape $\hookrightarrow$ stands for an injective map. (And indeed, the canonical inclusion $\iota : f(R) \to S$ is injective.)
- An arrow of shape $\twoheadrightarrow$ stands for a surjective map. (And indeed, the canonical projection π is surjective.)
- An arrow with a $\cong$ sign above (or below) it stands for an isomorphism. (And indeed, our f' is an isomorphism.)

Note that all four arrows in our diagram are ring morphisms; we thus say that our diagram is a **diagram of rings**.

Thus, the first isomorphism theorem for rings shows that each ring morphism can be decomposed (in a natural way) into a composition of a surjective ring morphism, a ring isomorphism and an injective ring morphism.

In Theorem 2.9.9 **(c)**, we have defined our isomorphism f' explicitly. Alternatively, it can be characterized (uniquely) by the equation $f = \iota \circ f' \circ \pi$ stated in Theorem 2.9.9 **(e)**:

Theorem 2.9.10 (First isomorphism theorem for rings, abstract form)**.** Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Recall that $\operatorname{Ker} f$ is an ideal of R, and that $\operatorname{Im} f = f(R)$ is a subring of S. Then:

(a) There is a unique ring morphism $f' : R/\operatorname{Ker} f \to f(R)$ that satisfies the equation $f = \iota \circ f' \circ \pi$ (that is, for which the diagram (20) is commutative).

(b) This morphism f' is a ring isomorphism:

Proof. **(a)** Theorem 2.9.9 **(e)** shows that the ring isomorphism $f' : R/\operatorname{Ker} f \to f(R)$ constructed in Theorem 2.9.9 **(c)** satisfies the equation $f = \iota \circ f' \circ \pi$. Hence, there exists **at least one** ring morphism $f' : R/\operatorname{Ker} f \to f(R)$ that satisfies the equation $f = \iota \circ f' \circ \pi$ (namely, the isomorphism f' we were just talking about). It thus remains to prove that this morphism f' is unique.

To show this, we consider an arbitrary ring morphism $f' : R/\operatorname{Ker} f \to f(R)$ that satisfies the equation $f = \iota \circ f' \circ \pi$. Then, for any $r \in R$, we have

$$\begin{aligned} f(r) &= \left(\iota \circ f' \circ \pi\right)(r) && \left(\text{since } f = \iota \circ f' \circ \pi\right) \\ &= \iota\left(f'(\pi(r))\right) \\ &= f'(\pi(r)) && (\text{since the definition of } \iota \text{ yields } \iota(s) = s \text{ for each } s \in S) \\ &= f'(\overline{r}) && (\text{since the definition of } \pi \text{ yields } \pi(r) = \overline{r}) \end{aligned}$$

and thus $f'(\overline{r}) = f(r)$. Thus, f' must be the map

$$\begin{aligned} R/\operatorname{Ker} f &\to f(R), \\ \overline{r} &\mapsto f(r), \end{aligned}$$

which has been called f' in Theorem 2.9.9 **(c)**. In particular, there is only one option for f'. Thus, we have shown that f' is unique, and the proof of Theorem 2.9.10 **(a)** is complete.

(b) As we explained above, the unique ring morphism $f' : R/\operatorname{Ker} f \to f(R)$ that satisfies the equation $f = \iota \circ f' \circ \pi$ is precisely the map that was called f' in Theorem 2.9.9 **(c)**. But the latter map is a ring isomorphism (by Theorem 2.9.9 **(c)**). Hence, Theorem 2.9.10 **(b)** follows. □

There are also second, third and fourth isomorphism theorems. You will meet them in Section 2.17.

2.10. Direct products of rings ([DumFoo04, §7.6])

2.10.1. Direct products of two rings

Here is a way of building new rings from old[55]:

Proposition 2.10.1. Let R and S be two rings. Then, the Cartesian product

$$R \times S = \{\text{all pairs } (r,s) \text{ with } r \in R \text{ and } s \in S\}$$

becomes a ring if we endow it with the entrywise addition and multiplication operations (i.e., addition defined by $(r,s) + (r',s') = (r+r', s+s')$, and multiplication defined by $(r,s) \cdot (r',s') = (rr', ss')$) and the zero $(0_R, 0_S)$ and the unity $(1_R, 1_S)$.

Definition 2.10.2. This ring is denoted by $R \times S$ and is called the **direct product** of R and S.

[55] There are several other such ways. We will see a few in this course.

Proof of Proposition 2.10.1. We must check that the ring axioms are satisfied for $R \times S$. Each one is straightforward to verify. For example, in order to check the associativity of multiplication, we need to check that

$$(r,s)\left((r',s')\left(r'',s''\right)\right) = \left((r,s)\left(r',s'\right)\right)\left(r'',s''\right) \quad \text{for all } (r,s), \left(r',s'\right), \left(r'',s''\right) \in R \times S$$

(because any element of $R \times S$ is a pair). We can do this by computing both sides and comparing: We have

$$(r,s)\left((r',s')\left(r'',s''\right)\right) = (r,s)\left(r'r'',s's''\right) = \left(r\left(r'r''\right),s\left(s's''\right)\right) \quad \text{and}$$
$$\left((r,s)\left(r',s'\right)\right)\left(r'',s''\right) = \left(rr',ss'\right)\left(r'',s''\right) = \left(\left(rr'\right)r'',\left(ss'\right)s''\right).$$

The right hand sides of these two equalities are equal, since $r\left(r'r''\right) = \left(rr'\right)r''$ and $s\left(s's''\right) = \left(ss'\right)s''$. Thus, the left hand sides are equal as well; this proves the associativity of multiplication. All other ring axioms follow similarly. □

2.10.2. Direct products of any number of rings

More generally, we can define the direct product $R_1 \times R_2 \times \cdots \times R_n$ of any number of rings in the same way (but using n-tuples instead of pairs). Even more generally, we can define the direct product $\prod_{i \in I} R_i$ of any family of rings (including infinite families).

To do so, we recall the notion of a "family":

A **family** is a collection of objects (the "entries" of the family) indexed by the elements of a given set I (the "indexing set"). To be more specific: A **family** indexed by a set I means a way of assigning some object x_i to each element $i \in I$. This family is denoted by $(x_i)_{i \in I}$ (pronounced "the family consisting of x_i for each $i \in I$"), and the set I is called its **indexing set**, whereas the objects x_i are called the **entries** of this family.[56] Two families $(x_i)_{i \in I}$ and $(y_i)_{i \in I}$ are considered to be equal if each $i \in I$ satisfies $x_i = y_i$.

For example, the family $(\mathbb{Z}/n)_{n \in \mathbb{N}}$ consists of all the quotient rings $\mathbb{Z}/n$ of the ring $\mathbb{Z}$ with $n \in \mathbb{N}$. Its indexing set is $\mathbb{N}$, and its entries are the quotient rings $\mathbb{Z}/n$. For another example, the family $\left(n^2\right)_{n \in \mathbb{N}}$ consists of the squares of all nonnegative integers n. Its indexing set is $\mathbb{N}$, and its entries are the squares n^2.

The notion of a family encompasses several well-known mathematical concepts:

- n-tuples: If $I = \{1, 2, \ldots, n\}$, then a family $(x_i)_{i \in I}$ is the n-tuple $(x_1, x_2, \ldots, x_n)$.
- infinite sequences: If $I = \mathbb{N} = \{0, 1, 2, \ldots\}$, then a family $(x_i)_{i \in I}$ is the sequence $(x_0, x_1, x_2, \ldots)$.

[56] Programmers know families under the name "dictionaries" or "associative arrays" (although the indexing set I is usually finite in any real-life programming situation).

- sequences infinite on both sides: If $I = \mathbb{Z}$, then a family $(x_i)_{i \in I}$ is the "infinite-on-both-sides sequence" $(\ldots, x_{-2}, x_{-1}, x_0, x_1, x_2, \ldots)$.
- maps (i.e., functions): If I and R are any two sets, then a map $f : I \to R$ can be viewed as a family $(f(i))_{i \in I}$ whose entries are the values of f. (Fine print: The family $(f(i))_{i \in I}$ does not "know" the set R, so it does not fully represent the map f.)

Now, if $(X_i)_{i \in I}$ is a family of sets (i.e., if X_i is a set for each $i \in I$), then the **Cartesian product** $\prod_{i \in I} X_i$ of these sets is defined to be the set of all families $(x_i)_{i \in I}$ that satisfy $x_i \in X_i$ for each $i \in I$. For instance, an element of the Cartesian product $\prod_{n \in \mathbb{N}} (\mathbb{Z}/n)$ is a family $(x_n)_{n \in \mathbb{N}}$, where each x_n is a residue class in the corresponding ring $\mathbb{Z}/n$.

We are now ready to define the direct product $\prod_{i \in I} R_i$ of an arbitrary family of rings:

Proposition 2.10.3. Let I be any set. Let $(R_i)_{i \in I}$ be a family of rings (i.e., let R_i be a ring for each $i \in I$). Then, the Cartesian product

$$\prod_{i \in I} R_i = \left\{\text{all families } (r_i)_{i \in I} \text{ with } r_i \in R_i \text{ for each } i \in I\right\}$$

becomes a ring if we endow it with the entrywise addition and multiplication operations (i.e., addition defined by $(r_i)_{i \in I} + (s_i)_{i \in I} = (r_i + s_i)_{i \in I}$, and multiplication defined by $(r_i)_{i \in I} \cdot (s_i)_{i \in I} = (r_i s_i)_{i \in I}$) and the zero $\left(0_{R_i}\right)_{i \in I}$ and the unity $\left(1_{R_i}\right)_{i \in I}$.

Definition 2.10.4. The ring defined in Proposition 2.10.3 is denoted by $\prod_{i \in I} R_i$ and is called the **direct product** of the rings R_i. In some special cases, there are alternative notations for it:

- If $I = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$, then the ring $\prod_{i \in I} R_i$ is also denoted by $R_1 \times R_2 \times \cdots \times R_n$, and we identify each family $(r_i)_{i \in I} = (r_i)_{i \in \{1,2,\ldots,n\}}$ with the n-tuple $(r_1, r_2, \ldots, r_n)$. (Thus, the elements of $R_1 \times R_2 \times \cdots \times R_n$ are n-tuples whose entries belong to $R_1, R_2, \ldots, R_n$, respectively.) In particular, for $n = 2$, this recovers the definition of $R \times S$ in Definition 2.10.2.
- If all the rings R_i are equal to some ring R, then their direct product $\prod_{i \in I} R_i = \prod_{i \in I} R$ is also denoted R^I. Note that this is the same notation that we previously used for the ring of all functions from I to R (with pointwise addition and multiplication); however, these two notations

don't really clash, since these two rings are the same (at least if we identify a function $f : I \to R$ with the family $(f(i))_{i \in I}$). (Pointwise addition/multiplication of functions corresponds precisely to entrywise addition/multiplication in the direct product $\prod_{i \in I} R$.)

- If $n \in \mathbb{N}$, and if R is a ring, then the ring $R^{\{1,2,\ldots,n\}} = \underbrace{R \times R \times \cdots \times R}_{n \text{ times}}$ is also called R^n.

2.10.3. Examples

Here are some examples of direct products:

- The ring $\mathbb{Z}^3 = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ consists of all triples (r, s, t) of integers. They are added and multiplied entrywise: i.e., we have

$$(r, s, t) + (r', s', t') = (r + r', s + s', t + t') \qquad \text{and}$$
$$(r, s, t) \cdot (r', s', t') = (rr', ss', tt').$$

  Note that this ring is **not** an integral domain, since $(0, 1, 0) \cdot (1, 0, 0) = (0, 0, 0)$. Generally, direct products of rings are never integral domains, unless all but one factors are trivial rings.

- If R, S and T are three rings, then the direct products $R \times S \times T$ and $(R \times S) \times T$ are not quite the same (e.g., the former consists of triples (r, s, t), while the latter consists of nested pairs $((r, s), t)$); but they are isomorphic through a rather obvious isomorphism: Namely, the map

$$R \times S \times T \to (R \times S) \times T,$$
$$(r, s, t) \mapsto ((r, s), t)$$

  is a ring isomorphism. This is a quick test of understanding – if you understand the definitions, then this should be completely obvious to you. Similarly, the rings $R \times S \times T$ and $R \times (S \times T)$ are isomorphic. You can easily generalize this to direct products of more than three rings. We say that the direct product of rings is "associative up to isomorphism".

- Likewise, the direct product of rings is "commutative up to isomorphism": That is, if R and S are two rings, then the map

$$R \times S \to S \times R,$$
$$(r, s) \mapsto (s, r)$$

  is a ring isomorphism.

- The ring $\mathbb{C}$ consists of complex numbers, which are defined as pairs of real numbers (the real part and the imaginary part). Thus, $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ as sets. Since complex numbers are added entrywise, we even have $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ as additive groups (i.e., the additive groups $(\mathbb{C}, +, 0)$ and $(\mathbb{R} \times \mathbb{R}, +, 0)$ are identical). However, $\mathbb{C}$ is **not** $\mathbb{R} \times \mathbb{R}$ as rings (because complex numbers are not multiplied entrywise). Even worse, $\mathbb{C}$ is not even isomorphic to $\mathbb{R} \times \mathbb{R}$ as rings. One way to see this is by noticing that $\mathbb{C}$ is an integral domain (even a field) whereas $\mathbb{R} \times \mathbb{R}$ is not (for example, $(1,0) \cdot (0,1) = (0,0)$). Another way to see this is by noticing that $-1_{\mathbb{C}}$ is a square in $\mathbb{C}$, but $-1_{\mathbb{R}\times\mathbb{R}} = (-1,-1)$ is not a square in $\mathbb{R} \times \mathbb{R}$.

  Note that these arguments make sense because of the "isomorphism principle" (which we stated in Subsection 2.7.4). We recall that this principle says that isomorphic rings "behave the same" as far as their properties are concerned – at least those properties that can be stated in terms of the ring itself. For example, if R and S are two isomorphic rings, and if one of R and S is a field, then so is the other. For yet another example, if R and S are two isomorphic rings, and R has (say) 15 units, then so does S. For yet another example, if R and S are two isomorphic rings, and R satisfies some property like "$x\,(x+1_R)\,(x-1_R) = 0$ for all $x \in R$", then so does S (with 1_R replaced by 1_S). The only properties of a ring that are not preserved under isomorphism are properties that refer to specific "outside" objects (for example, the rings $R \times S$ and $S \times R$ from the previous example are isomorphic, but they generally contain different elements). This all is a general feature of isomorphisms of any sorts of objects – not just of rings but also of groups, vector spaces and topological spaces.

- Let R be any ring. Let $n \in \mathbb{N}$. Let $R^{n=n}$ be the set of all **diagonal** matrices in the matrix ring $R^{n\times n}$. In other words,

$$\begin{aligned} R^{n=n} &= \left\{ \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix} \;\mid\; a_1, a_2, \ldots, a_n \in R \right\} \\ &= \left\{ \operatorname{diag}(a_1, a_2, \ldots, a_n) \;\mid\; a_1, a_2, \ldots, a_n \in R \right\}, \end{aligned}$$

  where we are using the notation

$$\begin{aligned} &\operatorname{diag}(a_1, a_2, \ldots, a_n) = (\text{the diagonal matrix with diagonal } (a_1, a_2, \ldots, a_n)) \\ &= \begin{pmatrix} a_1 & 0 & \cdots & 0 \\ 0 & a_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & a_n \end{pmatrix}. \end{aligned}$$

(For example,

$$R^{2=2} = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in R \right\} = \left\{ \operatorname{diag}(a, b) \mid a, b \in R \right\}.$$

)

It is easy to see that $R^{n=n}$ is a subring of $R^{n \times n}$. Moreover, $R^{n=n} \cong R^n$ as rings (where, as we recall, $R^n = \underbrace{R \times R \times \cdots \times R}_{n \text{ times}} = R^{\{1,2,\ldots,n\}}$). Indeed, the map

$$\begin{aligned} R^n &\to R^{n=n}, \\ (a_1, a_2, \ldots, a_n) &\mapsto \operatorname{diag}(a_1, a_2, \ldots, a_n) \end{aligned}$$

is a ring isomorphism. For example, it respects multiplication, since

$$\operatorname{diag}(a_1, a_2, \ldots, a_n) \cdot \operatorname{diag}(b_1, b_2, \ldots, b_n) = \operatorname{diag}(a_1 b_1, a_2 b_2, \ldots, a_n b_n)$$

for any $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in R^n$.

It is easy to see that a direct product of commutative rings is commutative.

Exercise 2.10.1. Prove that the direct product $(\mathbb{Z}/2)^2 = (\mathbb{Z}/2) \times (\mathbb{Z}/2)$ is isomorphic to the ring B_4 from Subsection 2.1.2.

Exercise 2.10.2. Let R be any ring. Let I be an infinite set. As we recall, the direct product $R^I = \prod_{i \in I} R$ consists of all families $(r_i)_{i \in I}$ of elements of R. (For instance, if $I = \mathbb{N}$, then these families are just the infinite sequences $(r_0, r_1, r_2, \ldots) = (r_i)_{i \in \mathbb{N}}$ of elements of R.)

(a) We say that a family $(r_i)_{i \in I}$ is **finitary** if it has only finitely many nonzero entries (i.e., if there are only finitely many $i \in I$ that satisfy $r_i \neq 0$). Consider the set of all finitary families in R^I. Is this set a subring of R^I ?

(b) We say that a family $(r_i)_{i \in I}$ is **quasifinitary** if it all but finitely many of its entries are equal (i.e., if there exists some $c \in R$ such that only finitely many $i \in I$ that satisfy $r_i \neq c$). Consider the set of all quasifinitary families in R^I. Is this set a subring of R^I ?

(c) We say that a family $(r_i)_{i \in I}$ is **entry-finite** if it has only finitely many distinct entries (i.e., if the set $\{r_i \mid i \in I\}$ is finite). Consider the set of all entry-finite families in R^I. Is this set a subring of R^I ?

(For example, if $R = \mathbb{Z}$ and $I = \mathbb{N}$, then the family $(3, 1, 0, 0, 0, 0, \ldots)$ (with all entries after the 1 being zeroes) is finitary; the family $(3, 1, 1, 1, \ldots)$ (with all entries after the 3 being equal to 1) is quasifinitary; the family $(1, 2, 1, 2, 1, 2, \ldots)$ (alternating between 1's and 2's) is entry-finite.)

2.10.4. Direct products and idempotents

Direct products of rings are closely related to idempotents. One part of the connection is easy: If R and S are two rings, then their direct product $R \times S$ has the two idempotents $(1_R, 0_S)$ and $(0_R, 1_S)$ which, in a sense, "reveal" its two factors; in particular, the multiples of $(1_R, 0_S)$ form a "copy" of R (since these multiples are precisely the elements of the form $(r, 0_S)$ for $r \in R$), whereas the multiples of $(0_R, 1_S)$ form a "copy" of S. The following exercise states this claim precisely:

Exercise 2.10.3. Let R and S be two rings. Let $a := (1_R, 0_S) \in R \times S$ and $b := (0_R, 1_S) \in R \times S$. Prove the following:

(a) The principal ideal $a(R \times S)$ consists of all elements of the form $(r, 0_S)$ with $r \in R$.

(b) The principal ideal $b(R \times S)$ consists of all elements of the form $(0_R, s)$ with $s \in S$.

If the ring R is commutative, then this connection has a converse as well: Any idempotent in a commutative ring R can be used to split R into a direct product of two rings![57] Here are the details:

Exercise 2.10.4. Let R be a commutative ring, and let e be an idempotent element of R. As we know from Exercise 2.2.8 **(a)** (applied to $a = e$), the element $1 - e$ is then idempotent as well.

(a) Show that the principal ideal eR is itself a ring, with addition and multiplication inherited from R and with zero 0_R and with unity e. (This makes eR a subring of R in the sense of [DumFoo04], but not in our sense, since its unity is not generally the unity of R.)

(b) Show that the same holds for the principal ideal $(1 - e) R$ (except that its unity will be $1 - e$ instead of e).

(c) Consider the map

$$f : (eR) \times ((1 - e) R) \to R, \quad (a, b) \mapsto a + b.$$

Prove that this map f is a ring isomorphism.

Exercise 2.10.4 **(c)** shows that if a commutative ring R has an idempotent element e, then R can be decomposed (up to isomorphism) as a direct product $A \times B$ of two rings A and B (namely, $A = eR$ and $B = (1 - e) R$). If e is not one

[57] If the idempotent is 0 or 1, then one of the two factors will be a trivial ring.

of the two trivial idempotents 0 and 1, then these two rings A and B will be nontrivial, so the decomposition really deserves its name.[58]

Conversely, as we said above, any direct product of two nontrivial rings has nontrivial idempotents: If R and S are two rings, then $(1_R, 0_S)$ and $(0_R, 1_S)$ are two idempotent elements of the direct product $R \times S$.

Parts **(a)** and **(b)** of Exercise 2.10.4 can be generalized somewhat: Instead of requiring R to be commutative, it suffices to require that $er = re$ for all $r \in R$. We cannot, however, drop this requirement altogether (for instance, the matrix ring $\mathbb{R}^{2\times 2}$ has many idempotents, but cannot be written as a direct product of two nontrivial rings).

Exercise 2.10.5. Let R be a commutative ring, and n be a positive integer. An $n \times n$-matrix

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix} \in R^{n\times n}$$

is said to be **circulant** if it has the property that

$$a_{i,j} = a_{i',j'} \text{ whenever } i - j \equiv i' - j' \bmod n.$$

In other words, an $n \times n$-matrix $A \in R^{n\times n}$ is circulant if and only if each row of A equals the preceding row of A, cyclically rotated by 1 step to the right. For instance, a 4×4-matrix is circulant if and only if it has the form $\begin{pmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{pmatrix}$ for some $a, b, c, d \in R$.

Let $\operatorname{Circ}_n(R)$ denote the set of all circulant $n \times n$-matrices $A \in R^{n\times n}$.

Let $S \in \operatorname{Circ}_n(R)$ be the specific circulant $n \times n$-matrix whose first row is $(0, 1, 0, 0, 0, \ldots, 0)$ (that is, the second entry is 1 while all the other entries are 0). Thus,

$$S = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

(a) Compute S^n.

[58] As an example, take $R = \mathbb{Z}/6\mathbb{Z}$, and let e be the idempotent element $\overline{3} = 3 + 6\mathbb{Z}$ of R (this is idempotent since $3^2 = 9 \equiv 3 \bmod 6$ and thus $\overline{3}^2 = \overline{3^2} = \overline{3}$). Then, $eR = \{\overline{0}, \overline{3}\} \cong \mathbb{Z}/2\mathbb{Z}$ and $(1-e)R = \{\overline{0}, \overline{2}, \overline{4}\} \cong \mathbb{Z}/3\mathbb{Z}$. Hence, the ring isomorphism $R \cong (eR) \times ((1-e)R)$ becomes a ring isomorphism $\mathbb{Z}/6\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. We will soon revisit this isomorphism (it is an instance of the Chinese Remainder Theorem).

(b) Prove that every circulant matrix $A \in R^{n \times n}$ can be written as $a_0 S^0 + a_1 S^1 + \cdots + a_{n-1} S^{n-1}$, where $a_0, a_1, \ldots, a_{n-1}$ are the entries of the first row of A (from left to right).

(c) Prove that

$$\operatorname{Circ}_n(R) = \left\{ a_0 S^0 + a_1 S^1 + \cdots + a_{n-1} S^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in R \right\}.$$

(d) Show that $\operatorname{Circ}_n(R)$ is a **commutative** subring of the matrix ring $R^{n \times n}$.

(e) Assume that $n \geq 2$, and that the element $n \cdot 1_R$ of R is invertible. Find an idempotent e in $\operatorname{Circ}_n(R)$ that is distinct from both the zero matrix 0 and the identity matrix I_n.

(f) Under the same assumptions as in part **(e)**, prove that $\operatorname{Circ}_n(R)$ is isomorphic to a direct product of two rings, one of which is R.

(g) Which of the above claims remain true if we no longer require that R be commutative?

2.10.5. Boolean rings

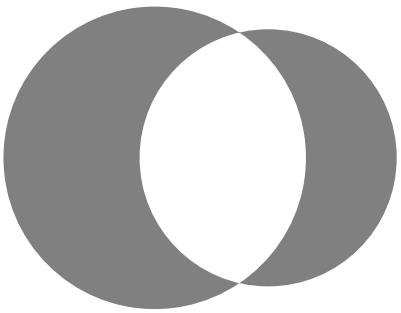
Another example of rings comes from (fairly basic) set theory. It rests upon the notion of "symmetric difference":

Definition 2.10.5. The **symmetric difference** of two sets A and B is defined to be the set

$$\begin{aligned} &(A \cup B) \setminus (A \cap B) \\ &= (A \setminus B) \cup (B \setminus A) \\ &= \{x \mid x \text{ belongs to exactly one of the two sets } A \text{ and } B\}. \end{aligned}$$

This symmetric difference is denoted by $A \triangle B$.

In terms of Venn diagrams, this symmetric difference $A \triangle B$ is the grey zone in the following Venn diagram (where the two circles are A and B):



Now, let S be any set. Let $\mathcal{P}(S)$ denote the power set of S (that is, the set of all subsets of S). It is easy to check that the following ten properties hold:

$$\begin{aligned}
A \triangle B &= B \triangle A \qquad \text{for any sets } A \text{ and } B; \\
A \cap B &= B \cap A \qquad \text{for any sets } A \text{ and } B; \\
(A \triangle B) \triangle C &= A \triangle (B \triangle C) \qquad \text{for any sets } A, B \text{ and } C; \\
(A \cap B) \cap C &= A \cap (B \cap C) \qquad \text{for any sets } A, B \text{ and } C; \\
A \triangle \varnothing &= \varnothing \triangle A = A \qquad \text{for any set } A; \\
A \triangle A &= \varnothing \qquad \text{for any set } A; \\
A \cap S &= S \cap A = A \qquad \text{for any subset } A \text{ of } S; \\
\varnothing \cap A &= A \cap \varnothing = \varnothing \qquad \text{for any set } A; \\
A \cap (B \triangle C) &= (A \cap B) \triangle (A \cap C) \qquad \text{for any sets } A, B \text{ and } C; \\
(A \triangle B) \cap C &= (A \cap C) \triangle (B \cap C) \qquad \text{for any sets } A, B \text{ and } C.
\end{aligned}$$

Therefore, $\mathcal{P}(S)$ becomes a commutative ring, where the addition is defined to be the operation $\triangle$, the multiplication is defined to be the operation $\cap$, the zero is defined to be the set $\varnothing$, and the unity is defined to be the set S. (The ten properties listed above show that the axioms of a commutative ring are satisfied for $(\mathcal{P}(S), \triangle, \cap, \varnothing, S)$. In particular, the sixth property shows that every subset A of S has an additive inverse – namely, itself. Of course, it is unusual for an element of a commutative ring to be its own additive inverse, but in this example it happens all the time!)

The commutative ring $\mathcal{P}(S)$ has the property that each element $a \in \mathcal{P}(S)$ is idempotent (i.e., satisfies $a \cdot a = a$). (Indeed, this simply means that each $A \subseteq S$ satisfies $A \cap A = A$.)

Exercise 2.10.6.

(a) Prove that the ring $\mathcal{P}(S)$ is isomorphic to the direct product $(\mathbb{Z}/2\mathbb{Z})^S = \prod_{s \in S} (\mathbb{Z}/2\mathbb{Z})$.

(b) Let F be the set of all **finite** subsets of S. Prove that F is an ideal of $\mathcal{P}(S)$.

(c) Assume that S is infinite. Prove that the ideal F is not principal.

(d) Instead, assume that S is finite. Prove that every ideal of $\mathcal{P}(S)$ is principal.

[**Hint:** For part **(d)**, let I be an ideal of $\mathcal{P}(S)$, and pick a subset $T \in I$ of largest size. Argue that each subset of T must also belong to I. Conclude that every set in I must be a subset of T.]

Forget that we fixed S. As we noticed, the ring $\mathcal{P}(S)$ that we have just defined has the strange-looking property that each of its elements is idempotent. Rings with this property are called **Boolean rings**. (Of course, $\mathcal{P}(S)$ is the eponymic

example for a Boolean ring; but there are also others.) Let us now study Boolean rings in general:

Definition 2.10.6. A **Boolean ring** means a ring R such that every $a \in R$ satisfies $a^2 = a$ (that is, every $a \in R$ is idempotent). (Keep in mind that rings must have a 1 according to our definition.)

Exercise 2.10.7. Let R be a Boolean ring. Prove the following:

(a) We have $2a = 0$ for each $a \in R$.

(b) We have $-a = a$ for each $a \in R$.

(c) The ring R is commutative.

(d) If R is finite, then $R \cong (\mathbb{Z}/2\mathbb{Z})^n$ for some $n \in \mathbb{N}$.

[**Hint:** In part **(a)**, use $a^2 = a$ and $(a+1)^2 = a+1$. In part **(c)**, expand $(a+b)^2$ (but don't use the binomial formula, since you don't know yet that $ab = ba$). Finally, for part **(d)**, use strong induction on $|R|$ as follows: Pick some $e \in R$ that is distinct from 0 and 1 (if no such e exists, the claim is obvious). Then, e is idempotent, so Exercise 2.10.4 **(c)** decomposes the ring R as a direct product of two smaller rings. You can use without proof that direct products are associative up to isomorphism (so that $A_1 \times A_2 \times \cdots \times A_m \cong (A_1 \times A_2 \times \cdots \times A_k) \times (A_{k+1} \times A_{k+2} \times \cdots \times A_m)$ for any rings $A_1, A_2, \ldots, A_m$).]

2.11. A few operations on ideals ([DumFoo04, §7.3])

Next, we shall see three ways to build new ideals of a ring from old. One of these three ways is intersection: If I and J are two ideals of a ring R, then their intersection $I \cap J$ is easily seen to be an ideal as well (see Proposition 2.11.2 **(a)** below). Let us now define two other ways:

Definition 2.11.1. Let I and J be two ideals of a ring R.

(a) Then, $I + J$ denotes the subset

$$\{i + j \mid i \in I \text{ and } j \in J\} \text{ of } R.$$

(b) Next, we define a further subset IJ, also denoted $I \cdot J$. Unlike $I + J$, this will **not** be defined as $\{i \cdot j \mid i \in I \text{ and } j \in J\}$. Instead, $IJ = I \cdot J$ will be defined as the set

$$\{\text{all finite sums of } (I,J)\text{-products}\},$$

where an (I,J)**-product** means a product of the form ij with $i \in I$ and $j \in J$. In other words,

$$IJ = \{i_1 j_1 + i_2 j_2 + \cdots + i_k j_k \mid k \in \mathbb{N} \text{ and } i_1, i_2, \ldots, i_k \in I \text{ and } j_1, j_2, \ldots, j_k \in J\}.$$

Note that our definition of IJ was more complicated than the one of $I+J$, as it involved an additional step (viz., taking finite sums). The purpose of this step is to ensure that IJ is closed under addition (which will later be used to argue that IJ is an ideal of R). It is forced to us if we try to construct an ideal of R that contains all (I,J)-products. We could have added the same step to our definition of $I+J$, but it would not have changed anything, since a finite sum of (I,J)-sums (i.e., of sums of the form $i+j$ with $i \in I$ and $j \in J$) can be rewritten as a single (I,J)-sum:

$$\begin{aligned}&(i_1+j_1)+(i_2+j_2)+\cdots+(i_k+j_k)\\ &= \underbrace{(i_1+i_2+\cdots+i_k)}_{\substack{\in I \\ \text{(since } I \text{ is closed under addition)}}} + \underbrace{(j_1+j_2+\cdots+j_k)}_{\substack{\in J \\ \text{(since } J \text{ is closed under addition)}}}.\end{aligned}$$

For (I,J)-products, however, this is not generally the case (although you won't find a counterexample for $R=\mathbb{Z}$).

Here is an assortment of facts about the above-defined operations on ideals (see Exercise 2.11.1 for a proof):[59]

Proposition 2.11.2. Let R be a ring.

(a) Let I and J be two ideals of R. Then, $I+J$ and $I \cap J$ and IJ are ideals of R as well.

(b) Let I and J be two ideals of R. Then, $IJ \subseteq I \cap J \subseteq I \subseteq I+J$ and $IJ \subseteq I \cap J \subseteq J \subseteq I+J$.

(c) The set of all ideals of R is a monoid with respect to the binary operation $+$, with neutral element $\{0_R\} = 0R$. That is,

$$\begin{aligned}(I+J)+K &= I+(J+K) && \text{for any three ideals } I,J,K \text{ of } R;\\ I+\{0_R\} &= \{0_R\}+I = I && \text{for any ideal } I \text{ of } R.\end{aligned}$$

(d) The set of all ideals of R is a monoid with respect to the binary operation $\cap$, with neutral element $R = 1R$. That is,

$$\begin{aligned}(I \cap J) \cap K &= I \cap (J \cap K) && \text{for any three ideals } I,J,K \text{ of } R;\\ I \cap R &= R \cap I = I && \text{for any ideal } I \text{ of } R.\end{aligned}$$

[59] Recall that if R is any ring, then the one-element set $\{0_R\}$ and the entire ring R are ideals of R. Both of these ideals are principal ($\{0_R\} = 0_R R$ and $R = 1_R R$); they "bookend" all ideals of R (in the sense that $\{0_R\} \subseteq I \subseteq R$ for each ideal I of R).

(Here, the ideals $0_R R$ and $1_R R$ are defined as in Proposition 2.8.5, even though R is not required to be commutative.)

(e) The set of all ideals of R is a monoid with respect to the binary operation $\cdot$, with neutral element $R = 1R$. That is,

$$(IJ)\,K = I\,(JK) \qquad \text{for any three ideals } I, J, K \text{ of } R;$$
$$IR = RI = I \qquad \text{for any ideal } I \text{ of } R.$$

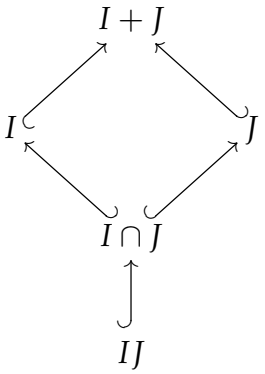
(f) Addition and intersection of ideals are commutative:

$$I + J = J + I \qquad \text{and} \qquad I \cap J = J \cap I \qquad \text{for any ideals } I, J \text{ of } R.$$

(g) If the ring R is commutative, then $IJ = JI$ for any two ideals I and J of R.

Proposition 2.11.2 shows that the operations $+$, $\cap$ and $\cdot$ on the set of all ideals of R satisfy a number of laws similar to the basic laws of arithmetic. This is known as **ideal arithmetic**. However, ideals cannot be subtracted (i.e., there is no operation that undoes addition of ideals[60]), and thus the ideals of R do not form an actual ring. (Likewise, there is no "division" operation on ideals that undoes multiplication, although something vaguely similar is defined in Exercise 2.11.6 below.)

Here is a diagram showing the inclusions between the ideals IJ, $I \cap J$, $I + J$, I, J:



(Recall that an arrow of type $X \hookrightarrow Y$ means a canonical inclusion from X to Y, which entails that $X \subseteq Y$.)

Exercise 2.11.1. Prove Proposition 2.11.2.

[**Hint:** You can be terse here, as there is a lot to show, much of it straightforward. Part **(d)** is obvious. For part **(e)**, I recommend using the notion of "(I, J)-products" from Definition 2.11.1; it is often easier to talk abstractly about sums of (I, J)-products than to write them out as $i_1 j_1 + i_2 j_2 + \cdots + i_k j_k$. For the proof of $(IJ)\,K = I\,(JK)$, you can start out by showing that any (IJ, K)-product belongs to $I\,(JK)$.]

[60] That is, if I and J are two ideals, then you cannot recover I from J and $I + J$.

The following proposition tells us how ideal arithmetic looks like when we apply it to principal ideals of $\mathbb{Z}$:

Proposition 2.11.3. Let $n, m \in \mathbb{Z}$. Let $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$. Then:

(a) We have $IJ = nm\mathbb{Z}$.

(b) We have $I \cap J = \operatorname{lcm}(n, m)\,\mathbb{Z}$.

(c) We have $I + J = \gcd(n, m)\,\mathbb{Z}$.

Proof. **(a)** From $n \in I$ and $m \in J$, we see that nm is an (I, J)-product. Thus, nm is a finite sum of (I, J)-products (of just one, to be specific). In other words, $nm \in IJ$. Since IJ is an ideal of $\mathbb{Z}$, this entails that every multiple of nm also belongs to IJ (by the second ideal axiom); in other words, $nm\mathbb{Z} \subseteq IJ$.

Conversely: If $i \in I$ and $j \in J$, then $i = nx$ for some $x \in \mathbb{Z}$ (since $i \in I = n\mathbb{Z}$) and $j = my$ for some $y \in \mathbb{Z}$ (since $j \in J = m\mathbb{Z}$) and therefore $ij = (nx)(my) = nm(xy) \in nm\mathbb{Z}$. Thus, every (I, J)-product belongs to $nm\mathbb{Z}$ (because an (I, J)-product always has the form ij for some $i \in I$ and $j \in J$). Hence, any sum of (I, J)-products also belongs to $nm\mathbb{Z}$ (since $nm\mathbb{Z}$ is closed under addition). In other words, $IJ \subseteq nm\mathbb{Z}$ (since any element of IJ is a sum of (I, J)-products). Therefore, $IJ = nm\mathbb{Z}$ (since we already have seen that $nm\mathbb{Z} \subseteq IJ$). This proves Proposition 2.11.3 **(a)**.

(b) We have

$$\begin{aligned} I \cap J &= \{\text{all elements of } I \text{ that also belong to } J\} \\ &= \{\text{all multiples of } n \text{ that also are multiples of } m\} \\ &\qquad \left(\begin{array}{c} \text{since } I = n\mathbb{Z} = \{\text{all multiples of } n\} \\ \text{and } J = m\mathbb{Z} = \{\text{all multiples of } m\} \end{array} \right) \\ &= \{\text{all common multiples of } n \text{ and } m\} \\ &= \{\text{all multiples of } \operatorname{lcm}(n, m)\} \\ &\qquad \left(\begin{array}{c} \text{since a result in elementary number theory} \\ \text{says that the common multiples of } n \text{ and } m \\ \text{are precisely the multiples of } \operatorname{lcm}(n, m) \end{array} \right) \\ &= \operatorname{lcm}(n, m)\,\mathbb{Z}. \end{aligned}$$

This proves Proposition 2.11.3 **(b)**.

(c) First, we shall show that $I + J \subseteq \gcd(n, m)\,\mathbb{Z}$. Indeed, any element of I is a multiple of n (since $I = n\mathbb{Z}$), thus a multiple of $\gcd(n, m)$ (since n is a multiple of $\gcd(n, m)$). Similarly, any element of J is a multiple of $\gcd(n, m)$. Thus, an element of $I + J$ is a sum of two multiples of $\gcd(n, m)$, and therefore itself a multiple of $\gcd(n, m)$. In other words, any element of $I + J$ belongs to $\gcd(n, m)\,\mathbb{Z}$. In other words, $I + J \subseteq \gcd(n, m)\,\mathbb{Z}$.

Now, we need to prove that $\gcd(n,m)\mathbb{Z} \subseteq I+J$. For this, it suffices to show that $\gcd(n,m) \in I+J$, because $I+J$ is an ideal (and thus will contain any multiple of $\gcd(n,m)$ once we know it contains $\gcd(n,m)$). But Bezout's theorem shows that $\gcd(n,m) = xn+ym$ for some integers x and y. Thus, $\gcd(n,m) \in I+J$ (since $xn = nx \in n\mathbb{Z} = I$ and $ym = my \in m\mathbb{Z} = J$). This finishes our proof of $\gcd(n,m)\mathbb{Z} \subseteq I+J$. Combining this with $I+J \subseteq \gcd(n,m)\mathbb{Z}$, we obtain $I+J = \gcd(n,m)\mathbb{Z}$. This proves Proposition 2.11.3 **(c)**. □

Exercise 2.11.2. Let R be any nontrivial ring, and consider the ideals I, J, K of the upper-triangular matrix ring $R^{2\leq 2}$ defined in Exercise 2.8.5 **(a)**. Show that $IJ = \{0\}$ but $JI = K$. (Thus, $IJ \neq JI$ in this case.)

Exercise 2.11.3. Let R be a ring. Let I, J, K be three ideals of R. Prove that

$$I(J+K) = IJ + IK \qquad \text{and} \qquad (I+J)K = IK + JK.$$

Exercise 2.11.4. Let R be a commutative ring. Let a and b be two elements of R. Prove that $(a+b)R \subseteq aR + bR$.

(Recall that $(a+b)R$, aR and bR are principal ideals, and the "$+$" sign in "$aR+bR$" is a sum of two ideals, not a sum of two elements of R.)

Exercise 2.11.5. Let R be a commutative ring. Let I be an ideal of R. Let a and b be two elements of R such that $a-b \in I$. Prove that $aR + I = bR + I$.

The next exercise defines yet another (less frequently used) operation on ideals:

Exercise 2.11.6. Let R be a ring. Let I and J be two ideals of R.

We say that a given element $a \in R$ **leads** J into I if and only if each $j \in J$ satisfies $aj \in I$ and $ja \in I$. In other words, an element $a \in R$ leads J into I if and only if multiplying this element with any element of J (from the left or from the right) produces an element of I.

We let $(I : J)$ be the set of all elements $a \in R$ that lead J into I.

(a) Prove that $(I : J)$ is an ideal of R. (This is called the **colon ideal** of I and J.)

(b) For $R = \mathbb{Z}$, compute the colon ideals $(6\mathbb{Z} : 2\mathbb{Z})$ and $(6\mathbb{Z} : 4\mathbb{Z})$.

(c) Let I, J and K be three ideals of R. Prove that

$$(I : J)(J : K) \cap (J : K)(I : J) \subseteq (I : K).$$

(d) Let I, J and K be three ideals of R. Prove that

$$(I : (J+K)) = (I : J) \cap (I : K).$$

2.12. The Chinese Remainder Theorem ([DumFoo04, §7.6])

2.12.1. Introduction

In Subsection 2.10.3, we have seen some examples of direct products. These examples were not very surprising; they were rings defined in a way that makes the product structure already quite evident. For example, the ring of diagonal $n \times n$-matrices was a direct product because you can easily see that the diagonal entries of diagonal matrices don't "interfere" with each other when the matrices are multiplied. Keywords like "entrywise", "pointwise" and "coordinatewise" tend to signal that some structure is a direct product. The 6-element ring $\mathbb{Z}/6$, on the other hand, does not look at all like a direct product. Yet, it is isomorphic to a direct product:

$$\mathbb{Z}/6 \cong (\mathbb{Z}/2) \times (\mathbb{Z}/3)\,.$$

Specifically, there is a ring isomorphism

$$\mathbb{Z}/6 \to (\mathbb{Z}/2) \times (\mathbb{Z}/3)\,,$$

which sends

$$\begin{aligned}
&\overline{0} \mapsto \left(\overline{0}, \overline{0}\right) \qquad \left(\text{that is, } 0+6\mathbb{Z} \mapsto \left(0+2\mathbb{Z},\ 0+3\mathbb{Z}\right)\right),\\
&\overline{1} \mapsto \left(\overline{1}, \overline{1}\right),\\
&\overline{2} \mapsto \left(\overline{2}, \overline{2}\right) = \left(\overline{0}, \overline{2}\right),\\
&\overline{3} \mapsto \left(\overline{3}, \overline{3}\right) = \left(\overline{1}, \overline{0}\right),\\
&\overline{4} \mapsto \left(\overline{4}, \overline{4}\right) = \left(\overline{0}, \overline{1}\right),\\
&\overline{5} \mapsto \left(\overline{5}, \overline{5}\right) = \left(\overline{1}, \overline{2}\right).
\end{aligned}$$

The reason why this works is that 2 and 3 are coprime. More generally:

Theorem 2.12.1 (The Chinese Remainder Theorem for two integers)**.** Let n and m be two coprime integers. Then,

$$\mathbb{Z}/\left(nm\right) \cong (\mathbb{Z}/n) \times (\mathbb{Z}/m) \qquad \text{as rings.}$$

More concretely, there is a ring isomorphism

$$\mathbb{Z}/\left(nm\right) \to (\mathbb{Z}/n) \times (\mathbb{Z}/m)$$

that sends each residue class $\overline{r}$ to the pair $(\overline{r}, \overline{r})$ (or, to use somewhat less ambiguous notation, sends each residue class $r + nm\mathbb{Z}$ to the pair $(r + n\mathbb{Z},\ r + m\mathbb{Z})$).

Rather than prove this theorem in this form, I will generalize it and then prove the generalization. After all, this is a course on rings, not just on $\mathbb{Z}/n$. So I will state and prove a "Chinese Remainder Theorem" for arbitrary rings.

In this theorem, $\mathbb{Z}$ will be replaced by an arbitrary ring R, and the integers n and m will be replaced by two ideals I and J of R (since ideals are what we can quotient rings by)[61]. The condition "n and m are coprime" will be replaced by the condition "$I + J = R$". Indeed, two integers n and m are coprime if and only if the corresponding principal ideals $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$ of $\mathbb{Z}$ satisfy $I + J = \mathbb{Z}$ (this follows easily from Proposition 2.11.3 **(c)**[62]). Two ideals I and J of a ring R satisfying $I + J = R$ are said to be **comaximal**:

2.12.2. The Chinese Remainder Theorem for two ideals

Definition 2.12.2. Let I and J be two ideals of a ring R. We say that I and J are **comaximal** if $I + J = R$.

Now we can state the general version of the Chinese Remainder Theorem. We will state this version in two parts, since they have slightly different assumptions (the first part requires R to be commutative, while the second one does not). Both parts will have to be combined to recover Theorem 2.12.1 later.

Theorem 2.12.3 (The Chinese Remainder Theorem for two ideals: ideal part)**.** Let I and J be two comaximal ideals of a commutative ring R. (Recall that "comaximal" means that $I + J = R$.) Then,

$$I \cap J = IJ.$$

Theorem 2.12.4 (The Chinese Remainder Theorem for two ideals: quotient part)**.** Let I and J be two comaximal ideals of a ring R. (Recall that "comaximal" means that $I + J = R$.) Then:

(a) We have

$$R/\left(I \cap J\right) \cong \left(R/I\right) \times \left(R/J\right).$$

(b) More concretely, there is a ring isomorphism

$$R/\left(I \cap J\right) \to \left(R/I\right) \times \left(R/J\right)$$

that sends each residue class $r + (I \cap J)$ to the pair $(r + I,\ r + J)$.

[61] I could also replace the integers n and m by two elements of R, but that would be less general: Quotienting by an element is tantamount to quotienting by a principal ideal, and principal ideals are just one kind of ideals.

[62] *Proof.* Let n and m be two integers. Let $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$ be the corresponding principal ideals of $\mathbb{Z}$. Then, Proposition 2.11.3 **(c)** yields $I + J = \gcd(n, m)\,\mathbb{Z}$. If n and m are coprime, then $\gcd(n, m) = 1$, so this rewrites as $I + J = 1\mathbb{Z} = \mathbb{Z}$. Conversely, if $I + J = \mathbb{Z}$, then $1 \in \mathbb{Z} = I + J = \gcd(n, m)\,\mathbb{Z}$, which shows that 1 is a multiple of $\gcd(n, m)$; but this entails that $\gcd(n, m) = 1$, and therefore n and m are coprime. Thus, we have shown that n and m are coprime if and only if $I + J = \mathbb{Z}$.

Let us now prove these theorems. Before we do so, let us agree on a convention that will save us some parentheses:

Convention 2.12.5. The "/" sign will have higher precedence than the "$\times$" sign, but lower precedence than the "implied $\cdot$ sign". Thus, the expression "$(R/I) \times (R/J)$" can be abbreviated as "$R/I \times R/J$" (without worrying that it might be misunderstood as "$R/\left(I \times R\right)/J$", whatever this would mean), and similarly the expression "$R/\left(IJ\right)$" can be abbreviated as "R/IJ" (without worrying that it might be misunderstood as "$(R/I)\,J$").

Proof of Theorem 2.12.3. We have $1 \in R = I + J$ (since I and J are comaximal). In other words,

$$\text{there exist } i \in I \text{ and } j \in J \text{ with } 1 = i + j.$$

Consider these i and j.

Proposition 2.11.2 **(b)** yields $IJ \subseteq I \cap J$. Thus, we only need to show that $I \cap J \subseteq IJ$.

So let $a \in I \cap J$. Thus, $a \in I$ and $a \in J$. Now,

$$a = a \cdot \underbrace{1}_{=i+j} = a \cdot (i+j) = \underbrace{ai}_{\substack{=ia \\ \text{(since } R \text{ is} \\ \text{commutative)}}} + aj = \underbrace{ia}_{\substack{\in IJ \\ \text{(since } i \in I \text{ and } a \in J\text{)}}} + \underbrace{aj}_{\substack{\in IJ \\ \text{(since } a \in I \text{ and } j \in J\text{)}}}$$

$$\in IJ + IJ = IJ.$$

(The last equality relied on the fact that $K + K = K$ for any ideal K of R. This is an easy consequence of the fact that K is a subgroup of the additive group $(R, +, 0)$.)

Forget that we fixed a. We thus have shown that $a \in IJ$ for each $a \in I \cap J$. In other words, $I \cap J \subseteq IJ$. As we said above, this completes the proof of Theorem 2.12.3. $\square$

Proof of Theorem 2.12.4. We have $1 \in R = I + J$ (since I and J are comaximal). In other words,

$$\text{there exist } i \in I \text{ and } j \in J \text{ with } 1 = i + j.$$

Consider these i and j.

Consider the map[63]

$$\begin{aligned} f : R &\to R/I \times R/J, \\ r &\mapsto \left(r + I,\ r + J\right). \end{aligned}$$

It is straightforward to see that this map f is a ring morphism (from R to the direct product $R/I \times R/J$).

[63] Recall that "$R/I \times R/J$" means "$(R/I) \times (R/J)$".

Moreover, we claim that $\operatorname{Ker} f = I \cap J$. Indeed, let $x \in \operatorname{Ker} f$. Thus, $f(x) = 0_{R/I \times R/J} = (0+I,\ 0+J)$. Since $f(x)$ was defined to be $(x+I,\ x+J)$, this means that $(x+I,\ x+J) = (0+I,\ 0+J)$. In other words, $x+I = 0+I$ and $x+J = 0+J$. In other words, $x \in I$ and $x \in J$. In other words, $x \in I \cap J$.

Forget that we fixed x. We thus have shown that $x \in I \cap J$ for each $x \in \operatorname{Ker} f$. In other words, $\operatorname{Ker} f \subseteq I \cap J$. Reading this argument in reverse shows that $I \cap J \subseteq \operatorname{Ker} f$. Thus,

$$\operatorname{Ker} f = I \cap J.$$

Now, we claim that f is surjective. Indeed, $1 = i + j$, so that $1 - i = j \in J$ and thus $1 + J = i + J$. Now, $i + I = 0 + I$ (since $i \in I$) and $i + J = 1 + J$ (since $1 + J = i + J$). But the definition of f yields $f(i) = (i+I,\ i+J) = (0+I,\ 1+J)$ (since $i+I = 0+I$ and $i+J = 1+J$). Similarly, $f(j) = (1+I,\ 0+J)$. Now, for every $x \in R$ and $y \in R$, we have

$$\begin{aligned}
f(yi+xj) &= \underbrace{f(y)}_{\substack{=(y+I,\ y+J)\\ \text{(by the definition of } f\text{)}}} \underbrace{f(i)}_{=(0+I,\ 1+J)} + \underbrace{f(x)}_{\substack{=(x+I,\ x+J)\\ \text{(by the definition of } f\text{)}}} \underbrace{f(j)}_{=(1+I,\ 0+J)} \\
&\qquad \left(\text{since } f \text{ is a ring morphism}\right) \\
&= \underbrace{(y+I,\ y+J)\,(0+I,\ 1+J)}_{\substack{=((y+I)(0+I),\ (y+J)(1+J))\\ \text{(since the multiplication of } R/I \times R/J \\ \text{is defined to be entrywise)}}} + \underbrace{(x+I,\ x+J)\,(1+I,\ 0+J)}_{\substack{=((x+I)(1+I),\ (x+J)(0+J))\\ \text{(since the multiplication of } R/I \times R/J \\ \text{is defined to be entrywise)}}} \\
&= \left(\underbrace{(y+I)\,(0+I)}_{\substack{=y\cdot 0+I\\ =0+I}},\ \underbrace{(y+J)\,(1+J)}_{\substack{=y\cdot 1+J\\ =y+J}} \right) + \left(\underbrace{(x+I)\,(1+I)}_{\substack{=x\cdot 1+I\\ =x+I}},\ \underbrace{(x+J)\,(0+J)}_{\substack{=x\cdot 0+J\\ =0+J}} \right) \\
&= (0+I,\ y+J) + (x+I,\ 0+J) \\
&= \left(\underbrace{(0+I)+(x+I)}_{\substack{=0+x+I\\ =x+I}},\ \underbrace{(y+J)+(0+J)}_{\substack{=y+0+J\\ =y+J}} \right) \\
&\qquad \left(\text{since the addition of } R/I \times R/J \text{ is defined to be entrywise}\right) \\
&= (x+I,\ y+J),
\end{aligned}$$

which shows that the pair $(x+I,\ y+J)$ lies in the image of f.

Thus, every element of the form $(x+I,\ y+J)$ for some $x \in R$ and $y \in R$ lies in the image of f. Since every element of $R/I \times R/J$ has this form[64], we thus conclude that every element of $R/I \times R/J$ lies in the image of f. In other words, f is surjective. In other words, $f(R) = R/I \times R/J$.

[64] because every element of R/I has the form $x+I$ for some $x \in R$, while every element of R/J has the form $y+J$ for some $y \in R$

Now, recall the First isomorphism theorem for rings (Theorem 2.9.9 **(c)**). Applying it to $S = R/I \times R/J$ (and to our ring morphism $f : R \to R/I \times R/J$), we see that the map

$$\begin{aligned} f' : R/\operatorname{Ker} f &\to f(R), \\ \overline{r} &\mapsto f(r) \end{aligned}$$

is well-defined and is a ring isomorphism.

In our case right now, we have $f(R) = R/I \times R/J$ and $\operatorname{Ker} f = I \cap J$, so that we can restate this as follows: The map

$$\begin{aligned} f' : R/(I \cap J) &\to R/I \times R/J, \\ \overline{r} &\mapsto f(r) \end{aligned}$$

is well-defined and is a ring isomorphism. This map f' sends each residue class $\overline{r} = r + (I \cap J)$ to $f(r) = (r + I,\ r + J)$ (by the definition of f). Thus, we have found a ring isomorphism

$$R/(I \cap J) \to R/I \times R/J$$

that sends each residue class $r + (I \cap J)$ to the pair $(r + I,\ r + J)$ (namely, f'). This proves part **(b)** of Theorem 2.12.4. Of course, part **(a)** thus follows. □

You can get rid of the commutativity requirement on R in Theorem 2.12.3 if you replace IJ by $IJ + JI$. (Checking this is a nice exercise on making sure you understand the above proof.)

2.12.3. Application to integers

As a corollary of Theorems 2.12.3 and 2.12.4, we can now prove the good old number-theoretical Chinese Remainder Theorem (Theorem 2.12.1), which we will repeat for convenience:

Theorem 2.12.6 (The Chinese Remainder Theorem for two integers)**.** Let n and m be two coprime integers. Then,

$$\mathbb{Z}/(nm) \cong (\mathbb{Z}/n) \times (\mathbb{Z}/m) \qquad \text{as rings.}$$

More concretely, there is a ring isomorphism

$$\mathbb{Z}/(nm) \to (\mathbb{Z}/n) \times (\mathbb{Z}/m)$$

that sends each residue class $\overline{r}$ to the pair $(\overline{r},\ \overline{r})$ (or, to use somewhat less ambiguous notation, sends each residue class $r + nm\mathbb{Z}$ to the pair $(r + n\mathbb{Z},\ r + m\mathbb{Z})$).

Proof. Let $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$. Proposition 2.11.3 then yields $IJ = nm\mathbb{Z}$ and $I \cap J = \operatorname{lcm}(n,m)\,\mathbb{Z}$ and $I + J = \gcd(n,m)\,\mathbb{Z}$. Since n and m are coprime, we have $\gcd(n,m) = 1$; thus, $I + J = \underbrace{\gcd(n,m)}_{=1}\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$. In other words, the ideals I and J of $\mathbb{Z}$ are comaximal. Hence, Theorem 2.12.3 yields $I \cap J = IJ = nm\mathbb{Z}$. Furthermore, part **(a)** of Theorem 2.12.4 yields $R/(I \cap J) \cong (R/I) \times (R/J)$. In view of $\underbrace{R}_{=\mathbb{Z}} / \underbrace{(I \cap J)}_{=nm\mathbb{Z}} = \mathbb{Z}/(nm\mathbb{Z}) = \mathbb{Z}/(nm)$ and $\underbrace{R}_{=\mathbb{Z}} / \underbrace{I}_{=n\mathbb{Z}} = \mathbb{Z}/(n\mathbb{Z}) = \mathbb{Z}/n$ and $\underbrace{R}_{=\mathbb{Z}} / \underbrace{J}_{=m\mathbb{Z}} = \mathbb{Z}/(m\mathbb{Z}) = \mathbb{Z}/m$, this rewrites as $\mathbb{Z}/(nm) \cong (\mathbb{Z}/n) \times (\mathbb{Z}/m)$. This proves the first claim of Theorem 2.12.6. The "More concretely" claim likewise follows from part **(b)** of Theorem 2.12.4. □

2.12.4. Comaximality for products of ideals

We shall next prove some auxiliary results about comaximal ideals, which will later help us generalize Theorem 2.12.3 and Theorem 2.12.4 to k ideals instead of 2 ideals. These can also serve as exercises on ideal arithmetic.

Proposition 2.12.7. Let I, J, K be three ideals of a ring R. Then:

(a) We have $(I + K)(J + K) \subseteq IJ + K$.

(b) If $I + K = R$ and $J + K = R$, then $IJ + K = R$.

Proof. Using Proposition 2.11.2 **(a)**, we easily see that the sets $I + K$ and $J + K$ and $IJ + K$ are ideals of R. Hence, these sets are closed under addition.

(a) Let $x \in I + K$ and $y \in J + K$. We shall show that $xy \in IJ + K$.

Indeed, $x \in I + K$. In other words, we can write x in the form $x = i + a$ for some $i \in I$ and $a \in K$. Consider these i and a.

Also, $y \in J + K$. In other words, we can write y in the form $y = j + b$ for some $j \in J$ and $b \in K$. Consider these j and b.

Now, multiplying the two equalities $x = i + a$ and $y = j + b$, we obtain

$$xy = (i + a)(j + b) = ij + ib + aj + ab.$$

From $a \in K$ and $b \in K$, we conclude that each of the three products ib, aj, ab belongs to K (by the second ideal axiom, since K is an ideal). Hence, the sum of these three products also belongs to K (since K is an ideal and thus is closed under addition). In other words, $ib + aj + ab \in K$. Furthermore, from $i \in I$ and $j \in J$, we see that ij is an (I, J)-product and therefore a sum of (I, J)-products (namely, of just one such product). Hence, $ij \in IJ$ (by the definition of IJ). Now,

$$xy = \underbrace{ij}_{\in IJ} + \underbrace{ib + aj + ab}_{\in K} \in IJ + K.$$

Forget that we fixed x and y. We thus have shown that $xy \in IJ + K$ for each $x \in I + K$ and $y \in J + K$. In other words, every $(I + K,\ J + K)$-product belongs to $IJ + K$ (since every $(I + K,\ J + K)$-product has the form xy for some $x \in I + K$ and $y \in J + K$).

Since $IJ + K$ is closed under addition, we thus conclude that any finite sum of $(I + K,\ J + K)$-products belongs to $IJ + K$ as well. However, the definition of $(I + K)(J + K)$ yields

$$(I + K)(J + K) = \{\text{all finite sums of } (I + K,\ J + K)\text{-products}\} \subseteq IJ + K$$

(since any finite sum of $(I + K,\ J + K)$-products belongs to $IJ + K$). This proves Proposition 2.12.7 **(a)**.

(b) Assume that $I + K = R$ and $J + K = R$. Proposition 2.11.2 **(e)** yields that $RR = R$. Hence,

$$R = \underbrace{R}_{=I+K}\ \underbrace{R}_{=J+K} = (I + K)(J + K) \subseteq IJ + K \qquad \text{(by Proposition 2.12.7 \textbf{(a)})}.$$

Combined with $IJ + K \subseteq R$ (which is obvious), this yields $IJ + K = R$. Thus, Proposition 2.12.7 **(b)** is proved. □

Exercise 2.12.1.

(a) Recall the following fact from elementary number theory: If a, b, c are three integers such that each of a and b is coprime to c, then ab is also coprime to c. How does Proposition 2.12.7 **(b)** generalize this fact?

(b) What property of greatest common divisors of integers does Proposition 2.12.7 **(a)** generalize?

Proposition 2.12.7 **(b)** can be extended by replacing the two ideals I and J by k ideals $I_1, I_2, \ldots, I_k$:

Proposition 2.12.8. Let $I_1, I_2, \ldots, I_k$ be k ideals of a ring R. Let K be a further ideal of R. Assume that

$$I_i + K = R \qquad \text{for each } i \in \{1, 2, \ldots, k\}. \tag{21}$$

Then, $I_1 I_2 \cdots I_k + K = R$.

Proof. We proceed by induction on k:

Base case: The ideal R is the neutral element of the monoid of ideals of R under multiplication (see Proposition 2.11.2 **(e)**). Thus, the empty product of ideals of R is defined to be R.

Now, in the case $k = 0$, the product $I_1 I_2 \cdots I_k$ is an empty product of ideals and therefore equals R (by the previous sentence). Hence, in this case, we have

$\underbrace{I_1 I_2 \cdots I_k}_{=R} + K = R + K = R$ (this is very easy to check). Thus, Proposition 2.12.8 is proved for $k = 0$.

Induction step: Let m be a positive integer. Assume (as the induction hypothesis) that Proposition 2.12.8 holds for $k = m - 1$. We must prove that Proposition 2.12.8 holds for $k = m$.

So let $I_1, I_2, \ldots, I_m$ be m ideals of a ring R. Let K be a further ideal of R. Assume that

$$I_i + K = R \qquad \text{for each } i \in \{1, 2, \ldots, m\}. \tag{22}$$

We must then show that $I_1 I_2 \cdots I_m + K = R$.

The equality (22) holds for each $i \in \{1, 2, \ldots, m\}$, and thus in particular for each $i \in \{1, 2, \ldots, m-1\}$. Hence, we can apply Proposition 2.12.8 to $k = m - 1$ (since our induction hypothesis says that Proposition 2.12.8 holds for $k = m - 1$). Thus we obtain $I_1 I_2 \cdots I_{m-1} + K = R$. Since we also have $I_m + K = R$ (by (22), applied to $i = m$), we can thus apply Proposition 2.12.7 **(b)** to $I = I_1 I_2 \cdots I_{m-1}$ and $J = I_m$. We thus obain

$$\left(I_1 I_2 \cdots I_{m-1}\right) I_m + K = R.$$

In other words, $I_1 I_2 \cdots I_m + K = R$ (since $\left(I_1 I_2 \cdots I_{m-1}\right) I_m = I_1 I_2 \cdots I_m$). Thus, we have proved that Proposition 2.12.8 holds for $k = m$. This completes the induction step, and thus Proposition 2.12.8 is proved by induction. □

Lemma 2.12.9. Let $I_1, I_2, \ldots, I_k$ be k ideals of a ring R. Then, $I_1 I_2 \cdots I_k \subseteq I_1 \cap I_2 \cap \cdots \cap I_k$.

Proof. We proceed by induction on k:

Base case: In the case $k = 0$, both $I_1 I_2 \cdots I_k$ and $I_1 \cap I_2 \cap \cdots \cap I_k$ are the ideal R (indeed, this can be seen as in the proof of Proposition 2.12.8, since R is the neutral element for both the multiplication and the intersection of ideals of R). Thus, in the case $k = 0$, we have $I_1 I_2 \cdots I_k \subseteq I_1 \cap I_2 \cap \cdots \cap I_k$ (since $R \subseteq R$). In other words, Lemma 2.12.9 is proved for $k = 0$.

Induction step: Let m be a positive integer. Assume (as the induction hypothesis) that Lemma 2.12.9 holds for $k = m - 1$. We must prove that Lemma 2.12.9 holds for $k = m$.

So let $I_1, I_2, \ldots, I_m$ be m ideals of a ring R. We must show that $I_1 I_2 \cdots I_m \subseteq I_1 \cap I_2 \cap \cdots \cap I_m$.

We can apply Lemma 2.12.9 to $k = m - 1$ (since our induction hypothesis says that Lemma 2.12.9 holds for $k = m - 1$). Thus we obtain $I_1 I_2 \cdots I_{m-1} \subseteq I_1 \cap I_2 \cap \cdots \cap I_{m-1}$.

However, Proposition 2.11.2 **(b)** yields that $IJ \subseteq I \cap J$ for any two ideals I and J of R. Applying this to $I = I_1 I_2 \cdots I_{m-1}$ and $J = I_m$, we obtain

$$\begin{aligned}\left(I_1 I_2 \cdots I_{m-1}\right) I_m &\subseteq \underbrace{\left(I_1 I_2 \cdots I_{m-1}\right)}_{\subseteq I_1 \cap I_2 \cap \cdots \cap I_{m-1}} \cap I_m \subseteq \left(I_1 \cap I_2 \cap \cdots \cap I_{m-1}\right) \cap I_m \\ &= I_1 \cap I_2 \cap \cdots \cap I_m.\end{aligned}$$

Since $(I_1 I_2 \cdots I_{m-1}) I_m = I_1 I_2 \cdots I_m$, we can rewrite this as

$$I_1 I_2 \cdots I_m \subseteq I_1 \cap I_2 \cap \cdots \cap I_m.$$

Thus, we have proved that Lemma 2.12.9 holds for $k = m$. This completes the induction step, and thus Lemma 2.12.9 is proved by induction. □

Corollary 2.12.10. Let $I_1, I_2, \ldots, I_k$ be k ideals of a ring R. Let K be a further ideal of R. Assume that

$$I_i + K = R \qquad \text{for each } i \in \{1, 2, \ldots, k\}.$$

Then, $(I_1 \cap I_2 \cap \cdots \cap I_k) + K = R$.

Proof. Lemma 2.12.9 yields $I_1 I_2 \cdots I_k \subseteq I_1 \cap I_2 \cap \cdots \cap I_k$.

It is easy to see that if I, J, L are three ideals of R such that $I \subseteq J$, then $I + L \subseteq J + L$. Applying this to $I = I_1 I_2 \cdots I_k$, $J = I_1 \cap I_2 \cap \cdots \cap I_k$ and $L = K$, we obtain

$$I_1 I_2 \cdots I_k + K \subseteq (I_1 \cap I_2 \cap \cdots \cap I_k) + K$$

(since $I_1 I_2 \cdots I_k \subseteq I_1 \cap I_2 \cap \cdots \cap I_k$). Hence,

$$(I_1 \cap I_2 \cap \cdots \cap I_k) + K \supseteq I_1 I_2 \cdots I_k + K = R \qquad \text{(by Proposition 2.12.8)}.$$

Combining this with $(I_1 \cap I_2 \cap \cdots \cap I_k) + K \subseteq R$ (which is obvious), we obtain $(I_1 \cap I_2 \cap \cdots \cap I_k) + K = R$. Thus, Corollary 2.12.10 is proven. □

2.12.5. The Chinese Remainder Theorem for k ideals

As we already suggested, Theorem 2.12.3 and Theorem 2.12.4 can be generalized to k ideals. First, a convention:

Definition 2.12.11. Let $I_1, I_2, \ldots, I_k$ be k ideals of a ring R. We say that these k ideals $I_1, I_2, \ldots, I_k$ are **mutually comaximal** if $I_i + I_j = R$ holds for all $1 \leq i < j \leq k$.

In other words, k ideals $I_1, I_2, \ldots, I_k$ are mutually comaximal if I_i and I_j are comaximal for every $i < j$. When $k > 2$, this is a **much stronger** statement than $I_1 + I_2 + \cdots + I_k = R$.

For example, if $n_1, n_2, \ldots, n_k$ are k arbitrary integers, then the k principal ideals $n_1\mathbb{Z}, n_2\mathbb{Z}, \ldots, n_k\mathbb{Z}$ are mutually comaximal if $n_1, n_2, \ldots, n_k$ are mutually coprime (that is, if n_i is coprime to n_j for all $i < j$). When $k > 2$, this is a **much stronger** statement than $\gcd(n_1, n_2, \ldots, n_k) = 1$. Be warned! Lots of mistakes have been made by mistaking "mutually coprime" for "gcd of all k numbers is 1".

Enough of the warning labels; here are the theorems:

Theorem 2.12.12 (The Chinese Remainder Theorem for k ideals: ideal part)**.** Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of a commutative ring R. Then,

$$I_1 \cap I_2 \cap \cdots \cap I_k = I_1 I_2 \cdots I_k.$$

Theorem 2.12.13 (The Chinese Remainder Theorem for k ideals: quotient part)**.** Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of a ring R. Then:

(a) We have

$$R/\left(I_1 \cap I_2 \cap \cdots \cap I_k\right) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_k.$$

(b) More concretely, there is a ring isomorphism

$$R/\left(I_1 \cap I_2 \cap \cdots \cap I_k\right) \to R/I_1 \times R/I_2 \times \cdots \times R/I_k$$

that sends each residue class $r + (I_1 \cap I_2 \cap \cdots \cap I_k)$ to the k-tuple $(r + I_1,\ r + I_2,\ \ldots,\ r + I_k)$.

Proof of Theorem 2.12.12. We proceed by induction on k:

Induction base: You can take $k = 1$ as a base case (it is utterly trivial), or even $k = 0$ if you are brave enough[65].

Induction step: Let n be a positive integer. (You can assume $n > 1$ if it makes you sleep better.) Assume (as the induction hypothesis) that Theorem 2.12.12 holds for $k = n - 1$. We must now prove that Theorem 2.12.12 holds for $k = n$.

So let $I_1, I_2, \ldots, I_n$ be n mutually comaximal ideals of a commutative ring R. Then, the induction hypothesis yields that Theorem 2.12.12 holds for $I_1, I_2, \ldots, I_{n-1}$. In particular, we have

$$I_1 \cap I_2 \cap \cdots \cap I_{n-1} = I_1 I_2 \cdots I_{n-1}. \tag{23}$$

Recall that the ideals $I_1, I_2, \ldots, I_n$ are mutually comaximal. Hence, for each $i \in \{1, 2, \ldots, n-1\}$, the ideals I_i and I_n are comaximal, i.e., satisfy $I_i + I_n = R$. Hence, Corollary 2.12.10 (applied to $k = n - 1$ and $K = I_n$) yields that $(I_1 \cap I_2 \cap \cdots \cap I_{n-1}) + I_n = R$. In other words, the two ideals $I_1 \cap I_2 \cap \cdots \cap I_{n-1}$ and I_n are comaximal.

Hence, we can apply Theorem 2.12.3 to $I = I_1 \cap I_2 \cap \cdots \cap I_{n-1}$ and $J = I_n$. We thus obtain

$$\left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right) \cap I_n = \left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right) I_n. \tag{24}$$

[65] Make sure to understand the empty product of ideals of R to be R itself, since R is the neutral element of the monoid of ideals of R under multiplication (see Proposition 2.11.2 **(e)**).

Likewise, the empty intersection of ideals of R is R itself, since R is the neutral element of the monoid of ideals of R under intersection (see Proposition 2.11.2 **(d)**).

Now,

$$\begin{aligned} I_1 \cap I_2 \cap \cdots \cap I_n &= (I_1 \cap I_2 \cap \cdots \cap I_{n-1}) \cap I_n \\ &= (I_1 \cap I_2 \cap \cdots \cap I_{n-1})\, I_n \qquad \text{(by (24))} \\ &= (I_1 I_2 \cdots I_{n-1})\, I_n \qquad \text{(by (23))} \\ &= I_1 I_2 \cdots I_n. \end{aligned}$$

Thus, we have proved that Theorem 2.12.12 holds for $k = n$. This completes the induction step. Thus, that Theorem 2.12.12 is proved. □

Proof of Theorem 2.12.13. We proceed by induction on k:

Induction base: Again, you can use $k = 0$ as the base case[66] (or $k = 1$ if you want to avoid trivialities).

Induction step: Let n be a positive integer. (Again, you can assume $n > 1$ if you prefer.) Assume (as the induction hypothesis) that Theorem 2.12.13 holds for $k = n - 1$. We must now prove that Theorem 2.12.13 holds for $k = n$.

So let $I_1, I_2, \ldots, I_n$ be n mutually comaximal ideals of a ring R. Then, the induction hypothesis yields that Theorem 2.12.13 holds for $I_1, I_2, \ldots, I_{n-1}$. In particular**,** part **(a)** of Theorem 2.12.13 shows that

$$R/\left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right) \cong R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1}. \tag{25}$$

Furthermore, part **(b)** of Theorem 2.12.13 shows that there is a ring isomorphism

$$R/\left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right) \to R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1} \tag{26}$$

that does what you would expect it to do (viz., sends each residue class $r + (I_1 \cap I_2 \cap \cdots \cap I_{n-1})$ to the $(n-1)$-tuple $(r + I_1,\ r + I_2,\ \ldots,\ r + I_{n-1})$).

Recall that the ideals $I_1, I_2, \ldots, I_n$ are mutually comaximal. Hence, for each $i \in \{1, 2, \ldots, n-1\}$, the ideals I_i and I_n are comaximal, i.e., satisfy $I_i + I_n = R$. Hence, Corollary 2.12.10 (applied to $k = n - 1$ and $K = I_n$) yields that $(I_1 \cap I_2 \cap \cdots \cap I_{n-1}) + I_n = R$. In other words, the two ideals $I_1 \cap I_2 \cap \cdots \cap I_{n-1}$ and I_n are comaximal.

Hence, we can apply Theorem 2.12.4 to $I = I_1 \cap I_2 \cap \cdots \cap I_{n-1}$ and $J = I_n$. We thus obtain (from part **(a)** of Theorem 2.12.4) that

$$\begin{aligned} &R/\left(\left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right) \cap I_n\right) \\ &\cong R/\left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right) \times R/I_n; \end{aligned} \tag{27}$$

furthermore, we obtain (from part **(b)**) that there is a ring isomorphism

$$\begin{aligned} &R/\left(\left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right) \cap I_n\right) \\ &\to R/\left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right) \times R/I_n \end{aligned} \tag{28}$$

[66] Just as in the above proof of Theorem 2.12.12, the empty intersection of ideals of R is R by definition. Thus, $R/\left(I_1 \cap I_2 \cap \cdots \cap I_k\right) = R/R$ is a trivial ring for $k = 0$.

Also, keep in mind that an empty direct product (i.e., a direct product of 0 rings) is a trivial ring whose only element is the 0-tuple $()$.

that does what you expect (viz., sends each residue class $r + ((I_1 \cap I_2 \cap \cdots \cap I_{n-1}) \cap I_n)$ to the pair $(r + (I_1 \cap I_2 \cap \cdots \cap I_{n-1}),\ r + I_n)$).

Now, let us combine the isomorphisms that we have found. This requires a little bit of yak-shaving. We will need the following lemma:

Lemma 2.12.14. Let A, B, C be three rings.

(a) If $A \cong B$, then $A \times C \cong B \times C$.

(b) More specifically: If $f : A \to B$ is a ring isomorphism, then the map

$$f \times \mathrm{id}_C : A \times C \to B \times C$$

(this is the map that sends each pair $(a,\ c) \in A \times C$ to $(f(a),\ \mathrm{id}_C(c)) = (f(a),\ c) \in B \times C$) is a ring isomorphism, too.

This lemma simply says that if you replace a ring in a direct product by an isomorphic one, then the whole direct product too stays isomorphic. I won't offend your intellect with the proof of this lemma; it is a purely paint-by-numbers affair. Such lemmas are a dime a dozen, and you are supposed to invent one whenever you need it. The idea behind this lemma is simply that isomorphisms behave like equalities.

So let us go back to our proof of Theorem 2.12.13. We have

$$\begin{aligned}
R/(I_1 \cap I_2 \cap \cdots \cap I_n) &= R/((I_1 \cap I_2 \cap \cdots \cap I_{n-1}) \cap I_n) \\
&\cong \underbrace{R/(I_1 \cap I_2 \cap \cdots \cap I_{n-1})}_{\substack{\cong R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1} \\ \text{(by (25))}}} \times R/I_n \qquad \text{(by (27))} \\
&\cong (R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1}) \times R/I_n \\
&\qquad \text{(by Lemma 2.12.14 \textbf{(a)})} \\
&\cong R/I_1 \times R/I_2 \times \cdots \times R/I_n;
\end{aligned}$$

this proves part **(a)** of Theorem 2.12.13 for $k = n$.

It remains to prove part **(b)**. Here we will need Lemma 2.12.14 **(b)**. Indeed, (26) gives us a ring isomorphism $R/(I_1 \cap I_2 \cap \cdots \cap I_{n-1}) \to R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1}$, which we can call f; thus, Lemma 2.12.14 **(b)** yields a ring isomorphism

$$\begin{aligned}
R/(I_1 \cap I_2 \cap \cdots \cap I_{n-1}) \times R/I_n \to (R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1}) \times R/I_n, \\
(a,\ c) \mapsto (f(a),\ c).
\end{aligned}$$

Now, we compose the arrows in our quiver:

$$\begin{aligned}
&R/\left(I_1 \cap I_2 \cap \cdots \cap I_n\right) \\
&= R/\left(\left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right) \cap I_n\right) \\
&\to R/\left(I_1 \cap I_2 \cap \cdots \cap I_{n-1}\right) \times R/I_n \qquad \text{(this is the isomorphism from (28))} \\
&\to \left(R/I_1 \times R/I_2 \times \cdots \times R/I_{n-1}\right) \times R/I_n \\
&\qquad \text{(this is the isomorphism we just constructed using Lemma 2.12.14 \textbf{(b)})} \\
&\to R/I_1 \times R/I_2 \times \cdots \times R/I_n.
\end{aligned}$$

All these arrows are ring isomorphisms; hence, so is their composition. It remains to show that this isomorphism does what you expect (i.e., sends each residue class $r + \left(I_1 \cap I_2 \cap \cdots \cap I_n\right)$ to $\left(r + I_1,\ r + I_2,\ \ldots,\ r + I_n\right)$). This is completely straightforward, and becomes even more so if you drop the details and just write $\overline{r}$ for all possible cosets $r + J$ no matter what J is: Following a coset $\overline{r} = r + \left(I_1 \cap I_2 \cap \cdots \cap I_n\right)$ through the above arrows, we obtain

$$\overline{r} = \overline{r} \mapsto \left(\overline{r},\ \overline{r}\right) \mapsto \left(\left(\overline{r},\ \overline{r},\ \ldots,\ \overline{r}\right),\ \overline{r}\right) \mapsto \left(\overline{r},\ \overline{r},\ \ldots,\ \overline{r}\right).$$

While the different $\overline{r}$'s mean different things (namely, they are cosets for different ideals), we are never in any danger of confusing them for one another, since we know what sets these maps go between. So the $\left(\overline{r},\ \overline{r},\ \ldots,\ \overline{r}\right)$ at the end of this computation must be $\left(r + I_1,\ r + I_2,\ \ldots,\ r + I_n\right)$, since it is an element of $R/I_1 \times R/I_2 \times \cdots \times R/I_n$. So our isomorphism sends $r + \left(I_1 \cap I_2 \cap \cdots \cap I_n\right)$ to $\left(r + I_1,\ r + I_2,\ \ldots,\ r + I_n\right)$. Thus, part **(b)** of Theorem 2.12.13 is proved for $k = n$.

Both parts of Theorem 2.12.13 are thus proved for $k = n$. This completes the induction step, and thus the proof. □

2.12.6. Applying to integers again

We can again apply this to $R = \mathbb{Z}$:

Theorem 2.12.15 (The Chinese Remainder Theorem for k integers)**.** Let $n_1, n_2, \ldots, n_k$ be k mutually coprime integers. ("Mutually coprime" means that n_i is coprime to n_j whenever $i < j$.) Then,

$$\mathbb{Z}/\left(n_1 n_2 \cdots n_k\right) \cong \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_k.$$

More concretely, there is a ring isomorphism

$$\mathbb{Z}/\left(n_1 n_2 \cdots n_k\right) \to \mathbb{Z}/n_1 \times \mathbb{Z}/n_2 \times \cdots \times \mathbb{Z}/n_k$$

that does what you expect (i.e., sends each residue class $r + n_1 n_2 \cdots n_k \mathbb{Z}$ to the k-tuple $\left(r + n_1\mathbb{Z},\ r + n_2\mathbb{Z},\ \ldots,\ r + n_k\mathbb{Z}\right)$).

Proof. This can be derived from Theorem 2.12.12 and Theorem 2.12.13, in the same way as we derived Theorem 2.12.6 from Theorem 2.12.3 and Theorem 2.12.4. Details are LTTR. □

Corollary 2.12.16. Let $p_1, p_2, \ldots, p_k$ be k distinct primes. Let $i_1, i_2, \ldots, i_k$ be k nonnegative integers. Then,

$$\mathbb{Z}/\left(p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}\right) \cong \mathbb{Z}/p_1^{i_1} \times \mathbb{Z}/p_2^{i_2} \times \cdots \times \mathbb{Z}/p_k^{i_k}.$$

More concretely, there is a ring isomorphism

$$\mathbb{Z}/\left(p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k}\right) \to \mathbb{Z}/p_1^{i_1} \times \mathbb{Z}/p_2^{i_2} \times \cdots \times \mathbb{Z}/p_k^{i_k}$$

that does what you expect.

Proof. The prime powers $p_1^{i_1}, p_2^{i_2}, \ldots, p_k^{i_k}$ are mutually coprime; thus, we can apply Theorem 2.12.15 to $n_j = p_j^{i_j}$. □

Note that it is important that the primes be distinct in Corollary 2.12.16. For example, $\mathbb{Z}/p^2$ is not isomorphic to $\mathbb{Z}/p \times \mathbb{Z}/p$ (not even as additive groups, let alone as rings).

The Chinese Remainder Theorem (and Corollary 2.12.16 in particular) has many down-to-earth consequences. For example, here is one:

Exercise 2.12.2. Let n be a positive integer. Let k be the number of distinct prime factors of n. (For instance, if $n = 360 = 2^3 \cdot 3^2 \cdot 5$, then $k = 3$.)

Show that the ring $\mathbb{Z}/n$ has exactly 2^k idempotent elements.

Let us next use the Chinese Remainder Theorem to revisit Exercise 1.5.5. That exercise asked you to count how many of the numbers $0, 1, \ldots, n-1$ appear as remainders of a perfect square divided by n, when n is 7 or 14. Let us now ask ourselves the same question for an arbitrary positive integer n. It is not hard to see that this question is equivalent to asking how many elements of the ring $\mathbb{Z}/n$ are squares in this ring. Here I am using the following terminology:

Definition 2.12.17. Let R be a ring. An element $r \in R$ is said to be a **square** (in R) if there exists some $u \in R$ such that $r = u^2$.

For example, the squares in $\mathbb{R}$ are the nonnegative reals, whereas the squares in $\mathbb{Z}$ are the perfect squares. For another example, the squares in $\mathbb{Z}/7\mathbb{Z}$ are the four elements $\overline{0}, \overline{1}, \overline{2}, \overline{4}$. (Indeed, this is equivalent to the answer to Exercise 1.5.5 **(a)**.)

If n is a positive integer, then an element $i \in \{0, 1, \ldots, n-1\}$ is the remainder of some perfect square divided by n if and only if the element $\overline{i} = i + n\mathbb{Z}$ is a

square in $\mathbb{Z}/n$. Thus, counting distinct remainders of perfect squares divided by n is equivalent to counting squares in $\mathbb{Z}/n$.

Now, I claim that the latter can be done easily when the prime factorization of n is known. The way to do it is in three steps:

1. Answer the question (i.e., "how many squares does $\mathbb{Z}/n$ have?") when n is prime.
2. Extend the answer to the case when n is a prime power (i.e., a number of the form p^i with p prime and $i \in \mathbb{N}$).
3. Finally, extend the answer to all positive integers n.

This three-step program is a standard strategy for answering number-theoretical questions. Typically, the three steps each have methods tailored to them:

1. When n is prime, the ring $\mathbb{Z}/n$ is a field. This makes many tactics available that would otherwise not work; e.g., Gaussian elimination works over fields but not generally over arbitrary rings (we will learn more about this later).
2. There are many tools for "lifting" results about primes to analogous results about prime powers.
3. Here, the Chinese Remainder Theorem becomes useful. Any positive integer $\mathbb{Z}/n$ is a product of finitely many mutually coprime prime powers $p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$. Thus, the Chinese Remainder Theorem (more precisely, Corollary 2.12.16) yields

$$\mathbb{Z}/n \cong \mathbb{Z}/p_1^{a_1} \times \mathbb{Z}/p_2^{a_2} \times \cdots \times \mathbb{Z}/p_k^{a_k}. \tag{29}$$

For our specific question (counting squares in $\mathbb{Z}/n$), Step 1 is quite easy (see Exercise 2.12.3 **(c)** below). (More precisely, that exercise covers the case when n is odd. But the only even prime is 2, and you can count the squares in $\mathbb{Z}/2$ on your hands[67].) Step 2 is both trickier and more laborious (see Exercises 2.12.5 and 2.12.6 below). Step 3 is now easy (assuming Steps 1 and 2 are done): If $A_1, A_2, \ldots, A_k$ are rings, then the squares in the direct product $A_1 \times A_2 \times \cdots \times A_k$ are just the k-tuples $(a_1, a_2, \ldots, a_k)$ where each a_i is a square in A_i; thus,

$$\begin{aligned}&(\text{the number of squares in } A_1 \times A_2 \times \cdots \times A_k) \\ &= \prod_{i=1}^{k} (\text{the number of squares in } A_i)\,.\end{aligned} \tag{30}$$

[67] Not fingers, hands.

Furthermore, isomorphic rings have the same number of squares (since any ring morphism sends squares to squares). Thus, (29) yields

$$\begin{aligned}
&(\text{the number of squares in } \mathbb{Z}/n) \\
&= \left(\text{the number of squares in } \mathbb{Z}/p_1^{a_1} \times \mathbb{Z}/p_2^{a_2} \times \cdots \times \mathbb{Z}/p_k^{a_k}\right) \\
&= \prod_{i=1}^{k} \left(\text{the number of squares in } \mathbb{Z}/p_i^{a_i}\right) \qquad \left(\text{by (30)}\right).
\end{aligned}$$

As promised, we shall now compute the number of squares in $\mathbb{Z}/p$ when p is an odd prime. Better even, let us compute the number of squares in any finite field F that satisfies $2 \cdot 1_F \neq 0_F$. (This is a more general question, since $\mathbb{Z}/p$ is a finite field whenever p is a prime, and it satisfies $2 \cdot 1_F \neq 0_F$ whenever p is odd.)

Exercise 2.12.3. Let F be a field.

(a) Prove that if $a, b \in F$ satisfy $a^2 = b^2$, then $a = b$ or $a = -b$.

From now on, assume that $2 \cdot 1_F \neq 0_F$ (that is, $1_F + 1_F \neq 0_F$). Note that this is satisfied whenever $F = \mathbb{Z}/p\mathbb{Z}$ for a prime $p > 2$ (but also for various other finite fields), but fails when $F = \mathbb{Z}/2\mathbb{Z}$.

(b) Prove that $a \neq -a$ for every nonzero $a \in F$.

From now on, assume that F is finite.

(c) Prove that the number of squares in F is $\dfrac{1}{2}\left(|F| + 1\right)$.

(d) Conclude that $|F|$ is odd.

[**Hint:** For part **(c)**, argue that each nonzero square in F can be written as α^2 for exactly two distinct elements $\alpha \in F$.]

Our next step towards counting squares in $\mathbb{Z}/n$ is the following exercise ([21w, homework set #2, Exercise 4]):

Exercise 2.12.4. Let p be a prime number.

(a) Prove that if a and b are two integers such that $a^2 \equiv b^2 \bmod p^2$, then $a \equiv b \bmod p^2$ or $a \equiv -b \bmod p^2$ or $a \equiv b \equiv 0 \bmod p$.

(b) Prove that the number of squares in the ring $\mathbb{Z}/p^2$ is $\dfrac{p^2 - p}{2} + 1$.

When the prime number p is distinct from 2, this can be extended to higher powers of p:

Exercise 2.12.5. Let $p > 2$ be a prime number. Let k be a positive integer.

(a) Prove that if a and b are two integers such that $a^2 \equiv b^2 \bmod p^k$, then $a \equiv b \bmod p^k$ or $a \equiv -b \bmod p^k$ or $a \equiv b \equiv 0 \bmod p$.

(b) Prove that the number of squares in the ring $\mathbb{Z}/p^k$ that are units is $\dfrac{p^k - p^{k-1}}{2}$.

(c) Prove that there is a bijection

$$\text{from the set } \left\{\text{squares in the ring } \mathbb{Z}/p^k \text{ that are not units}\right\}$$
$$\text{to the set } \left\{\text{squares in the ring } \mathbb{Z}/p^{k-2}\right\}$$

whenever $k \geq 2$.

(d) Prove that the number of all squares in the ring $\mathbb{Z}/p^k$ is

$$\frac{1}{2}\begin{cases} p^k - p^{k-1} + p^{k-2} - p^{k-3} + p^{k-4} - p^{k-5} \pm \cdots - p^1 + 2, & \text{if } k \text{ is even;} \\ p^k - p^{k-1} + p^{k-2} - p^{k-3} + p^{k-4} - p^{k-5} \pm \cdots - p^0, & \text{if } k \text{ is odd.} \end{cases}$$

Something similar works when p is 2, but there are some nuances:

Exercise 2.12.6. Let $k \geq 2$ be an integer.

(a) Prove that if a and b are two integers such that $a^2 \equiv b^2 \bmod 2^k$, then $a \equiv b \bmod 2^{k-1}$ or $a \equiv -b \bmod 2^{k-1}$ or $a \equiv b \equiv 0 \bmod 2$.

(b) Conversely, prove that if a and b are two integers such that $a \equiv b \bmod 2^{k-1}$ or $a \equiv -b \bmod 2^{k-1}$, then $a^2 \equiv b^2 \bmod 2^k$.

(c) Prove that the number of squares in the ring $\mathbb{Z}/2^k$ that are units is 2^{k-3} if $k \geq 3$, and is 1 otherwise.

(d) Compute the number of all squares in the ring $\mathbb{Z}/2^k$.

The Chinese Remainder Theorem can be used to break rings into smaller ones:

Exercise 2.12.7.

(a) Let $n_1, n_2, \ldots, n_k$ be k mutually coprime integers. ("Mutually coprime" means that n_i is coprime to n_j whenever $i < j$.) Let R be any ring. For any integer m, we let mR denote the ideal $\{mr \mid r \in R\}$ of R (this is easily seen to be an ideal, whether or not R is commutative), and we let R/m denote the corresponding quotient ring R/mR. Prove that

$$R/\left(n_1 n_2 \cdots n_k\right) \cong R/n_1 \times R/n_2 \times \cdots \times R/n_k.$$

(b) Let R be a finite ring whose size $|R|$ is a product $p_1 p_2 \cdots p_k$ of distinct primes $p_1, p_2, \ldots, p_k$ (such as $3 \cdot 5 \cdot 11$). Prove that R is commutative, and is isomorphic to $\mathbb{Z}/p_1 \times \mathbb{Z}/p_2 \times \cdots \times \mathbb{Z}/p_k$.

(c) Let R instead be a finite ring such that there exists no prime p satisfying $p^3 \mid |R|$. (This is a weaker assumption than in part **(b)**.) Prove that R is commutative.

2.12.7. Remark on noncommutative rings

Theorem 2.12.12 becomes false if we drop the assumption that R be commutative. Indeed, even Theorem 2.12.3 becomes false for noncommutative R, as the following exercise (taken from [vanDal06, Example 4]) shows:

Exercise 2.12.8. Let R be any nontrivial ring, and consider the ideals I, J, K of the upper-triangular matrix ring $R^{2\leq 2}$ defined in Exercise 2.8.5 **(a)**.

(a) Prove that I and J are comaximal (i.e., we have $I + J = R^{2\leq 2}$).

(b) Prove that $I \cap J \neq IJ$.

However, we can tweak Theorem 2.12.12 to make it work for noncommutative rings R as well:

Theorem 2.12.18. Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of a (not necessarily commutative) ring R. Let $I_1 * I_2 * \cdots * I_k$ denote the sum of all the $k!$ products $J_1 J_2 \cdots J_k$, where $J_1, J_2, \ldots, J_k$ are the k ideals $I_1, I_2, \ldots, I_k$ in some order. (For example, if $k = 3$, then $I_1 * I_2 * I_3 = I_1 I_2 I_3 + I_1 I_3 I_2 + I_2 I_1 I_3 + I_2 I_3 I_1 + I_3 I_1 I_2 + I_3 I_2 I_1$.)

Then,

$$I_1 \cap I_2 \cap \cdots \cap I_k = I_1 * I_2 * \cdots * I_k.$$

Exercise 2.12.9. Prove Theorem 2.12.18.

[**Hint:** The proof is a not-too-difficult adaptation of our above proof of Theorem 2.12.12.]

Theorem 2.12.18 can be improved even further. Namely, instead of summing all the $k!$ products $J_1 J_2 \cdots J_k$, we can sum the two products $I_1 I_2 \cdots I_k$ and $I_k I_{k-1} \cdots I_1$ (that is, we can replace $I_1 * I_2 * \cdots * I_k$ by the sum $I_1 I_2 \cdots I_k + I_k I_{k-1} \cdots I_1$), and Theorem 2.12.18 will remain true! This fascinating result (and a further generalization) is proved in Birgit van Dalen's nicely written bachelor thesis [vanDal05], which is a good reason to learn Dutch[68]. As an exercise, we suggest proving its $k = 3$ case:

[68] See [vanDal06] for a summary in English.

Exercise 2.12.10. Let R be a ring. Let I, J, K be three mutually comaximal ideals of R. Prove that $I \cap J \cap K = IJK + KJI$.

Here are two similar exercises (the first again courtesy of [vanDal05]):

Exercise 2.12.11. Let R be a ring. Let I, J, K be three mutually comaximal ideals of R. Prove that $I \cap J \cap K = IJK + JKI + KIJ$.

Exercise 2.12.12. Let R be a ring. Let I, J, K be three mutually comaximal ideals of R. Prove that $IJ + JK + KI = R$.

The next exercise shows that comaximality of ideals is passed on from two ideals to their powers:

Exercise 2.12.13. Let R be a ring. Let I and J be two comaximal ideals of R. Let n be a positive integer.

(a) Prove that the ideals I and J^n are comaximal as well. (Here, J^n means $\underbrace{JJ\cdots J}_{n \text{ times}}$, where we refer to Definition 2.11.1 **(b)** for the definition of the product of two ideals.)

(b) Let m be a further positive integer. Prove that the ideals I^m and J^n are comaximal as well.

(c) By applying this to $R = \mathbb{Z}$, prove that if a and b are two coprime integers, then their powers a^m and b^n are also coprime whenever m and n are two positive integers.

2.13. Euclidean rings and Euclidean domains ([DumFoo04, §8.1])

2.13.1. All ideals of $\mathbb{Z}$ are principal

We have talked about ideals of $\mathbb{Z}$ a lot (they give rise to modular arithmetic), but you might have noticed that all of them were principal. This is no accident:

Proposition 2.13.1. Any ideal of $\mathbb{Z}$ is principal.

Proof. Let I be an ideal of $\mathbb{Z}$. We must show that I is principal.

If $I = \{0\}$, then this is clear (since $I = 0\mathbb{Z}$ in this case). So we WLOG assume that $I \neq \{0\}$. Since I always contains 0, this means that I must contain a nonzero integer as well. Hence, I contains a positive integer (because if I contains a negative integer a, then I must also contain $(-1)\,a$, which is positive). Let $b \in I$ be the **smallest** positive integer that I contains. Hence, I cannot

contain any positive integer smaller than b. However, I contains b, and thus contains every multiple of b (since I is an ideal). In other words, $b\mathbb{Z} \subseteq I$.

We will now show that $I \subseteq b\mathbb{Z}$. Indeed, let $a \in I$. Let r be the remainder of a divided by b. Then, $r \in \{0, 1, \ldots, b-1\}$ and $r \equiv a \bmod b$. Now, from $r \equiv a \bmod b$, we obtain $b \mid r - a$ and thus $r - a \in b\mathbb{Z} \subseteq I$. Hence, $r = \underbrace{r-a}_{\in I} + \underbrace{a}_{\in I} \in I + I = I$ (since I is an ideal of $\mathbb{Z}$). Hence, r cannot be a positive integer smaller than b (since I cannot contain any positive integer smaller than b). In other words, $r \notin \{1, 2, \ldots, b-1\}$. Contrasting this with $r \in \{0, 1, \ldots, b-1\}$, we obtain $r = 0$. Thus, $b \mid \underbrace{r}_{=0} - a = 0 - a \mid -a \mid a$, so that $a \in b\mathbb{Z}$.

Forget that we fixed a. We thus have shown that $a \in b\mathbb{Z}$ for each $a \in I$. In other words, $I \subseteq b\mathbb{Z}$. Combined with $b\mathbb{Z} \subseteq I$, this yields $I = b\mathbb{Z}$. Thus, I is principal, qed. □

The key to making this proof work was clearly the concept of division with remainder. Not every ring has this feature. However, many rings different from $\mathbb{Z}$ have it; thus, it is worth defining a word for them:

2.13.2. Euclidean rings and Euclidean domains

Definition 2.13.2. Let R be a commutative ring.

(a) A **norm** on R means a function $N : R \to \mathbb{N}$ with $N(0) = 0$.

(b) A norm N on R is said to be **Euclidean** if for any $a \in R$ and any nonzero $b \in R$, there exist elements $q, r \in R$ with

$$a = qb + r \qquad \text{and} \qquad (r = 0 \text{ or } N(r) < N(b)).$$

(c) We say that R is a **Euclidean ring** if R has a Euclidean norm.

(d) We say that R is a **Euclidean domain** if R is a Euclidean ring and is an integral domain.

You can think of the norm as a measure of the "size" of an element of R, similar to the absolute value of an integer or to the degree of a polynomial. (These will indeed be particular cases.) Note that we are **not** requiring that the norm have any nice algebraic properties (such as $N(ab) = N(a)\,N(b)$, which will be true for some Euclidean norms but not for others). We are also **not** requiring the q and the r in Definition 2.13.2 **(b)** to be unique. If your familiarity with norms comes from real analysis, be warned that the concept we have defined here has nothing in common with the one you know except for the name.

Some examples will help illustrate the definition:

- Any field F is a Euclidean domain. Indeed, any map $N : F \to \mathbb{N}$ with $N(0) = 0$ is a Euclidean norm on F. (To see that it satisfies the condition of Definition 2.13.2 **(b)**, just set $q = \dfrac{a}{b}$ and $r = 0$.)

- The ring $\mathbb{Z}$ is a Euclidean domain. Indeed, the map

$$\begin{aligned} N : \mathbb{Z} &\to \mathbb{N}, \\ a &\mapsto |a| \end{aligned}$$

  is a Euclidean norm on $\mathbb{Z}$. The fact that it is Euclidean follows from division with remainder[69]. However, the q and the r in Definition 2.13.2 **(b)** are not unique! For $a = 7$ and $b = 5$, there are **two** pairs $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ with

$$a = qb + r \qquad \text{and} \qquad (r = 0 \text{ or } N(r) < N(b)).$$

  These two pairs are $(1, 2)$ and $(2, -3)$. The second pair has negative r, which is why it does not qualify as a quotient-remainder pair in the sense of high school arithmetic; but this r nevertheless qualifies for the definition of a Euclidean norm.

- If F is a field, then the ring $F[x]$ of univariate polynomials over F is a Euclidean domain. We will discuss this later in more detail, when we study polynomials. However, polynomial rings in more than 1 variable are not Euclidean; neither are polynomial rings over non-fields.

- The ring $\mathbb{Z}[i]$ of Gaussian integers is a Euclidean domain. Indeed, we claim that the map

$$\begin{aligned} N : \mathbb{Z}[i] &\to \mathbb{N}, \\ a + bi &\mapsto a^2 + b^2 \qquad (\text{for all } a, b \in \mathbb{Z}) \end{aligned}$$

  is a Euclidean norm.

  To prove this, we must show that for any $\alpha \in \mathbb{Z}[i]$ and any nonzero $\beta \in \mathbb{Z}[i]$, there exist elements $q, r \in \mathbb{Z}[i]$ with

$$\alpha = q\beta + r \qquad \text{and} \qquad (r = 0 \text{ or } N(r) < N(\beta)). \tag{31}$$

  So let us fix an $\alpha \in \mathbb{Z}[i]$ and a nonzero $\beta \in \mathbb{Z}[i]$. We are looking for elements $q, r \in \mathbb{Z}[i]$ that satisfy (31). We can even replace the "$r = 0$

[69] In more detail: We need to show that for any $a \in \mathbb{Z}$ and any nonzero $b \in \mathbb{Z}$, there exist elements $q, r \in \mathbb{Z}$ with

$$a = qb + r \qquad \text{and} \qquad (r = 0 \text{ or } |r| < |b|).$$

To find these q, r, we divide a by $|b|$ with remainder. Let q_0 and r_0 be the quotient and the remainder that we obtain. If b is positive, we can then take $q = q_0$ and $r = r_0$. If b is negative, then we instead take $q = -q_0$ and $r = r_0$ (because $b = -|b|$).

or $N(r) < N(\beta)$" condition in (31) by the stronger condition "$N(r) < N(\beta)$".

To find the elements q, r we are seeking, we make the following observation: The absolute value $|z|$ of a complex number $z = a + bi$ (with $a, b \in \mathbb{R}$) is defined as $|z| = \sqrt{a^2 + b^2}$, whereas the norm $N(z)$ of a Gaussian integer $z = a + bi$ (with $a, b \in \mathbb{Z}$) is defined as $N(z) = a^2 + b^2$. Thus, any $z \in \mathbb{Z}[i]$ satisfies $N(z) = |z|^2$. Hence, we have the following chain of equivalences:

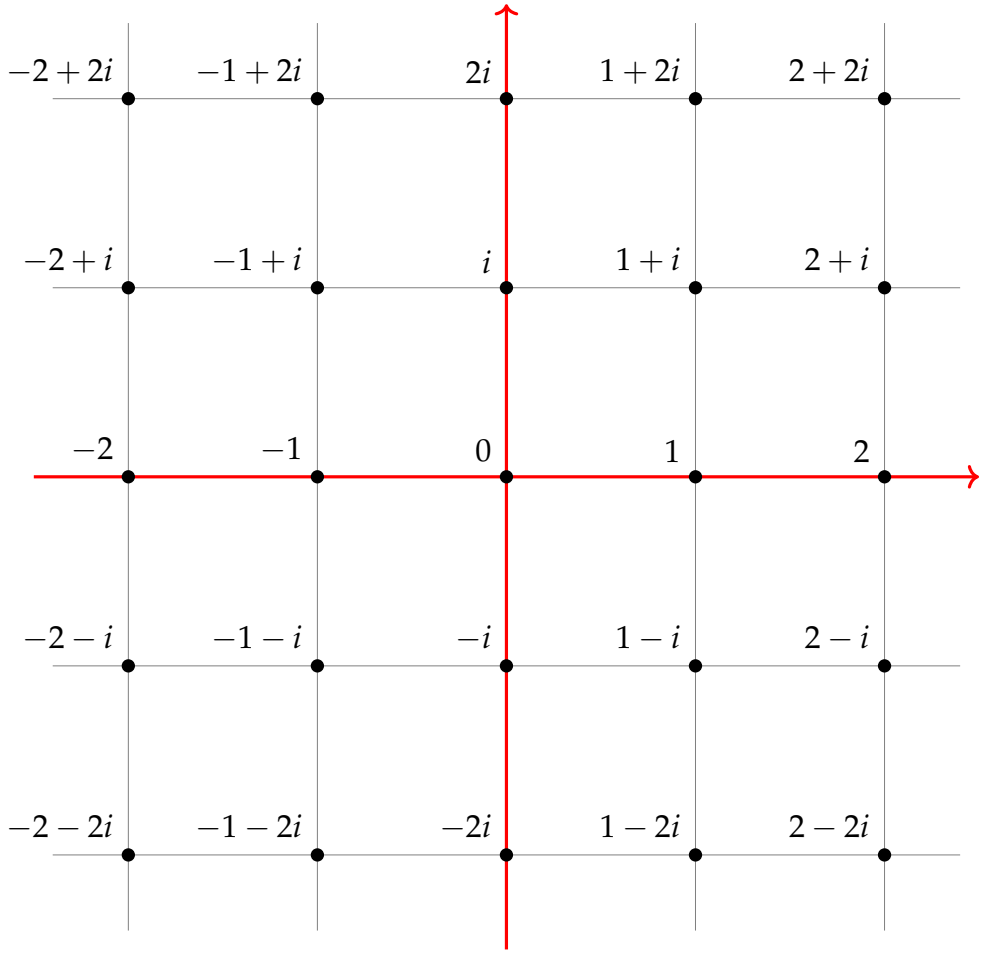
$$\begin{aligned}(N(r) < N(\beta)) &\iff \left(|r|^2 < |\beta|^2\right) \iff (|r| < |\beta|) \iff \left(\frac{|r|}{|\beta|} < 1\right) \\ &\iff \left(\left|\frac{r}{\beta}\right| < 1\right) \end{aligned} \tag{32}$$

(since $\dfrac{|z|}{|w|} = \left|\dfrac{z}{w}\right|$ for any two complex numbers z and $w \neq 0$). Moreover, we have the equivalence

$$(\alpha = q\beta + r) \iff \left(\frac{\alpha}{\beta} = q + \frac{r}{\beta}\right) \iff \left(\frac{\alpha}{\beta} - q = \frac{r}{\beta}\right). \tag{33}$$

Now, recall that we are looking for elements $q, r \in \mathbb{Z}[i]$ that satisfy $\alpha = q\beta + r$ and $N(r) < N(\beta)$. In view of (32) and (33), this means that we are looking for elements $q, r \in \mathbb{Z}[i]$ that satisfy $\dfrac{\alpha}{\beta} - q = \dfrac{r}{\beta}$ and $\left|\dfrac{r}{\beta}\right| < 1$. Equivalently, we can look for a Gaussian integer $q \in \mathbb{Z}[i]$ satisfying $\left|\dfrac{\alpha}{\beta} - q\right| < 1$ (because once such a q has been found, we can set $r = \alpha - q\beta$ and obtain $\dfrac{r}{\beta} = \dfrac{\alpha - q\beta}{\beta} = \dfrac{\alpha}{\beta} - q$, so that $\dfrac{\alpha}{\beta} - q = \dfrac{r}{\beta}$ and $\left|\dfrac{r}{\beta}\right| = \left|\dfrac{\alpha}{\beta} - q\right| < 1$). But finding such a q is easy if you remember the geometric meaning of the Gaussian integers: The Gaussian integers are the lattice points of a

square lattice in the plane:



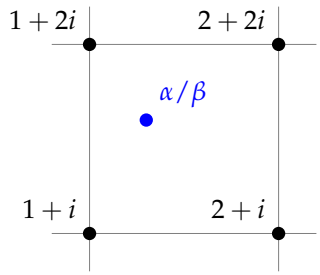
(imagine the lattice being extended to infinity in all four directions). So a Gaussian integer $q \in \mathbb{Z}[i]$ satisfying $\left|\frac{\alpha}{\beta} - q\right| < 1$ simply means a lattice point at a distance[70] less than 1 from the point $\frac{\alpha}{\beta}$. Geometrically, it is easy to see that such a lattice point exists (since the point $\frac{\alpha}{\beta}$ must lie in one of the squares of the lattice, and then have distance $< \frac{\sqrt{2}}{2}$ from one of

[70] The **distance** between two complex numbers x and y is defined to be the real number $|x - y|$.

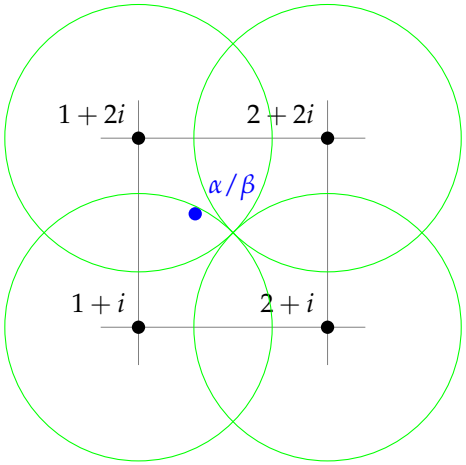
the four vertices of the square[71]; but this entails that $\frac{\alpha}{\beta}$ has distance < 1 from this latter vertex[72]). This can also be proved algebraically[73]. Thus, we have found q.

(A slightly restated version of this proof can be found in the proof of Theorem 3.1 in Keith Conrad's *The Gaussian integers* (see `https://kconrad.`

[71] Here is a close-up picture of the square (with one possible location of $\frac{\alpha}{\beta}$):



I am claiming that the point $\frac{\alpha}{\beta}$ has distance $< \frac{\sqrt{2}}{2}$ from one of the four vertices of the square in which it lies. The easiest way to see this geometrically is to draw circles of radius $\frac{\sqrt{2}}{2}$ around the vertices of the square, and convince yourself that these circles cover the entire square:



.

[72] since $\frac{\sqrt{2}}{2} < 1$

[73] *Proof.* Write the point $\frac{\alpha}{\beta}$ as $x + yi$, where x and y are real numbers. Each real number z has distance $\leq \frac{1}{2}$ from the nearest integer (which is either $\lfloor z \rfloor$ or $\lceil z \rceil$). Thus, x has distance $\leq \frac{1}{2}$ from some integer n, and likewise y has distance $\leq \frac{1}{2}$ from some integer m. Consider these n and m. Then, $|x - n| \leq \frac{1}{2}$ and $|y - m| \leq \frac{1}{2}$. Since n and m are integers, we have

`math.uconn.edu/math5230f12/handouts/Zinotes.pdf`).)

- The ring
$$\mathbb{Z}\left[\sqrt{-2}\right] := \left\{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\right\}$$
(this is another subring of $\mathbb{C}$, since $\sqrt{-2} = \sqrt{2}i$) is Euclidean, too. (See Exercise 2.13.1 for a proof.)

- The ring
$$\mathbb{Z}\left[\sqrt{-3}\right] := \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\right\}$$
(this is another subring of $\mathbb{C}$, since $\sqrt{-3} = \sqrt{3}i$) is **not** Euclidean. (For a proof, see `https://math.stackexchange.com/questions/115934` or Exercise 2.16.6 below.)

  However, there is a slightly larger ring that is Euclidean: namely, the so-called **ring of Eisenstein integers**, defined as
$$\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}$$
for $\omega = \dfrac{-1+\sqrt{-3}}{2}$. (See Exercise 2.13.3 below for the proof that this ring is Euclidean.)

- The ring
$$\mathbb{Z}\left[\sqrt{2}\right] := \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$$

$n + mi \in \mathbb{Z}[i]$, so that $n + mi$ is a lattice point. However, $\dfrac{\alpha}{\beta} = x + yi$, so that

$$\frac{\alpha}{\beta} - (n + mi) = (x + yi) - (n + mi) = (x - n) + (y - m)\, i.$$

Hence,

$$\begin{aligned}
\left|\frac{\alpha}{\beta} - (n + mi)\right| &= |(x - n) + (y - m)\, i| \\
&= \sqrt{(x-n)^2 + (y-m)^2} \qquad \left(\begin{array}{c}\text{by the definition of the absolute}\\ \text{value of a complex number,}\\ \text{since } x-n \text{ and } y-m \text{ are reals}\end{array}\right) \\
&= \sqrt{|x-n|^2 + |y-m|^2} \\
&\leq \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} \qquad \left(\text{since } |x-n| \leq \frac{1}{2} \text{ and } |y-m| \leq \frac{1}{2}\right) \\
&= \sqrt{\frac{1}{2}} = \frac{\sqrt{2}}{2} < 1.
\end{aligned}$$

Thus, the lattice point $n + mi$ has a distance of < 1 from the point $\dfrac{\alpha}{\beta}$.

(this is a subring of $\mathbb{R}$) is Euclidean. A Euclidean norm for it is the map

$$\begin{aligned} &\mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{N}, \\ &a + b\sqrt{2} \mapsto \left|a^2 - 2b^2\right| \qquad (\text{for } a, b \in \mathbb{Z}). \end{aligned}$$

(See Exercise 2.13.2 below for a proof.)

- The ring
$$\mathbb{Z}\left[\sqrt{14}\right] := \left\{a + b\sqrt{14} \mid a, b \in \mathbb{Z}\right\}$$
is Euclidean. A Euclidean norm for it is notoriously hard to construct (in particular, it is **not** the map sending each $a + b\sqrt{14}$ to $\left|a^2 - 14b^2\right|$). See `https://math.stackexchange.com/questions/1148364` .
- The ring $\mathbb{Z}\left[\sqrt{5}\right] := \left\{a + b\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$ is **not** Euclidean.
- For each $n \in \mathbb{Z}$, the ring $\mathbb{Z}/n$ is Euclidean (but is not a Euclidean domain in most cases). A Euclidean norm N on this ring is easy to construct (e.g., for $n > 0$, we can define $N(\overline{a})$ to be the smallest nonnegative integer in the residue class $\overline{a}$).

Thus, we have now seen multiple examples and non-examples of Euclidean rings and Euclidean domains. Now, we claim that all Euclidean domains have a property that we have previously proved for $\mathbb{Z}$:

Proposition 2.13.3. Let R be a Euclidean ring. Then, any ideal of R is principal.

Proof. The same argument we used for proving Proposition 2.13.1 can easily be adapted to prove Proposition 2.13.3. The main change is that you now need to take a nonzero $b \in I$ with smallest possible $N(b)$. (Here, N is a fixed Euclidean norm on R.) For details, see [DumFoo04, §8.1, proof of Proposition 1]. □

Remark 2.13.4. Euclidean domains are much more well-studied than Euclidean rings. Some authors go as far as using the word "Euclidean ring" as a synonym for "Euclidean domain" (which, of course, conflicts with our definition of the former).

See `https://kconrad.math.uconn.edu/blurbs/ringtheory/euclideanrk.pdf` for more about Euclidean domains.

Exercise 2.13.1. Prove that the ring

$$\mathbb{Z}\left[\sqrt{-2}\right] := \left\{a + b\sqrt{-2} \mid a, b \in \mathbb{Z}\right\}$$

is Euclidean, and that the map

$$\begin{aligned} N : \mathbb{Z}\left[\sqrt{-2}\right] &\to \mathbb{N}, \\ a + b\sqrt{-2} &\mapsto a^2 + 2b^2 \qquad (\text{for } a, b \in \mathbb{Z}) \end{aligned}$$

is a Euclidean norm for it.

[**Hint:** Imitate the above proof for $\mathbb{Z}[i]$.]

Exercise 2.13.2. Prove that the ring

$$\mathbb{Z}\left[\sqrt{2}\right] := \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$$

is Euclidean, and that the map

$$\begin{aligned} N : \mathbb{Z}\left[\sqrt{2}\right] &\to \mathbb{N}, \\ a + b\sqrt{2} &\mapsto \left|a^2 - 2b^2\right| \qquad (\text{for } a, b \in \mathbb{Z}) \end{aligned}$$

is a Euclidean norm for it.

[**Hint:** First, prove that the latter map N is multiplicative – i.e., that it satisfies $N(xy) = N(x) \cdot N(y)$ for all $x, y \in \mathbb{Z}\left[\sqrt{2}\right]$. Moreover, this still holds if we extend N to a map from $\mathbb{Q}\left[\sqrt{2}\right]$ to $\mathbb{Q}$ (defined by the same formula).]

Exercise 2.13.3. Let ω denote the complex number $\dfrac{-1+\sqrt{-3}}{2} \in \mathbb{C}$.

(a) Prove that $\omega^3 = 1$ and $\omega^2 + \omega + 1 = 0$.

(b) Prove that $|a + b\omega| = \sqrt{a^2 - ab + b^2}$ for any $a, b \in \mathbb{R}$.

(c) Define a subset $\mathbb{Z}[\omega]$ of $\mathbb{C}$ by

$$\mathbb{Z}[\omega] := \{a + b\omega \mid a, b \in \mathbb{Z}\}.$$

Prove that $\mathbb{Z}[\omega]$ is a subring of $\mathbb{C}$. (It is called the ring of **Eisenstein integers**.)

(d) Prove that $\mathbb{Z}\left[\sqrt{-3}\right]$ is a subring of $\mathbb{Z}[\omega]$.

(e) Prove that the ring $\mathbb{Z}[\omega]$ is Euclidean, and that the map

$$\begin{aligned} N : \mathbb{Z}[\omega] &\to \mathbb{N}, \\ a + b\omega &\mapsto a^2 - ab + b^2 \qquad (\text{for } a, b \in \mathbb{Z}) \end{aligned}$$

is a Euclidean norm for it.

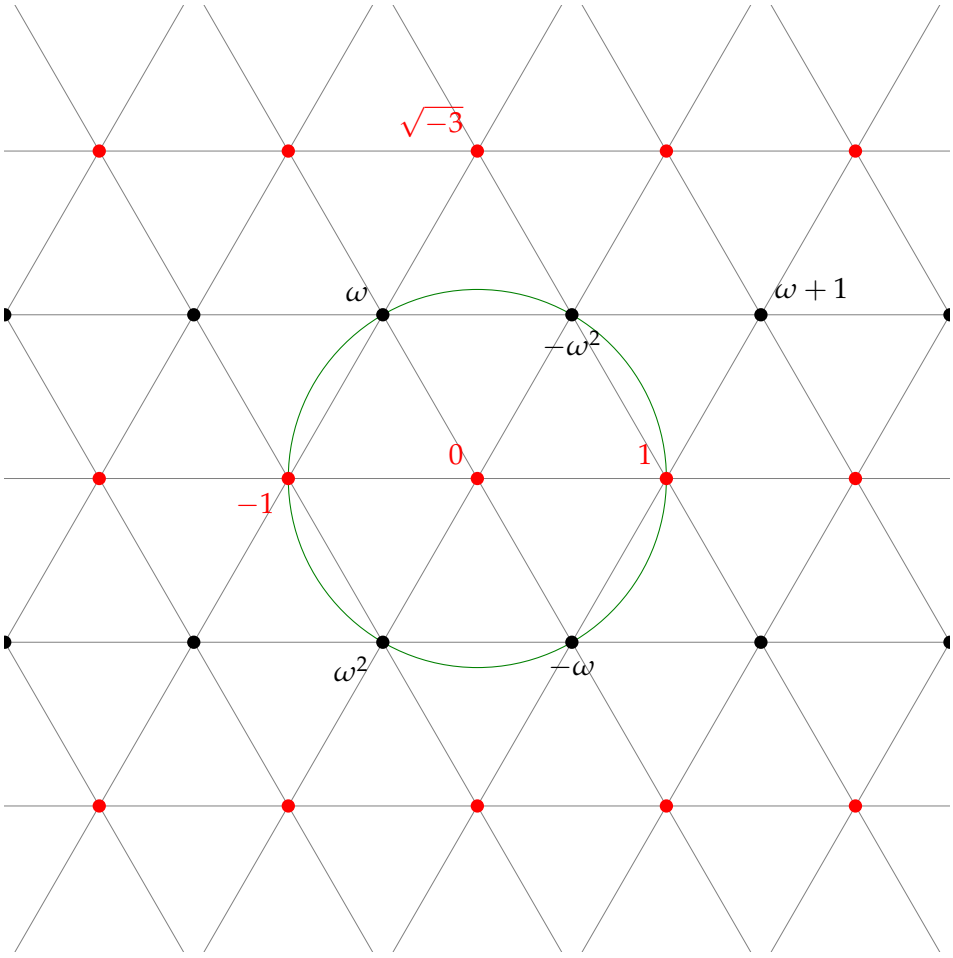
(f) Find all units of the ring $\mathbb{Z}[\omega]$.

(g) Show that an element $a + b\omega$ of $\mathbb{Z}[\omega]$ (with $a, b \in \mathbb{Z}$) belongs to $\mathbb{Z}\left[\sqrt{-3}\right]$ if and only if b is even.

(h) Consider $\mathbb{Z}[\omega]$ as an additive group, and $\mathbb{Z}\left[\sqrt{-3}\right]$ as a subgroup of $\mathbb{Z}[\omega]$. Prove that this subgroup $\mathbb{Z}\left[\sqrt{-3}\right]$ has index 2 in $\mathbb{Z}[\omega]$ (that is, the quotient group $\mathbb{Z}[\omega] / \mathbb{Z}\left[\sqrt{-3}\right]$ has size 2).

(i) If $z \in \mathbb{Z}[\omega]$ is any Eisenstein integer, then at least one of the three numbers z, $z\omega$, $z\omega^2$ belongs to $\mathbb{Z}\left[\sqrt{-3}\right]$.

[**Hint:** Geometrically speaking, the three complex numbers 1, ω, ω^2 are the vertices of an equilateral triangle inscribed in the unit circle. The elements of $\mathbb{Z}[\omega]$ are the grid points of a triangular lattice that looks as follows (imagine the picture extended to infinity all on sides):



(where the red points are the ones that belong to $\mathbb{Z}\left[\sqrt{-3}\right]$).]

Exercise 2.13.4. Fix an integer m. Consider the ring R_m defined in Exercise 2.3.2. Prove that R_m is a Euclidean domain. More concretely:

(a) For every nonzero $r \in R_m$, we let $\widetilde{r}$ be the smallest positive numerator of r.

(A "numerator" of a rational number r means an integer of the form dr with $d \in \mathbb{Z}$. In other words, if we write r as a ratio of two integers, then the numerator of this fraction is called a "numerator" of r. For example, 7 is a numerator of $\frac{7}{9}$, but so are 14 and 21 and -14 and so on.)

Prove that $\widetilde{r}$ exists.

(b) Prove that the map

$$\begin{aligned} N : R_m &\to \mathbb{N}, \\ r &\mapsto \widetilde{r} \qquad \text{for } r \neq 0, \\ 0 &\mapsto 0 \end{aligned}$$

is a Euclidean norm on R_m.

Exercise 2.13.5. Let $N_2 : \mathbb{Z} \to \mathbb{N}$ be the map that sends 0 to 0, while sending each nonzero integer n to $\lfloor \log_2 |n| \rfloor$. (Recall that $\lfloor x \rfloor$ denotes the **floor** of a real number x – that is, the largest integer that is $\leq x$. Thus, $N_2(7) = \lfloor \log_2 |7| \rfloor = \lfloor 2.807\ldots \rfloor = 2$.)

Prove that N_2 is a Euclidean norm on $\mathbb{Z}$.

Exercise 2.13.6. Let A and B be two Euclidean rings. Prove that the ring $A \times B$ is again Euclidean.

Exercise 2.13.7. Let R be a Euclidean ring. Let I be an ideal of R. Show that the quotient ring R/I is again Euclidean.

[**Hint:** Let N be a Euclidean norm on R. Define a norm $\overline{N}$ on R/I by setting $\overline{N}(x) = \min\{N(a) \mid a \in x\}$ for all residue classes $x \in R/I$.]

Exercise 2.13.8. Prove that if we replace the condition "$r = 0$ or $N(r) < N(b)$" by "$N(r) < N(b)$" in Definition 2.13.2, then the resulting notion of a Euclidean ring will be equivalent to ours (even though a given Euclidean norm N might no longer qualify as a Euclidean norm).

2.13.3. The (extended) Euclidean algorithm

Imagine that you are given some ideal I of $\mathbb{Z}$. Proposition 2.13.1 then guarantees that this ideal I is principal, i.e., has the form $I = c\mathbb{Z}$ for a single integer c. Now, suppose you want to actually find this c.

Our above proof of Proposition 2.13.1 is of some help here: It guarantees that $I = c\mathbb{Z}$, where c is the smallest positive integer contained in I (or 0 if no such integer exists)[74]. Depending on how much you know about I, this can make c easy to find. But this is not automatic. Indeed, in some cases (e.g., when

[74] This c was denoted by b in our proof of Proposition 2.13.1.

I is given as the set of all integers satisfying some complicated uncomputable condition), finding an integer $c \in \mathbb{Z}$ satisfying $I = c\mathbb{Z}$ is even algorithmically impossible[75], even though such a c exists for theoretical reasons.

However, if the ideal I is defined in a sufficiently simple way, then this problem might be algorithmically solvable. A particularly well-behaved example is when I is given in the form $I = a\mathbb{Z} + b\mathbb{Z}$ for two explicitly provided integers a and b. In this case, finding an integer c satisfying $I = c\mathbb{Z}$ amounts to finding the greatest common divisor $\gcd(a, b)$ of a and b (because Proposition 2.11.3 **(c)** yields that $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\,\mathbb{Z}$). The famous Euclidean algorithm computes this $\gcd(a, b)$, thus solving the problem of finding c. Furthermore, a variant of this algorithm – known as the **extended Euclidean algorithm** – computes two integers x and y satisfying $\gcd(a, b) = xa + yb$. These integers x and y "make the equality $a\mathbb{Z} + b\mathbb{Z} = \gcd(a, b)\,\mathbb{Z}$ explicit" (in the sense that they allow us to actually express an element of $\gcd(a, b)\,\mathbb{Z}$ in the form "a times an integer plus b times an integer", rather than merely guaranteeing that such an expression exists).

These two Euclidean algorithms (the usual one and the extended one) can be found in any textbook on elementary number theory (see, e.g., [Stein09, Algorithm 2.3.7] for the extended Euclidean algorithm; the usual can easily be obtained from it). Here, however, we are interested not in the integers but in their various generalizations. For what other commutative rings R do such algorithms (expressing an ideal of the form $aR + bR$ as a principal ideal cR) exist?[76]

Let us make this question more precise: We want an algorithm which, if you input two elements $a, b \in R$, outputs an element $c \in R$ that satisfies $aR + bR = cR$. Ideally, this algorithm should also provide "evidence" for this equality $aR + bR = cR$, that is, a way to express every element of cR as an element of $aR + bR$ and vice versa. In order to express every element of cR as an element of $aR + bR$, it suffices to write c as a sum $xa + yb$ with $x, y \in R$. In order to express every element of $aR + bR$ as an element of cR, it suffices to write a in the form $a = cu$ for some $u \in R$, and to write b in the form $b = cv$ for some $v \in R$. So we want our algorithm to output not only c but also x, y, u and v. In other words, we want it to output the 5-tuple (x, y, c, u, v) (there is nothing special about the order in which I listed its entries; I just picked it to put the most important output, c, in the middle).

Let me give this 5-tuple a name:

[75] Appreciators of theoretical computer science will easily concoct an ideal I of $\mathbb{Z}$ such that finding an integer c satisfying $I = c\mathbb{Z}$ is tantamount to solving the halting problem (which is known to be algorithmically unsolvable).

[76] Let me stress that the aR, bR and cR here are ideals. The "$+$" sign in "$aR + bR$" stands for a sum of ideals. Thus, the equality $aR + bR = cR$ has nothing to do with the equality $a + b = c$. (Indeed, the former equality neither implies nor follows from the latter; the ideals $(a + b)\,R$ and $aR + bR$ are not the same.)

Translated into the language of elements, the equality $aR + bR = cR$ says that the elements that can be written as a multiple of a plus a multiple of b are precisely the multiples of c.

Definition 2.13.5. Let a and b be two elements of a commutative ring R. Then, a **Bezout 5-tuple** for (a, b) shall mean

$$\text{a 5-tuple } (x, y, c, u, v) \in R^5 \text{ that satisfies}$$
$$xa + yb = c \text{ and } a = cu \text{ and } b = cv.$$

Example 2.13.6. Let $R = \mathbb{Z}$ and $a = 10$ and $b = 6$. Then, $(-1, 2, 2, 5, 3)$ is a Bezout 5-tuple for (a, b), since it satisfies $(-1)\, a + 2b = (-1)\, 10 + 2 \cdot 6 = 2 = c$ and $a = 10 = 2 \cdot 5 = cu$ and $b = 6 = 2 \cdot 3 = cv$. Another Bezout 5-tuple for (a, b) is $(1, -2, -2, -5, -3)$. Yet another is $(2, -3, 2, 5, 3)$. There are infinitely many Bezout 5-tuples (x, y, c, u, v) for (a, b), since we can always replace x and y by $x + 3$ and $y - 5$ without changing $xa + yb$.

For a general commutative ring R, a Bezout 5-tuple for (a, b) will not always exist. But when it does, it answers all our questions about the ideal $aR + bR$:

Proposition 2.13.7. Let R be a commutative ring. Let $a, b \in R$ be arbitrary, and let (x, y, c, u, v) be a Bezout 5-tuple for (a, b). Then:

(a) We have $aR + bR = cR$.

(b) Any element $ap + bq$ of $aR + bR$ can be explicitly expressed as an element of cR by rewriting it in the form $c\,(up + vq)$.

(c) Any element cr of cR can be explicitly expressed as an element of $aR + bR$ by rewriting it as $axr + byr$.

Proof. We know that (x, y, c, u, v) is a Bezout 5-tuple for (a, b). Thus, the definition of a Bezout 5-tuple yields that $xa + yb = c$ and $a = cu$ and $b = cv$.

Now, any element of $aR + bR$ has the form $ap + bq$ for some $p, q \in R$, and therefore belongs to cR, since

$$\underbrace{a}_{=cu} p + \underbrace{b}_{=cv} q = cup + cvq = c \underbrace{\left(up + vq\right)}_{\in R} \in cR.$$

This shows that $aR + bR \subseteq cR$.

On the other hand, any element of cR has the form cr for some $r \in R$, and therefore belongs to $aR + bR$, since

$$\underbrace{c}_{=xa+yb} r = (xa + yb)\, r = a \underbrace{xr}_{\in R} + b \underbrace{yr}_{\in R} \in aR + bR.$$

This shows that $cR \subseteq aR + bR$. Combining this with $aR + bR \subseteq cR$, we obtain $aR + bR = cR$. Therefore, part **(a)** is proved.

Part **(b)** was proved above (in the process of proving $aR + bR \subseteq cR$), and part **(c)** was proved as well (in the process of showing that $cR \subseteq aR + bR$). Thus, Proposition 2.13.7 is fully proved. □

Thus, our problem about $aR + bR$ is now reduced to the following: Given two elements a and b of a commutative ring R, when can we algorithmically find a Bezout 5-tuple for (a, b) ?

For most rings R, the answer is "no" already because such a Bezout 5-tuple doesn't always exist. However, the answer is "yes" when R is a Euclidean ring. To be more precise, it is "yes" when R is a Euclidean ring satisfying certain computability requirements:

Theorem 2.13.8. Let R be a Euclidean ring.

(a) Then, for any two elements $a, b \in R$, there exists a Bezout 5-tuple for (a, b).

(b) Moreover, there exists an algorithm that computes a Bezout 5-tuple for any pair $(a, b) \in R^2$, provided that the Euclideanness of R itself is algorithmic[77].

Proof. **(a)** Since R is Euclidean, there exists a Euclidean norm $N : R \to \mathbb{N}$. Consider this norm N.

We shall prove Theorem 2.13.8 **(a)** by strong induction on the nonnegative integer $N(b)$.

So let $n \in \mathbb{N}$. As the induction hypothesis, we assume that Theorem 2.13.8 **(a)** is true for any pair $(a, b) \in R^2$ satisfying $N(b) < n$. We must now prove that Theorem 2.13.8 **(a)** holds for any pair $(a, b) \in R^2$ satisfying $N(b) = n$.

So let $(a, b) \in R^2$ be a pair satisfying $N(b) = n$. Our goal is to prove that Theorem 2.13.8 **(a)** holds for this pair, i.e., to prove that there exists a Bezout 5-tuple for (a, b).

To construct this 5-tuple, we distinguish between two cases:

[77] By "the Euclideanness of R itself is algorithmic", we mean the following:

- There are algorithms for adding, subtracting and multiplying arbitrary elements of R.
- There is an algorithm for checking whether two given elements of R are equal.
- There is a Euclidean norm $N : R \to \mathbb{N}$ that can be computed by an algorithm (i.e., there is an algorithm that computes $N(a)$ for each $a \in R$).
- The q and the r in Definition 2.13.2 **(b)** can be computed an algorithm (i.e., there exists an algorithm that, if you input an element $a \in R$ and a nonzero element $b \in R$, will output a pair $(q, r) \in R^2$ such that $a = qb + r$ and ($r = 0$ or $N(r) < N(b)$)).

Actually, the computability of the norm N is not even necessary for our algorithm.

- *Case 1:* Assume that $b = 0$. Then, we set $(x, y, c, u, v) := (1, 0, a, 1, 0)$. It is easy to see that this is a Bezout 5-tuple for (a, b) (since $1a + 0b = a$ and $a = a \cdot 1$ and $b = 0 = a \cdot 0$). Hence, we have found a Bezout 5-tuple for (a, b) in Case 1.

- *Case 2:* Assume that $b \neq 0$. Since N is a Euclidean norm, there exist elements $q, r \in R$ with $a = qb + r$ and ($r = 0$ or $N(r) < N(b)$) (by Definition 2.13.2 **(b)**). Consider these elements q, r. From $a = qb + r$, we obtain $a - qb = r$. We have $r = 0$ or $N(r) < N(b)$; thus, we can break this case into two subcases:

  - *Subcase 2.1:* Assume that $r = 0$. Then, $a = qb + \underbrace{r}_{=0} = qb = bq$.

    Hence, $(0, 1, b, q, 1)$ is a Bezout 5-tuple for (a, b) (since $0a + 1b = b$ and $a = bq$ and $b = b \cdot 1$).

  - *Subcase 2.2:* Assume that $N(r) < N(b)$. Thus, by the induction hypothesis, Theorem 2.13.8 **(a)** is true for the pair (b, r) instead of (a, b). In other words,

    $$\text{there exists a Bezout 5-tuple } (x, y, c, u, v) \text{ for this pair } (b, r).$$

    Consider this 5-tuple. By the definition of a Bezout 5-tuple, it satisfies $xb + yr = c$ and $b = cu$ and $r = cv$.

    Now,

    $$(y,\ x - qy,\ c,\ qu + v,\ u) \text{ is a Bezout 5-tuple for the pair } (a, b),$$

    because

    $$ya + (x - qy)\, b = ya + xb - qyb = xb + y\underbrace{(a - qb)}_{=r} = xb + yr = c$$

    and

    $$a = q\underbrace{b}_{=cu} + \underbrace{r}_{=cv} = qcu + cv = c(qu + v)$$

    and

    $$b = cu.$$

    Thus, we have found a Bezout 5-tuple for (a, b) in Case 2 (since we have found such a tuple in each of the two subcases).

We have now found a Bezout 5-tuple for the pair (a, b) in each of the above three cases. Hence, such a 5-tuple always exists. This completes the induction step, and thus Theorem 2.13.8 **(a)** is proved.

(b) Our inductive proof of Theorem 2.13.8 **(a)** above gives a recursive algorithm for finding a Bezout 5-tuple for the pair (a, b). Indeed, depending on the

case and the subcase, it either solves this problem directly (in Case 1 and in Subcase 2.1), or reduces it to the analogous problem for a different pair (a, b) with a smaller value of $N(b)$ (in Subcase 2.2). Thus, by a (finite) sequence of such reductions, we eventually arrive at a pair for which we can directly find a Bezout 5-tuple, and thus we can do so for the original pair as well.

Here is this algorithm, spelled out as code (in Python):[78]

```
def bezout_5tuple(a, b):
        if b == 0:  # Case 1
                return (1, 0, a, 1, 0)
        q, r = quo_rem(a, b)
        if r == 0:  # Subcase 2.1
                return (0, 1, b, q, 1)
        # Subcase 2.2
        (x, y, c, u, v) = bezout_5tuple(b, r)
        return (y, x - q*y, c, q*u + v, u)
```

This function returns a Bezout 5-tuple for (a, b). □

Let us give an example for the algorithm that comes out of our above proof of Theorem 2.13.8 **(b)**. For simplicity, we use a very familiar ring – namely, $\mathbb{Z}$ – and a very familiar Euclidean norm:

- Let R be the Euclidean ring $\mathbb{Z}$, and let N be the Euclidean norm on $\mathbb{Z}$ that sends each integer a to $|a|$. We aim to compute a Bezout 5-tuple for the pair $(6, 14)$.

  The existence of such a 5-tuple is guaranteed by Theorem 2.13.8 **(a)** (applied to $a = 6$ and $b = 14$). Thus, in order to find such a 5-tuple, we inspect the proof of Theorem 2.13.8 **(a)** we gave above, in the specific situation when $a = 6$ and $b = 14$. This situation is an instance of Case 2 in the above proof (since $b \neq 0$), so the first step is to find elements $q, r \in R$ with $a = qb + r$ and ($r = 0$ or $N(r) < N(b)$). Such elements q, r are easily found by standard division with remainder; we obtain $q = 0$ and $r = 6$ (since $a = 6 = \underbrace{0}_{=q} \cdot \underbrace{14}_{=b} + \underbrace{6}_{=r}$ and $N(r) = 6 < 14 = N(b)$). Note that there is a different choice as well[79], but we pick this one.

  Thus, we are in Subcase 2.2 (since $r \neq 0$). To continue, we need to find a Bezout 5-tuple for the pair $(b, r) = (14, 6)$. How do we find such a 5-tuple?

  Again, we inspect the above proof of Theorem 2.13.8 **(a)**, but now for $a = 14$ and $b = 6$. This situation is again an instance of Case 2 (since

[78] The `quo_rem` function, applied to a pair (a, b), is assumed to return a pair (q, r) of elements $q, r \in R$ that satisfy $a = qb + r$ and ($r = 0$ or $N(r) < N(b)$). Such a pair exists, since N is a Euclidean norm.

[79] namely, $q = 1$ and $r = -8$

$b \neq 0$), so the first step is to find elements $q, r \in R$ with $a = qb + r$ and ($r = 0$ or $N(r) < N(b)$). Such elements q, r are easily found by standard division with remainder; we obtain $q = 2$ and $r = 2$ (since $a = 2b + 2$ and $N(2) < N(b)$). Thus, we are again in Subcase 2.2 (since $r \neq 0$). To continue, we need to find a Bezout 5-tuple for the pair $(b, r) = (6, 2)$. How do we find such a 5-tuple?

Again, we inspect the above proof of Theorem 2.13.8 **(a)**, but now for $a = 6$ and $b = 2$. This situation is again an instance of Case 2 (since $b \neq 0$), so the first step is to find elements $q, r \in R$ with $a = qb + r$ and ($r = 0$ or $N(r) < N(b)$). Such elements q, r are easily found by standard division with remainder; we obtain $q = 3$ and $r = 0$. Thus, we are in Subcase 2.1 (since $r = 0$), and we conclude that $(0, 1, b, q, 1) = (0, 1, 2, 3, 1)$ is a Bezout 5-tuple for $(a, b) = (6, 2)$.

Having found this Bezout 5-tuple for $(6, 2)$, we can now go back one step and obtain a Bezout 5-tuple for $(14, 6)$: Namely, as we learned in Subcase 2.2,

> if (x, y, c, u, v) is a Bezout 5-tuple for the pair (b, r) (where $a = qb + r$),
> then $(y,\ x - qy,\ c,\ qu + v,\ u)$ is a Bezout 5-tuple for the pair (a, b).

Thus, knowing that $(0, 1, 2, 3, 1)$ is a Bezout 5-tuple for the pair $(6, 2)$, we conclude (with $a = 14$ and $b = 6$ and $q = 2$ and $r = 2$) that

$$(1,\ 0 - 2 \cdot 1,\ 2,\ 2 \cdot 3 + 1,\ 3) = (1,\ -2,\ 2,\ 7,\ 3)$$

is a Bezout 5-tuple for the pair $(14, 6)$.

Having found this Bezout 5-tuple for $(14, 6)$, we can now go back one more step and obtain a Bezout 5-tuple for $(6, 14)$: Namely, as we learned in Subcase 2.2,

> if (x, y, c, u, v) is a Bezout 5-tuple for the pair (b, r) (where $a = qb + r$),
> then $(y,\ x - qy,\ c,\ qu + v,\ u)$ is a Bezout 5-tuple for the pair (a, b).

Thus, knowing that $(1,\ -2,\ 2,\ 7,\ 3)$ is a Bezout 5-tuple for the pair $(14, 6)$, we conclude (with $a = 6$ and $b = 14$ and $q = 0$ and $r = 6$) that

$$(-2,\ 1 - 0 \cdot (-2),\ 2,\ 0 \cdot 7 + 3,\ 7) = (-2,\ 1,\ 2,\ 3,\ 7)$$

is a Bezout 5-tuple for the pair $(6, 14)$. This is precisely what we were looking for. (The reader can easily verify that this is really a Bezout 5-tuple for $(6, 14)$, but our proof makes this verification redundant.)

Note that the computation we just showed has a distinctive "there-and-back-again" pattern: In its first half, we have been reducing our problem (to find a Bezout 5-tuple for $(6, 14)$) step-by-step to a simpler version of it (to find a

Bezout 5-tuple for $(6,2)$), which we then solved directly; then, in its second half, we have been retracing our steps backwards to transform the solution of the simpler version into a solution of the original problem. This is typical for recursive algorithms. In our specific case (when $R = \mathbb{Z}$), the first half of our computation is just the familiar Euclidean algorithm for computing the greatest common divisor of two integers a and b. Had we been only looking for this greatest common divisor (which in our case was 2), we could have stopped in the middle. However, to find the entire Bezout 5-tuple for the original pair (a,b), we had to retrace all our steps backwards. Thus, the algorithm we used to find a Bezout 5-tuple is known as the **(generalized) extended Euclidean algorithm**. Euclidean rings owe their name to this very algorithm.

2.14. Principal ideal domains ([DumFoo04, §8.1 and §8.2])

2.14.1. Principal ideal domains

Proposition 2.13.3 is so useful that its conclusion (viz., that any ideal of R is principal) has been given its own name:

Definition 2.14.1. An integral domain R is said to be a **principal ideal domain** (for short, **PID**) if each ideal of R is principal.

Thus, Proposition 2.13.3 yields the following:

Proposition 2.14.2. Any Euclidean domain is a PID.

The converse is not true, although counterexamples are hard to find. One of the simplest is the ring $\mathbb{Z}[\alpha] = \{a + b\alpha \mid a,b \in \mathbb{Z}\}$, where $\alpha = \dfrac{1+\sqrt{-19}}{2}$ (a complex number). (See [DumFoo04, page 282] for a proof that this ring is a PID but not a Euclidean domain.)

2.14.2. Divisibility in commutative rings

Much of the basic theory of commutative rings can be viewed as a project to generalize the classical arithmetic of the integers to wider classes of "numbers". As part of this project, we shall now define gcds and lcms in commutative rings. Our definition will be stated for arbitrary commutative rings, but we will soon see that they behave particularly well for when the ring is a PID (which is why we are only doing this definition now). [80]

[80] The notions of "greatest common divisor" and "lowest common multiple" that we will now introduce are not literal generalizations the corresponding notions from classical arithmetic. See below for the exact relation.

Definition 2.14.3. Let R be a commutative ring.
Let $a \in R$.

(a) A **multiple** of a means an element of the form ac with $c \in R$. In other words, it means an element of the principal ideal aR.

(b) A **divisor** of a means an element $d \in R$ such that a is a multiple of d (that is, $a \in dR$). We write "$d \mid a$" for "d is a divisor of a".

Now, let $a \in R$ and $b \in R$.

(c) A **common divisor** of a and b means an element of R that is a divisor of a and a divisor of b at the same time.

(d) A **common multiple** of a and b means an element of R that is a multiple of a and a multiple of b at the same time.

(e) A **greatest common divisor** (short: **gcd**) of a and b means a common divisor d of a and b such that **every** common divisor of a and b is a divisor of d.

(f) A **lowest common multiple** (short: **lcm**) of a and b means a common multiple m of a and b such that **every** common multiple of a and b is a multiple of m.

The concepts of "multiple" and "divisor" we just introduced are straightforward generalizations of the corresponding concepts from arithmetic[81]. (You recover the latter concepts if you set $R = \mathbb{Z}$.) The notions of "gcd" and "lcm" are a bit subtler: If a and b are two integers, then their greatest common divisor $\gcd(a, b)$ in the sense of classical arithmetic is a gcd of a and b in the sense of Definition 2.14.3 **(e)**; however, so is $-\gcd(a, b)$. So our new notion of a gcd is slightly more liberal than the classical notion, in the sense that it allows for negative gcds. The same holds for lcms. Thus, gcds and lcms in our sense are not literally unique. This is one reason why we said "a gcd" and "a lcm" (rather than "the gcd" and "the lcm") in Definition 2.14.3. Another reason is that a and b might not have any gcd to begin with. (We will later see some examples where this happens.)

Let us first state some basic properties of divisibility:

[81] Here I am assuming that you are using the "right" definitions of the latter concepts. For example, every integer (including 0 itself) is a divisor of 0. Some authors dislike this and prefer to explicitly require 0 to not divide 0; in that case, of course, my definition does not agree with theirs.

Proposition 2.14.4. Let R be a commutative ring. Then:

(a) We have $a \mid a$ for each $a \in R$.

(b) If $a, b, c \in R$ satisfy $a \mid b$ and $b \mid c$, then $a \mid c$.

(c) If $a, b, c \in R$ satisfy $a \mid b$ and $a \mid c$, then $a \mid b + c$.

(d) If $a, b, c, d \in R$ satisfy $a \mid b$ and $c \mid d$, then $ac \mid bd$.

Proof. Easy (and analogous to the classical proofs for $R = \mathbb{Z}$). □

2.14.3. Gcds and lcms

Before we explore gcds and lcms in arbitrary commutative rings, let us record the precise relation between them and the classical arithmetic notions:

Proposition 2.14.5. Let a and b be two integers. Let $g = \gcd(a, b)$ and $\ell = \operatorname{lcm}(a, b)$, where we are using the classical arithmetic definitions of gcd and lcm. Then:

(a) The gcds of a and b (in the sense of Definition 2.14.3 **(e)**) are g and $-g$.

(b) The lcms of a and b (in the sense of Definition 2.14.3 **(f)**) are ℓ and $-\ell$.

Proof. **(a)** It is known from classical arithmetic that g is a common divisor of a and b, and that every common divisor of a and b is a divisor of g. In other words, g is a gcd of a and b in the sense of Definition 2.14.3 **(e)**. It is easy to see that this property is inherited by $-g$ as well (since divisibilities don't change when we replace g by $-g$). Thus, both numbers g and $-g$ are gcds of a and b in the sense of Definition 2.14.3 **(e)**. It remains to show that they are the only gcds of a and b in this sense.

So let u be a gcd of a and b in the sense of Definition 2.14.3 **(e)**. We must show that $u \in \{g, -g\}$.

From the way we introduced u, we know that u is a common divisor of a and b, and that every common divisor of a and b is a divisor of u. The first of these two facts yields that $u \mid g$ (since any common divisor of a and b is a divisor of g); the second yields that $g \mid u$ (since g is a common divisor of a and b, and thus is a divisor of u). Combining $u \mid g$ and $g \mid u$, we find $u = \pm g$. In other words, $u \in \{g, -g\}$. This finishes our proof of part **(a)**.

(b) The proof is similar to that for part **(a)**. □

Now, what about gcds and lcms in other rings? The existence of a gcd is far from god-given, as the following example shows:

Example 2.14.6. Let R be the ring

$$\mathbb{Z}\left[\sqrt{-3}\right] = \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\right\}.$$

Let $a = 4$ and $b = 2\left(1 + \sqrt{-3}\right)$. Then, a and b have no gcd in R; nor do they have an lcm in R. You will prove this in Exercise 2.16.6.

2.14.4. Associate elements

Uniqueness of gcds and lcms is a simpler question: They are rarely unique on the nose, but they are always unique up to multiplication by a unit when the ring is an integral domain. Before we show this, let me introduce a word for this:

Definition 2.14.7. Let R be a commutative ring. Let $a, b \in R$. We say that a is **associate** to b in R (and we write $a \sim b$) if there exists a unit u of R such that $a = bu$.

Instead of saying "a is associate to b", we shall also say that "a and b are associate". (This is justified by the fact – which we will prove in Proposition 2.14.8 – that $\sim$ is an equivalence relation.)

For example:

- Two integers a and b are associate in $\mathbb{Z}$ if and only if $a = \pm b$ (that is, if and only if $a = b$ or $a = -b$).
- Any two nonzero elements a and b of a field are associate in that field (since $\dfrac{a}{b}$ is a unit and satisfies $a = b \cdot \dfrac{a}{b}$). The element 0 is associate only to itself.
- Let F be a field. In the polynomial ring $F[x]$, any nonzero polynomial $f \in F[x]$ is associate to a monic polynomial (since its leading coefficient is a unit, and dividing f by this coefficient results in a monic polynomial).
- It is not hard to prove that the only units of the ring $\mathbb{Z}[i]$ are the four Gaussian integers $1, i, -1, -i$. Thus, two Gaussian integers α and β in $\mathbb{Z}[i]$ are associate if and only if $\alpha \in \{\beta, i\beta, -\beta, -i\beta\}$.

A general property of associateness is the following:

Proposition 2.14.8. Let R be a commutative ring. The relation $\sim$ is an equivalence relation.

Proof. This is fairly straightforward. We need to show that the relation $\sim$ is reflexive, symmetric and transitive.

Reflexivity: Any $a \in R$ satisfies $a \sim a$, since the unity 1_R is a unit and satisfies $a = a1_R$.

Symmetry: If $a, b \in R$ satisfy $a \sim b$, then they also satisfy $b \sim a$. Indeed, $a \sim b$ shows that there is a unit u of R such that $a = bu$; but this unit u clearly has an inverse u^{-1}, which is itself a unit and satisfies $b = au^{-1}$. But this shows that $b \sim a$.

Transitivity: If $a, b, c \in R$ satisfy $a \sim b$ and $b \sim c$, then they also satisfy $a \sim c$. Indeed, there exist two units u and v of R such that $b = cu$ and $a = bv$ (since $b \sim c$ and $a \sim b$); but the product uv of these two units is again a unit, and satisfies $a = \underbrace{b}_{=cu} v = cuv$, so that $a \sim c$. □

Note that an element a of a ring R is associate to 1 if and only if a is a unit.

If two elements a and b of a ring R are associate, then each is a multiple of the other (i.e., we have $a \mid b$ and $b \mid a$). When R is an integral domain, the converse holds as well:

Proposition 2.14.9. Let R be an integral domain. Let $a, b \in R$ be such that $a \mid b$ and $b \mid a$. Then, $a \sim b$.

Proof. From $a \mid b$, we see that there exists an $x \in R$ such that $b = ax$. Consider this x.

From $b \mid a$, we see that there exists a $y \in R$ such that $a = by$. Consider this y.

If $a = 0$, then the claim is easy (indeed, if $a = 0$, then $b = \underbrace{a}_{=0} x = 0$, so that $a = 0 = b$ and thus $a \sim b$). Hence, we WLOG assume that $a \neq 0$.

Now, $a = \underbrace{b}_{=ax} y = axy$. In other words, $a(1 - xy) = 0$. Since $a \neq 0$, we thus conclude $1 - xy = 0$ (since R is an integral domain). In other words, $xy = 1$. Thus, y is a unit (since R is commutative). Hence, from $a = by$, we obtain $a \sim b$. □

Note that Proposition 2.14.9 becomes false if we drop the "integral domain" condition. Some sophisticated counterexamples can be found at `https://math.stackexchange.com/questions/14270/` and in Exercise 6.3.3 below.

Associate elements "look the same" to divisibility, by which I mean that a divisibility relation of the form $a \mid b$ remains equivalent if we replace a by an element associate to a or replace b by an element associate to b. In other words:

Proposition 2.14.10. Let R be a commutative ring. Let $a, b, a', b' \in R$ be such that $a \sim a'$ and $b \sim b'$. Then, $a \mid b$ if and only if $a' \mid b'$.

Proof. $\Longrightarrow$: Assume that $a \mid b$. From $a \sim a'$, we see that $a = a'u$ for some unit u of R. Hence, $a' \mid a$. Also, from $b \sim b'$, we obtain $b' \sim b$ (since Proposition 2.14.8

shows that the relation $\sim$ is symmetric). In other words, $b' = bv$ for some unit v of R. Thus, $b \mid b'$. Hence, $a' \mid a \mid b \mid b'$. Thus, we have proved the "$\Longrightarrow$" direction of Proposition 2.14.10.

$\Longleftarrow$: This is analogous to the "$\Longrightarrow$" direction, since Proposition 2.14.8 shows that the relation $\sim$ is symmetric. □

Exercise 2.14.1. Let R be a commutative ring. Let $a, b, c, d \in R$ satisfy $a \sim b$ and $c \sim d$. Prove that $ac \sim bd$.

2.14.5. Uniqueness of gcds and lcms in an integral domain

We can now state the uniqueness of gcds and lcms in the form in which it does hold:

Proposition 2.14.11. Let R be an integral domain. Let $a, b \in R$. Then:

(a) Any two gcds of a and b are associate (i.e., associate to each other).

(b) Any two lcms of a and b are associate (i.e., associate to each other).

Proof. **(a)** Let c and d be two gcds of a and b. We must show that $c \sim d$.

Any common divisor of a and b is a divisor of c (since c is a gcd of a and b); however, d is a common divisor of a and b (since d is a gcd of a and b). Thus, d is a divisor of c. In other words, $d \mid c$. The same argument, with the roles of c and d swapped, yields $c \mid d$. Hence, Proposition 2.14.9 (applied to c and d instead of a and b) yields $c \sim d$.

(b) Analogous to part **(a)**. □

From Proposition 2.14.11, we recover the fact that gcds and lcms of integers are unique up to sign (since two integers a and b are associate in $\mathbb{Z}$ if and only if $a = \pm b$).

2.14.6. Existence of gcds and lcms in a PID

We have now talked enough about uniqueness; when do gcds and lcms exist? The following fact covers one important case:

Theorem 2.14.12. Let R be a PID. Let $a, b \in R$. Then, there exist a gcd and an lcm of a and b.

This will follow from the following proposition, which characterizes lcms and partly characterizes gcds in terms of principal ideals:

Proposition 2.14.13. Let R be a commutative ring. Let $a, b, c \in R$.

(a) If $aR + bR = cR$, then c is a gcd of a and b.

(b) We have $aR \cap bR = cR$ if and only if c is an lcm of a and b.

Note that $aR + bR = cR$ is an equality between ideals (the $+$ sign on the left hand side is a sum of ideals); it is **not** to be confused with $a + b = c$. Confusingly, $a + b = c$ does **not** imply $aR + bR = cR$ (since there is no "distributivity law" that would equate $(a + b) R$ with $aR + bR$). Instead, it is easy to see that "$aR + bR = cR$" is equivalent to "a and b are multiples of c, and there exist two elements $u, v \in R$ satisfying $c = au + bv$".

Note the difference between the two parts of Proposition 2.14.13: Part **(b)** is an "if and only if", while part **(a)** is only an "if". This is no accident: Proposition 2.14.13 **(a)** cannot be extended to an "if and only if" statement. For example, in the polynomial ring $\mathbb{Q}[x, y]$, the two polynomials x and y have gcd 1; however, 1 is not a $\mathbb{Q}[x, y]$-linear combination of x and y.

Proof of Proposition 2.14.13. **(a)** Assume that $aR + bR = cR$. Thus, $c \in cR = aR + bR$. In other words, there exist $x, y \in R$ such that $c = ax + by$. Hence, if r is a common divisor of a and b, then $r \mid c$ [82]. Thus, we have shown that any common divisor of a and b is a divisor of c.

We have $a \in aR \subseteq aR + bR = cR$. In other words, $c \mid a$. Similarly, $c \mid b$. Hence, c is a common divisor of a and b. Combining this result with the result of the previous paragraph, we conclude that c is a gcd of a and b. This proves Proposition 2.14.13 **(a)**.

(b) Recall that an lcm of a and b was defined (in Definition 2.14.3 **(f)**) to be a common multiple m of a and b with the property that every common multiple of a and b is a multiple of m. Hence, we have the following chain of equivalences:

$$\begin{aligned}
&(c \text{ is an lcm of } a \text{ and } b) \\
&\iff \left(\begin{array}{c} c \text{ is a common multiple of } a \text{ and } b, \text{ and} \\ \text{every common multiple of } a \text{ and } b \text{ is a multiple of } c \end{array} \right) \\
&\iff (c \in aR \cap bR \text{ and every element of } aR \cap bR \text{ is a multiple of } c)
\end{aligned}$$

(since the common multiples of a and b are precisely the elements of $aR \cap bR$).

Now, let us look a bit closer at the statements on the right hand side. The statement "$c \in aR \cap bR$" is equivalent to "$cR \subseteq aR \cap bR$" (indeed, the set $aR \cap bR$ is an ideal of R, and thus it contains the element c if and only if it

[82] *Proof.* Let r be a common divisor of a and b. Thus, $r \mid a$ and $r \mid b$. In other words, we can write a and b in the forms $a = ra'$ and $b = rb'$ for some $a', b' \in R$. Using these a', b', we obtain $c = \underbrace{a}_{=ra'} x + \underbrace{b}_{=rb'} y = ra'x + rb'y = r(a'x + b'y)$, so that $r \mid c$. Qed.

contains all multiples of c; in other words, it contains the element c if and only if it contains the subset cR). The statement "every element of $aR \cap bR$ is a multiple of c" is equivalent to "$aR \cap bR \subseteq cR$" (since cR is the set of all multiples of c). Thus, our chain of equivalences can be continued as follows:

$$\begin{aligned}
&(c \text{ is an lcm of } a \text{ and } b) \\
&\iff \left(\underbrace{c \in aR \cap bR}_{\iff cR \subseteq aR \cap bR} \text{ and } \underbrace{\text{every element of } aR \cap bR \text{ is a multiple of } c}_{\iff aR \cap bR \subseteq cR} \right) \\
&\iff (cR \subseteq aR \cap bR \text{ and } aR \cap bR \subseteq cR) \\
&\iff (aR \cap bR = cR) .
\end{aligned}$$

This proves Proposition 2.14.13 **(b)**. □

Proof of Theorem 2.14.12. The sum $aR + bR$ is an ideal of R, and thus is a principal ideal (since R is a PID). In other words, $aR + bR = cR$ for some $c \in R$. Consider this c. Hence, Proposition 2.14.13 **(a)** yields that c is a gcd of a and b. Hence, a gcd of a and b exists.

The intersection $aR \cap bR$ is an ideal of R, and thus is a principal ideal (since R is a PID). In other words, $aR \cap bR = cR$ for some $c \in R$. Consider this c. Hence, Proposition 2.14.13 **(b)** yields that c is an lcm of a and b. Hence, an lcm of a and b exists. Theorem 2.14.12 is now proven. □

So any two elements of a PID have a gcd and an lcm. If the PID is Euclidean, then the gcd can be computed by the Euclidean algorithm. Indeed, even more generally, if a pair (a, b) of two elements of a commutative ring R has a Bezout 5-tuple (see Definition 2.13.5 for the meaning of this notion), then it has a gcd:

Corollary 2.14.14. Let R be a commutative ring. Let $a, b \in R$. Let (x, y, c, u, v) be a Bezout 5-tuple for (a, b). Then, c is a gcd of a and b.

Proof. Proposition 2.13.7 **(a)** yields that $aR + bR = cR$. Hence, Proposition 2.14.13 **(a)** shows that c is a gcd of a and b. This proves Corollary 2.14.14. □

In a Euclidean ring R, we can use the (generalized) extended Euclidean algorithm (as explained in the proof of Theorem 2.13.8 **(b)**) to compute a Bezout 5-tuple for any pair $(a, b) \in R \times R$. Thus, by Corollary 2.14.14, we can compute a gcd of a and b. (See [DumFoo04, pages 275–276] for an example of this computation.)

2.14.7. More about gcds and lcms

In an integral domain R, the gcd and the lcm of two elements $a, b \in R$ determine one another (up to associates) via the formula

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) \sim ab.$$

This follows from the next exercise ([21w, homework set #2, Exercise 3]), which also shows that the existence of an lcm implies the existence of a gcd:

Exercise 2.14.2. Let R be an integral domain. Let $a \in R$ and $b \in R$. Assume that a and b have an lcm $\ell \in R$. Prove that a and b have a gcd $g \in R$, which furthermore satisfies $g\ell = ab$.

[**Hint:** If u and v are two elements of an integral domain R, with $v \neq 0$, then you can use the notation $\frac{u}{v}$ (or u/v) for the element $w \in R$ satisfying $u = vw$. This element w does not always exist, but when it does, it is unique, so the notation is unambiguous. It is also easy to see that standard rules for fractions, such as $\frac{u}{v} + \frac{x}{y} = \frac{uy+vx}{vy}$ and $\frac{u}{v} \cdot \frac{x}{y} = \frac{ux}{vy}$, hold as long as the fractions $\frac{u}{v}$ and $\frac{x}{y}$ exist.]

The converse of Exercise 2.14.2 is false: The existence of a gcd of two given elements a and b of an integral domain R does not imply the existence of an lcm of these two elements. However, if an integral domain R has a gcd for **each** pair of two elements a and b, then it also has an lcm for each pair. This will be stated as Exercise 2.14.4 below.

First, we state a more basic exercise, which generalizes the well-known property $\gcd(am, bm) = \gcd(a, b) \cdot |m|$ that holds for any three integers a, b, m:

Exercise 2.14.3. Let R be an integral domain. Let $a, b, m \in R$ be arbitrary. Assume that the elements a and b have a gcd g. Assume that the elements am and bm have a gcd h. Prove that $gm \sim h$.

Exercise 2.14.4. Let R be an integral domain. Assume that for every $a, b \in R$, the elements a and b have a gcd. Prove that for every $a, b \in R$, the elements a and b have an lcm.

[**Hint:** Let $a, b \in R$, and assume WLOG that $a, b \neq 0$. Let g be a gcd of a and b. It suffices to show that $\frac{ab}{g}$ is an lcm of a and b. To this purpose, show first that $\frac{ab}{g}$ is a common multiple of a and b. Now, let m be any common multiple of a and b. Let h be a gcd of am and bm. Argue that $ab \mid h \mid gm$ (by Exercise 2.14.3). Conclude that $\frac{ab}{g} \mid m$.]

Exercise 2.14.5. Let R be a PID. Let $a, b, c \in R$ be arbitrary. Prove the following:

(a) If $a \mid bc$, then $a \mid \gcd(a, b)\, c$. (Here and in the rest of this exercise, $\gcd(u, v)$ means some gcd of u and v. We don't care which one we choose, since they are all associate.)

(b) We have $\gcd(a, b) \mid \gcd(a, bc)$.

(c) We have $\gcd(a, bc) \mid \gcd(a, b) \gcd(a, c)$.

(d) We have $\gcd(a, b) \gcd(a, c) \mid a \gcd(b, c)$.

(e) If $\gcd(b, c) = 1$, then $\gcd(a, bc) \sim \gcd(a, b) \gcd(a, c)$.

See [Friedm19] for more about PIDs.

2.15. Unique factorization domains ([DumFoo04, §8.3])

2.15.1. Irreducible and prime elements

The notions of integral domains, of Euclidean domains and of PIDs are abstractions for certain properties that hold for the ring $\mathbb{Z}$: The first one abstracts the fact that products of nonzero integers are nonzero; the second abstracts division with remainder; the third abstracts the fact that each ideal of $\mathbb{Z}$ is principal. As we have seen, PIDs are a weaker form of Euclidean domains. Even weaker is the notion of a **UFD** (short for **Unique Factorization Domain**). This abstracts the existence and the uniqueness of a prime factorization for integers. How do we define it in arbitrary integral domain? What is a good analogue of a prime number in a general integral domain?

There are at least four such analogues. Let us introduce the first two:[83]

Definition 2.15.1. Let R be a commutative ring. Let $r \in R$ be nonzero and not a unit.

(a) We say that r is **irreducible** (in R) if it has the following property: Whenever $a, b \in R$ satisfy $ab = r$, at least one of a and b is a unit.

(b) We say that r is **prime** (in R) if it has the following property: Whenever $a, b \in R$ satisfy $r \mid ab$, we have $r \mid a$ or $r \mid b$.

Let us see what these concepts mean when $R = \mathbb{Z}$. Both notions "irreducible" and "prime" smell like prime numbers, but it is worth being precise: Not only the prime numbers $2, 3, 5, 7, 11, \ldots$ themselves, but also their negatives $-2, -3, -5, -7, -11, \ldots$ fit both bills (i.e., they are irreducible and prime in $\mathbb{Z}$). Let us be more explicit:

Proposition 2.15.2. Let $r \in \mathbb{Z}$. Then, we have the following equivalences:

$$(r \text{ is prime in } \mathbb{Z}) \iff (r \text{ is irreducible in } \mathbb{Z}) \iff (|r| \text{ is a prime number}).$$

Proof. It suffices to prove the three implications

$$(r \text{ is prime in } \mathbb{Z}) \implies (r \text{ is irreducible in } \mathbb{Z});$$
$$(r \text{ is irreducible in } \mathbb{Z}) \implies (|r| \text{ is a prime number});$$
$$(|r| \text{ is a prime number}) \implies (r \text{ is prime in } \mathbb{Z}).$$

[83] The other two are not properties of an element of R, but rather properties of an ideal of R. See Definition 2.17.7 for them.

All of them are LTTR. (The first one is actually a particular case of Proposition 2.15.3 further below. For the other two, it is recommended to WLOG assume that $r \geq 0$, since it is easy to see that none of the three statements involved changes when r is replaced by $-r$.) □

Thus, in the ring $\mathbb{Z}$, being prime and being irreducible is the same thing. What about arbitrary integral domains? Here it is not quite the case, as the following two examples show:

- In the ring $\mathbb{Z}\left[\sqrt{-5}\right]$, the element 3 is irreducible but not prime (in $\mathbb{Z}\left[\sqrt{-5}\right]$). (See [DumFoo04, §8.3] for the proof.)
- Here is an example using polynomials: Define a subset R of the univariate polynomial ring $\mathbb{Q}[x]$ by[84]

$$\begin{aligned} R &= \left\{ f \in \mathbb{Q}[x] \mid \text{the } x^1\text{-coefficient of } f \text{ is } 0 \right\} \\ &= \{ f \in \mathbb{Q}[x] \mid \text{the derivative of } f \text{ at } 0 \text{ is } 0 \} \\ &= \left\{ a_0 + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n \mid n \geq 0 \text{ and } a_0, a_2, a_3, \ldots, a_n \in \mathbb{Q} \right\}. \end{aligned}$$

  It is not hard to see that R is a subring of $\mathbb{Q}[x]$. (Indeed, if f and g are two polynomials whose x^1-coefficients are 0, then the same holds for $f+g$ and $f-g$ and fg. This is easiest to see by computing $f+g$ and $f-g$ and fg and checking that there is no way an x^1-monomial can appear in the results.)

  When we study polynomials later on, we will prove that $\mathbb{Q}[x]$ is an integral domain.[85] Thus, the ring R (being a subring of the integral domain $\mathbb{Q}[x]$) must itself be an integral domain (since a subring of an integral domain is always itself an integral domain[86]).

  Now, the ring R contains no polynomials of degree 1. However, if $a, b \in \mathbb{Q}[x]$ are two polynomials satisfying $x^3 = ab$, then $3 = \deg\left(x^3\right) = \deg(ab) = \deg a + \deg b$, which means that one of the polynomials a and b is either a constant (and thus a unit in R) or has degree 1 (and thus cannot lie in R). This quickly shows that the element x^3 of R is irreducible in R. However, this element is not prime in R (since $x^3 \mid x^2 x^2$ but $x^3 \nmid x^2$).

In each of these two examples, we found an irreducible element that is not prime. Can we do the opposite? No, as the following fact shows:

[84] The "x^1-coefficient" of a polynomial f means the coefficient of f before x^1. For example, the x^1-coefficient of $(x+1)^6$ is 6, whereas the x^1-coefficient of x^2+1 is 0.

[85] This is in fact pretty easy: When you multiply two nonzero polynomials in $\mathbb{Q}[x]$, their leading terms get multiplied, so their degrees get added; thus, the product cannot be 0.

[86] This is obvious if you recall the definition of an integral domain.

Proposition 2.15.3. Let R be an integral domain. Then, any prime element of R is irreducible.

Proof. Let $r \in R$ be prime. We must show that r is irreducible.

So let $a, b \in R$ satisfy $ab = r$. We must show that at least one of a and b is a unit.

We have $ab = r$, so that $r \mid ab$. Since r is prime, we thus obtain $r \mid a$ or $r \mid b$ (by the definition of "prime"). Assume WLOG that $r \mid a$ (since otherwise, we have $r \mid b$, so we can swap a with b to achieve $r \mid a$). Hence, $a = rx$ for some $x \in R$. Consider this x. Now, $r = \underbrace{a}_{=rx} b = rxb$, and therefore $r(1 - xb) = r - rxb = 0$, and thus $1 - xb = 0$ (since $r \neq 0$ and since R is an integral domain). In other words, $xb = 1$. This shows that b is a unit (since R is commutative). Thus we have shown that at least one of a and b is a unit. This completes the proof that r is irreducible. □

In a PID, the converse of Proposition 2.15.3 also holds:

Proposition 2.15.4. Let R be a PID. Let $r \in R$. Then, r is prime if and only if r is irreducible.

Proof. We already showed the "only if" part in Proposition 2.15.3. We thus only need to prove the "if" part.

Assume that r is irreducible. We must show that r is prime.

Let $a, b \in R$ satisfy $r \mid ab$. We must prove that $r \mid a$ or $r \mid b$.

Assume the contrary. Thus, we have neither $r \mid a$ nor $r \mid b$.

There is an $h \in R$ such that $ab = rh$ (since $r \mid ab$). Consider this h.

Since R is a PID, the ideal $aR + rR$ is principal; in other words, there exists some $g \in R$ such that $gR = aR + rR$. Consider this g. Hence, $a \in aR \subseteq aR + rR = gR$; in other words, $g \mid a$.

Also, $r \in rR \subseteq aR + rR = gR$; in other words, g is a divisor of r. However, r is irreducible, and thus every divisor of r is either a unit or associate to r [87]. Thus, g is either a unit or associate to r (since g is a divisor of r). However, if g was associate to r, then we would have $r \mid g \mid a$, which would contradict the fact that we don't have $r \mid a$. Thus, g cannot be associate to r, and so g must be a unit. Therefore, $1 = gg^{-1} \in gR = aR + rR$. Hence, there exist $u, v \in R$ such that $1 = au + rv$.

The same argument (using b instead of a) shows that there exist $u', v' \in R$ such that $1 = bu' + rv'$.

[87] *Proof.* Let d be a divisor of r. We must show that d is either a unit or associate to r.

Indeed, there exists some $q \in R$ such that $r = dq$ (since d is a divisor of r). Consider this q. Since r is irreducible, at least one of d and q is a unit. Hence, d is either a unit or associate to r (because if q is a unit, then d is associate to r (since $r = dq$ yields $r \sim d$ and thus $d \sim r$)).

Now, consider these four elements u, v, u', v'. Multiplying $1 = au + rv$ with $1 = bu' + rv'$ yields

$$\begin{aligned} 1 &= (au + rv)\left(bu' + rv'\right) = \underbrace{ab}_{=rh} uu' + rvbu' + aurv' + rvrv' \\ &= rhuu' + rvbu' + aurv' + rvrv' = r\underbrace{\left(huu' + vbu' + auv' + vrv'\right)}_{\in R} \in rR. \end{aligned}$$

In other words, there exists some $s \in R$ such that $1 = rs$. This shows that r is a unit. This contradicts the fact that r is irreducible. Thus, the proof of Proposition 2.15.4 is complete. □

Exercise 2.15.1. Fix an integer m. Consider the ring R_m from Exercise 2.3.2. Let $r \in R_m$ be nonzero.

(a) Define the **m-core** of r to be the smallest positive integer that is associate to r in R_m. Prove that the m-core of r can be obtained as follows: Pick a $k \in \mathbb{N}$ such that $m^k r \in \mathbb{Z}$ (such a k exists, since $r \in R_m$). Write the prime factorization of $\left|m^k r\right|$ as $\left|m^k r\right| = p_1 p_2 \cdots p_i q_1 q_2 \cdots q_j$, where $p_1, p_2, \ldots, p_i$ are primes that divide m and where $q_1, q_2, \ldots, q_j$ are primes that don't divide m. (The primes don't have to be distinct, and we allow $i = 0$ or $j = 0$.) Then, the m-core of r is $q_1 q_2 \cdots q_j$.

(b) Prove that r is prime in R_m if and only if the m-core of r is a prime number (in the usual number-theoretical sense).

So we have generalized (in two ways, to boot) the notion of a prime number. Let us now generalize prime factorization:

2.15.2. Irreducible factorizations and UFDs

Definition 2.15.5. Let R be an integral domain.

(a) An **irreducible factorization** of an element $r \in R$ means a tuple $(p_1, p_2, \ldots, p_n)$ of irreducible elements $p_1, p_2, \ldots, p_n$ of R such that $r \sim p_1 p_2 \cdots p_n$. (Note that this tuple $(p_1, p_2, \ldots, p_n)$ can be empty; in this case, the product $p_1 p_2 \cdots p_n$ is empty and thus equals to 1. Thus, the empty tuple is an irreducible factorization of any unit of R.)

(b) We say that R is a **unique factorization domain** (or, for short, **UFD**) if each nonzero $r \in R$ satisfies the following two statements:

1. There exists an irreducible factorization of r.
2. The irreducible factorization of r is unique up to associates. This means the following: If $(p_1, p_2, \ldots, p_n)$ and $(q_1, q_2, \ldots, q_m)$

> are two irreducible factorizations of r (so that $p_1, p_2, \ldots, p_n$ and $q_1, q_2, \ldots, q_m$ are irreducible elements of R satisfying $r \sim p_1 p_2 \cdots p_n$ and $r \sim q_1 q_2 \cdots q_m$), then we have $n = m$ and there is a bijection $\alpha : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, m\}$ such that $p_i \sim q_{\alpha(i)}$ for each $i \in \{1, 2, \ldots, n\}$.

My notion of an irreducible factorization differs slightly from that in [DumFoo04] (in that [DumFoo04] requires $r = p_1 p_2 \cdots p_n$, whereas we only require $r \sim p_1 p_2 \cdots p_n$); I hold mine to be slightly better-behaved (for example, $-1 \in \mathbb{Z}$ would not have an irreducible factorization in the [DumFoo04] sense). But my definition of a UFD is equivalent to the one in [DumFoo04], as can be easily seen.

Soon, we will see that every PID is a UFD, and there are more UFDs than PIDs. But first, let us see some examples of UFDs:

- The ring $\mathbb{Z}$ is a UFD. This is, of course, a consequence of Euclid's famous theorem that says that any positive integer can be uniquely decomposed into a product of primes. Our definition of an irreducible factorization differs slightly from the classical notion of a prime factorization in arithmetic, since our irreducible elements are allowed to be negative and since we only require $r \sim p_1 p_2 \cdots p_n$ (rather than $r = p_1 p_2 \cdots p_n$); but it is pretty easy to conciliate the two concepts by replacing all negative factors by their absolute values. For example, $(-3, -2, 2)$ is an irreducible factorization of -12, since $-12 \sim (-3) \cdot (-2) \cdot 2$; but of course it corresponds to the classical prime factorization $12 = 3 \cdot 2 \cdot 2$ of the positive integer 12.
- Any field is a UFD, since every nonzero element is a unit and thus has the empty tuple as its only irreducible factorization.
- We shall soon see that every PID is a UFD.
- The polynomial rings $\mathbb{Z}[x]$ (consisting of polynomials in one variable with integer coefficients) and $\mathbb{Q}[x, y]$ (consisting of polynomials in two variables with rational coefficients) are UFDs, even though they are not PIDs. (Of course, $\mathbb{Q}[x]$ is a PID and thus a UFD as well.)
- The rings

$$\begin{aligned}\mathbb{Z}[2i] &= \{a + b \cdot 2i \mid a, b \in \mathbb{Z}\} \\ &= \{\text{Gaussian integers with an even imaginary part}\}\end{aligned}$$

  and

$$\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\right\}$$

  are not UFDs. (See Exercise 2.16.5 for more on the former ring.)

Previously (in Proposition 2.15.4), we proved that an element of a PID is prime if and only if it is irreducible. We shall now prove the same result for UFDs (which is stronger, as we will soon see that every PID is a UFD):

Proposition 2.15.6. Let R be a UFD. Let $r \in R$. Then, r is prime if and only if r is irreducible.

Proof. $\Longrightarrow$: If r is prime, then r is irreducible (by Proposition 2.15.3).[88]

$\Longleftarrow$: Assume that r is irreducible. We must show that r is prime.

Let $a, b \in R$ satisfy $r \mid ab$. We must prove that $r \mid a$ or $r \mid b$.

Assume the contrary. Thus, neither a nor b is a multiple of r. Hence, in particular, a and b are nonzero (since 0 is a multiple of r). Thus, a and b have irreducible factorizations (since R is a UFD). Let $(p_1, p_2, \ldots, p_n)$ and $(q_1, q_2, \ldots, q_m)$ be irreducible factorizations of a and b. Thus, $p_1, p_2, \ldots, p_n$ and $q_1, q_2, \ldots, q_m$ are irreducible elements of R satisfying

$$a \sim p_1 p_2 \cdots p_n \qquad \text{and} \qquad b \sim q_1 q_2 \cdots q_m.$$

Multiplying $a \sim p_1 p_2 \cdots p_n$ with $b \sim q_1 q_2 \cdots q_m$, we see that

$$ab \sim p_1 p_2 \cdots p_n q_1 q_2 \cdots q_m \tag{34}$$

(since a product of two units is again a unit).

However, $r \mid ab$. Thus, there exists a $q \in R$ such that $ab = rq$. Consider this q. Note that ab is nonzero (since a and b are nonzero, but R is an integral domain). Thus, q is nonzero (since $q = 0$ would imply $ab = r \underbrace{q}_{=0} = 0$, which would contradict the previous sentence). Hence, q has an irreducible factorization (since R is a UFD). Let $(s_1, s_2, \ldots, s_k)$ be an irreducible factorization of q. Thus, $s_1, s_2, \ldots, s_k$ are irreducible elements of R satisfying $q \sim s_1 s_2 \cdots s_k$. From $q \sim s_1 s_2 \cdots s_k$, we obtain $rq \sim r s_1 s_2 \cdots s_k$. Since $ab = rq$, this rewrites as

$$ab \sim r s_1 s_2 \cdots s_k. \tag{35}$$

Now, we conclude that the two tuples

$$(p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_m) \text{ and } (r, s_1, s_2, \ldots, s_k)$$

are two irreducible factorizations of ab (since all their entries $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_m$ and $r, s_1, s_2, \ldots, s_k$ are irreducible, and since (34) and (35) hold). Thus, by the uniqueness condition in the definition of a UFD (which says that the irreducible factorization of an element is unique up to associates), these two tuples must be identical up to associates. In particular, every entry of the second tuple must be associate to some entry of the first. Hence, in

[88] Note that this holds for any integral domain, not just for any UFD.

particular, the entry r of the second factorization must be associate to one of the entries $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_m$ of the first. In other words, we must have

$$r \sim p_i \text{ for some } i \in \{1, 2, \ldots, n\} \tag{36}$$

or

$$r \sim q_j \text{ for some } j \in \{1, 2, \ldots, m\}. \tag{37}$$

However, both of these possibilities lead to contradictions: Indeed, if (36) holds, then we have $r \mid a$ (since[89] $r \sim p_i \mid p_1 p_2 \cdots p_n \sim a$), which contradicts the fact that a is not a multiple of r. Likewise, if (37) holds, then we have $r \mid b$, which contradicts the fact that b is not a multiple of r. Thus, we get a contradiction in either case, and our proof is complete. □

If R is a UFD, and if $r \in R$ is nonzero, then r is associate to a finite product $p_1 p_2 \cdots p_n$ of irreducible elements (by the definition of a UFD). This product can be simplified by collecting associate factors together. For example, in $\mathbb{Z}$, we have

$$-24 = 2 \cdot (-2) \cdot 2 \cdot 3 = -2^3 \cdot 3.$$

Here is what we get in general:

Proposition 2.15.7. Let R be a UFD. Let $r \in R$ be nonzero. Then:

(a) There exists a list $(q_1, q_2, \ldots, q_k)$ of **mutually non-associate** irreducible elements $q_1, q_2, \ldots, q_k \in R$ as well as a list $(e_1, e_2, \ldots, e_k)$ of **positive** integers such that

$$r \sim q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k}.$$

We shall refer to these two lists as the **prime power factorization** of r.

(b) These two lists are unique up to associates and up to simultaneous permutation. (That is, any two prime power factorizations of r can be transformed into one another by replacing the irreducible elements $q_1, q_2, \ldots, q_k$ by associates, and reordering them while carrying the exponents $e_1, e_2, \ldots, e_k$ along with them.)

Proof of Proposition 2.15.7. **(a)** Start with an irreducible factorization of r, and collect associate factors together. For example, if an irreducible factorization of r has the form $(p_1, p_2, p_3, p_4, p_5, p_6)$ with $p_1 \sim p_4$ and $p_2 \sim p_5 \sim p_6$ (and no other associate relations between its entries), then

$$r \sim p_1 p_2 p_3 p_4 p_5 p_6 \sim p_1 p_2 p_3 p_1 p_2 p_2 = p_1^2 p_2^3 p_3,$$

and this is a prime power factorization of r.

[89] We will use the fact that associates divide each other: i.e., if u and v are two elements of R satisfying $u \sim v$, then $u \mid v$.

(b) This follows from the uniqueness of an irreducible factorization (up to associates). □

Proposition 2.15.8. Let R be a UFD. Let $a, b \in R$ be nonzero. Then, there exists a list $(p_1, p_2, \ldots, p_n)$ of **mutually non-associate** irreducible elements $p_1, p_2, \ldots, p_n \in R$ as well as two lists $(e_1, e_2, \ldots, e_n)$ and $(f_1, f_2, \ldots, f_n)$ of **nonnegative** integers such that

$$a \sim p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \qquad \text{and} \qquad b \sim p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}.$$

Proof. Proposition 2.15.7 shows that a and b have prime power factorizations

$$a \sim q_1^{e_1} q_2^{e_2} \cdots q_k^{e_k} \qquad \text{and} \qquad b \sim r_1^{f_1} r_2^{f_2} \cdots r_m^{f_m}.$$

All we need now is to reconcile these prime power factorizations so that they contain the same irreducible elements (albeit possibly with 0 exponents). For this purpose, we do the following steps:

1. If some of the q_i are associate to some of the r_j, then we replace these q_i by the respective r_j.
2. If some of the q_i don't appear among the r_j, then we insert q_i^0 factors into the prime power factorization of b.
3. If some of the r_j don't appear among the q_i, then we insert r_j^0 factors into the prime power factorization of a.

For example, if $R = \mathbb{Z}$ and $a = 12$ and $b = 45$, and if we start with the prime power factorizations $a \sim 2^2 \cdot (-3)^1$ and $b \sim 3^2 \cdot 5^1$, then Step 1 transforms the prime power factorization of a into $a \sim 2^2 \cdot 3^1$ (since the -3 is replaced by the 3 from the prime power factorization of b); Step 2 then inserts a 2^0 factor into the prime power factorization of b (so it becomes $b \sim 2^0 \cdot 3^2 \cdot 5^1$); Step 3 then inserts a 5^0 factor into the prime power factorization of a (so it becomes $a \sim 2^2 \cdot 3^1 \cdot 5^0$). The resulting factorizations are $a \sim 2^2 \cdot 3^1 \cdot 5^0$ and $b \sim 2^0 \cdot 3^2 \cdot 5^1$, just as promised by Proposition 2.15.8. □

2.15.3. Gcds and lcms in a UFD

Proposition 2.15.9. Let R be a UFD. Let $a, b \in R$ be nonzero. Let $(p_1, p_2, \ldots, p_n)$, $(e_1, e_2, \ldots, e_n)$ and $(f_1, f_2, \ldots, f_n)$ be as in Proposition 2.15.8. Then:

(a) The element

$$p_1^{\min\{e_1, f_1\}} p_2^{\min\{e_2, f_2\}} \cdots p_n^{\min\{e_n, f_n\}}$$

is a gcd of a and b.

(b) The element

$$p_1^{\max\{e_1,f_1\}} p_2^{\max\{e_2,f_2\}} \cdots p_n^{\max\{e_n,f_n\}}$$

is an lcm of a and b.

Proof. This is done just as it is commonly done for integers in elementary number theory. The details are LTTR. (See, e.g., [Friedm19, proof of Proposition 1.11] for some details on the proof of part **(a)**; the proof of part **(b)** is similar.) □

Corollary 2.15.10. Any two elements in a UFD have a gcd and an lcm.

Proof. Let a and b be two elements of a UFD R. We must show that a and b have a gcd and an lcm.

If $b = 0$, then this is easy (just show that a is a gcd of a and 0, and that 0 is an lcm of a and 0). Thus, we WLOG assume that $b \neq 0$. For a similar reason, we WLOG assume that $a \neq 0$. Hence, Proposition 2.15.8 shows that there exists a list $(p_1, p_2, \ldots, p_n)$ of **mutually non-associate** irreducible elements $p_1, p_2, \ldots, p_n \in R$ as well as two lists $(e_1, e_2, \ldots, e_n)$ and $(f_1, f_2, \ldots, f_n)$ of **nonnegative** integers such that

$$a \sim p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \qquad \text{and} \qquad b \sim p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}.$$

Thus, Proposition 2.15.9 shows that a and b have a gcd and a lcm. □

2.15.4. Any PID is a UFD

Finally, as promised, let us state the following theorem, which provides us many UFDs to apply the above results to:

Theorem 2.15.11. Any PID is a UFD.

I won't prove Theorem 2.15.11 here; a proof can be found in [DumFoo04, §8.3, Theorem 14] or in [Mileti20, Corollary 12.2.13] or in [Swanso17, Theorem 36.3]. The proof of the existence of an irreducible factorization is rather philosophical and non-constructive; it yields no algorithm for actually finding such a factorization. (And indeed, there are UFDs in which finding such a factorization is algorithmically impossible.)[90] The proof of the uniqueness of an irreducible factorization is an analogue of the proof you know from elementary number theory (since we know that irreducible elements are prime).

[90] However, in many specific PIDs, there are easy (although slow) algorithms for finding irreducible factorizations. For instance, for $\mathbb{Z}[i]$, Exercise 2.16.4 asks you to find such an algorithm.

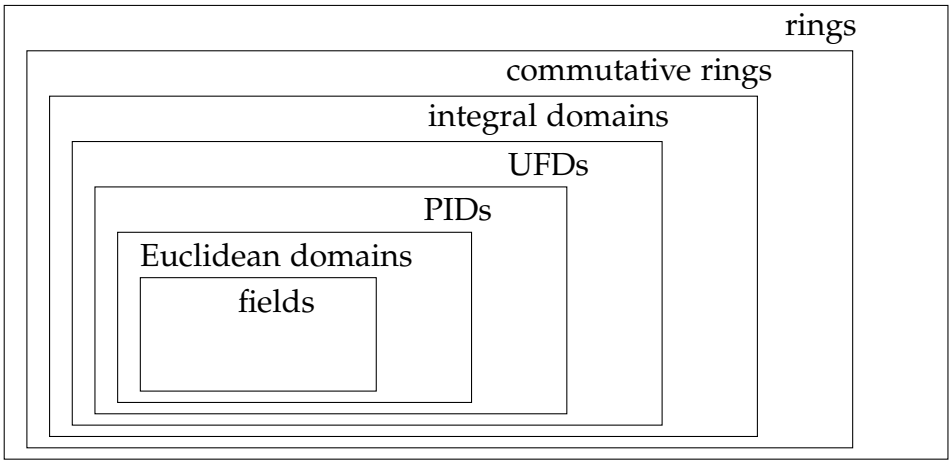
2.15.5. A synopsis

The following corollary combines several results we have seen above in a convenient hierarchy:

Corollary 2.15.12. We have

$$\{\text{fields}\} \subseteq \{\text{Euclidean domains}\} \subseteq \{\text{PIDs}\} \subseteq \{\text{UFDs}\}$$
$$\subseteq \{\text{integral domains}\} \subseteq \{\text{commutative rings}\} \subseteq \{\text{rings}\}.$$

Let us illustrate this hierarchy in a symbolic picture:



All the "$\subseteq$" signs in Corollary 2.15.12 are strict inclusions; let us briefly recall some examples showing this:

- The rings $\mathbb{Z}$ and $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\sqrt{-2}\right]$ and $\mathbb{Z}\left[\sqrt{2}\right]$ and the polynomial ring $\mathbb{Q}[x]$ are Euclidean domains, but not fields.
- The ring $\mathbb{Z}[\alpha]$ for $\alpha = \dfrac{1+\sqrt{-19}}{2}$ is a PID, but not a Euclidean domain.
- The polynomial rings $\mathbb{Q}[x,y]$ and $\mathbb{Z}[x]$ are UFDs, but not PIDs.
- The rings $\mathbb{Z}[2i]$ and $\mathbb{Z}\left[\sqrt{-3}\right]$ are integral domains, but not UFDs.
- The ring $\mathbb{Z}/6 \cong \mathbb{Z}/2 \times \mathbb{Z}/3$ is a commutative ring, but not an integral domain.
- The matrix ring $\mathbb{Q}^{2\times 2}$ and the ring of quaternions $\mathbb{H}$ are not commutative.

2.16. Application: Fermat's $p = x^2 + y^2$ theorem ([DumFoo04, §8.3])

2.16.1. Fermat's two-squares theorem

As an application of some of the above, we will show a result of Fermat:[91]

Theorem 2.16.1 (Fermat's two-squares theorem)**.** Let p be a prime number such that $p \equiv 1 \bmod 4$. Then, p can be written as a sum of two perfect squares.

For example,

$$5 = 1^2 + 2^2;$$
$$13 = 2^2 + 3^2;$$
$$17 = 1^2 + 4^2;$$
$$29 = 2^2 + 5^2.$$

(Note that the prime 2 can also be written as a sum of two perfect squares: $2 = 1^2 + 1^2$. But this would distract us from our proof.)

I will prove Theorem 2.16.1 using rings (specifically, using the ring $\mathbb{Z}/p$ of residue classes and the ring $\mathbb{Z}[i]$ of Gaussian integers). Some of the steps will be left as exercises.

First, we shall show a general curious fact about primes, known as **Wilson's theorem**:

Theorem 2.16.2 (Wilson's theorem)**.** Let p be a prime. Then, $(p-1)! \equiv -1 \bmod p$.

For example, for $p = 5$, this is saying that $4! \equiv -1 \bmod 5$. And indeed, $4! = 24 \equiv -1 \bmod 5$.

Proof of Theorem 2.16.2. We must show that $(p-1)! \equiv -1 \bmod p$. Equivalently, we must show that

$$\overline{(p-1)!} = \overline{-1} \text{ in } \mathbb{Z}/p. \tag{38}$$

However, $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$, so that

$$\overline{(p-1)!} = 1 \cdot 2 \cdot \cdots \cdot (p-1) = \overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1}. \tag{39}$$

Recall that every ring R has a group of units, which is denoted by $R^\times$. (See Theorem 2.5.3 for details.)

[91] The word "prime number" is understood as in classical number theory – i.e., a positive integer $p > 1$ whose only positive divisors are 1 and p. In particular, negative numbers are not allowed as prime numbers, even though they are prime elements of $\mathbb{Z}$.

But $\mathbb{Z}/p$ is a field (as we know, since p is prime) with p elements $\overline{0}, \overline{1}, \ldots, \overline{p-1}$. Its nonzero elements $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ are thus its units. In other words, its group of units $(\mathbb{Z}/p)^\times$ is precisely the set $\left\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\right\}$ (and all the $p-1$ elements $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ are distinct). Hence,

$$\prod_{a \in (\mathbb{Z}/p)^\times} a = \overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1}. \tag{40}$$

Recall that $(\mathbb{Z}/p)^\times$ is a group. In particular, any unit has an inverse, which is again a unit. The units $\overline{1}$ and $\overline{-1}$ are their own inverses (since $\overline{1} \cdot \overline{1} = \overline{1 \cdot 1} = \overline{1}$ and $\overline{-1} \cdot \overline{-1} = \overline{(-1) \cdot (-1)} = \overline{1}$), and they are the only units that are their own inverses (this is Exercise 2.5.1). The inverse of the inverse of a unit a is a. Hence, in the product $\prod_{a \in (\mathbb{Z}/p)^\times} a$, we can pair up each factor other than $\overline{1}$ and $\overline{-1}$ with its inverse:

$$\begin{aligned}\prod_{a \in (\mathbb{Z}/p)^\times} a &= \underbrace{\left(a_1 \cdot a_1^{-1}\right)}_{=\overline{1}} \cdot \underbrace{\left(a_2 \cdot a_2^{-1}\right)}_{=\overline{1}} \cdot \cdots \cdot \underbrace{\left(a_k \cdot a_k^{-1}\right)}_{=\overline{1}} \cdot \overline{1} \cdot \overline{-1} \\ &= \overline{1} \cdot \overline{1} \cdot \cdots \cdot \overline{1} \cdot \overline{1} \cdot \overline{-1} = \overline{-1}.\end{aligned} \tag{41}$$

Now, (39) becomes

$$\begin{aligned}\overline{(p-1)!} &= \overline{1} \cdot \overline{2} \cdot \cdots \cdot \overline{p-1} = \prod_{a \in (\mathbb{Z}/p)^\times} a \qquad \text{(by (40))} \\ &= \overline{-1} \qquad \text{(by (41))}.\end{aligned}$$

This proves (38) and thus Theorem 2.16.2.

(Caveat: The above was a little bit wrong for $p = 2$; in that case, the factors $\overline{1}$ and $\overline{-1}$ are actually one and the same factor. But our proof can easily be adapted to the above.) □

Corollary 2.16.3. Let p be an odd prime (i.e., a prime distinct from 2). Let $u = \dfrac{p-1}{2} \in \mathbb{N}$. Then, $u!^2 \equiv -(-1)^u \bmod p$.

Proof. This is [21w, homework set #2, Exercise 5 **(b)**]. Here is a sketch of the proof: From $u = \dfrac{p-1}{2}$, we obtain $2u = p-1$ and thus $2u+1 = p$. Also, $p-1 = 2u$ (since $2u = p-1$) and thus

$$\begin{aligned}(p-1)! = (2u)! &= \underbrace{1 \cdot 2 \cdot \cdots \cdot u}_{=u!} \cdot (u+1) \cdot (u+2) \cdot \cdots \cdot (2u) \\ &= u! \cdot ((u+1) \cdot (u+2) \cdot \cdots \cdot (2u)).\end{aligned}$$

In view of

$$(u+1)\cdot(u+2)\cdot\cdots\cdot(2u) = \prod_{k=u+1}^{2u} k = \prod_{j=1}^{u} \underbrace{(2u+1-j)}_{\substack{\equiv -j \bmod p \\ \text{(since } (2u+1-j)-(-j)=2u+1=p \\ \text{is divisible by } p\text{)}}}$$

$$\left(\begin{array}{c}\text{here, we have substituted } 2u+1-j \\ \text{for } k \text{ in the product}\end{array}\right)$$

$$\equiv \prod_{j=1}^{u} (-j) = (-1)^u \underbrace{\prod_{j=1}^{u} j}_{=u!} = (-1)^u\, u! \bmod p,$$

this becomes

$$(p-1)! = u! \cdot \underbrace{((u+1)\cdot(u+2)\cdot\cdots\cdot(2u))}_{\equiv (-1)^u u! \bmod p}$$

$$\equiv u! \cdot (-1)^u\, u! \equiv (-1)^u \cdot u!^2 \bmod p.$$

Hence,

$$(-1)^u \cdot u!^2 \equiv (p-1)! \equiv -1 \bmod p \qquad \text{(by Theorem 2.16.2)}.$$

Multiplying both sides of this congruence by $(-1)^u$, we obtain $u!^2 \equiv -(-1)^u \bmod p$. This proves Corollary 2.16.3. □

Corollary 2.16.4. Let p be a prime such that $p \equiv 1 \bmod 4$. Let $u = \dfrac{p-1}{2} \in \mathbb{N}$. Then, $u!^2 \equiv -1 \bmod p$.

Proof. From $p \equiv 1 \bmod 4$, we obtain $4 \mid p-1$, so that $2 \mid \dfrac{p-1}{2} = u$. Thus, u is even, so that $(-1)^u = 1$.

The prime p is odd (since $p \equiv 1 \bmod 4$). Hence, Corollary 2.16.3 yields $u!^2 \equiv -\underbrace{(-1)^u}_{=1} = -1 \bmod p$. This proves Corollary 2.16.4. □

Now, recall the ring $\mathbb{Z}[i]$ of Gaussian integers. Let $N : \mathbb{Z}[i] \to \mathbb{N}$ be the map that sends each Gaussian integer $a+bi$ (with $a, b \in \mathbb{Z}$) to $a^2+b^2 \in \mathbb{N}$. It is straightforward to see:

Proposition 2.16.5. We have $N(\alpha\beta) = N(\alpha)\, N(\beta)$ for any $\alpha, \beta \in \mathbb{Z}[i]$.

Proof. One way to prove this is by first showing that $N(\gamma) = \gamma\overline{\gamma}$ for each $\gamma \in \mathbb{Z}[i]$ (where $\overline{\gamma}$ denotes the complex conjugate of γ). Another is by direct

computation: Writing α and β as $\alpha = a + bi$ and $\beta = c + di$, we have $\alpha\beta = (a + bi)(c + di) = (ac - bd) + (ad + bc)\, i$ and therefore

$$\begin{aligned} N(\alpha\beta) &= N\left((ac - bd) + (ad + bc)\, i\right) = (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 = \underbrace{\left(a^2 + b^2\right)}_{=N(\alpha)} \underbrace{\left(c^2 + d^2\right)}_{=N(\beta)} = N(\alpha)\, N(\beta). \end{aligned}$$

□

Corollary 2.16.6. If z and w are two Gaussian integers satisfying $z \mid w$ in $\mathbb{Z}[i]$, then $N(z) \mid N(w)$ in $\mathbb{Z}$.

Proof. Exercise (specifically, [21w, homework set #2, Exercise 6 **(a)**]). □

Using this fact, we can characterize the units of $\mathbb{Z}[i]$:

Corollary 2.16.7. Let $\alpha \in \mathbb{Z}[i]$. Then, we have the following equivalence:

$$(\alpha \text{ is a unit of } \mathbb{Z}[i]) \iff (N(\alpha) = 1) \iff (\alpha \in \{1, i, -1, -i\}).$$

Proof. Exercise (specifically, [21w, homework set #2, Exercise 6 **(d)**]). □

The next lemma is also easy to see:

Lemma 2.16.8. Let α and β be Gaussian integers such that $\alpha \neq 0$. Then, $\alpha \mid \beta$ holds in $\mathbb{Z}[i]$ if and only if $\dfrac{\beta}{\alpha}$ is a Gaussian integer.

Proof. This is proved just as the analogous statement for integers is proved. □

Now we can prove Theorem 2.16.1:

Proof of Theorem 2.16.1. Let $u = \dfrac{p-1}{2}$. Then, $u \in \mathbb{N}$ (actually, $p \equiv 1 \bmod 4$ implies that u is even). Corollary 2.16.4 shows that $u!^2 \equiv -1 \bmod p$. That is,

$$p \mid u!^2 - \underbrace{(-1)}_{=i^2} = u!^2 - i^2 = (u! - i)(u! + i).$$

This is a divisibility in $\mathbb{Z}$, thus also in $\mathbb{Z}[i]$.

The number p is a prime number, and thus prime in $\mathbb{Z}$; but this does **not** mean that it is prime in $\mathbb{Z}[i]$. And in fact, we claim that it isn't. Indeed, if p

was prime in $\mathbb{Z}[i]$, then the divisibility $p \mid (u!-i)(u!+i)$ would entail that $p \mid u!-i$ or $p \mid u!+i$; however, neither $p \mid u!-i$ nor $p \mid u!+i$ is true[92].

Thus, we know that p is not prime in $\mathbb{Z}[i]$. But $\mathbb{Z}[i]$ is a Euclidean domain (as we proved in Subsection 2.13.2), and thus a PID (since Proposition 2.14.2 says that any Euclidean domain is a PID). Hence, every irreducible element of $\mathbb{Z}[i]$ is a prime element of $\mathbb{Z}[i]$ (by Proposition 2.15.4). Thus, p cannot be irreducible in $\mathbb{Z}[i]$ (since p is not prime in $\mathbb{Z}[i]$).

However, p is nonzero and not a unit of $\mathbb{Z}[i]$ (since $\dfrac{1}{p}$ is not a Gaussian integer). Therefore, since p is not irreducible, there exist two elements $\alpha, \beta \in \mathbb{Z}[i]$ that satisfy $\alpha\beta = p$ but are not units (by the definition of "irreducible"). Consider these α and β.

From $\alpha\beta = p$, we obtain $N(\alpha\beta) = N(p) = N(p+0i) = p^2+0^2 = p^2$. Thus, $p^2 = N(\alpha\beta) = N(\alpha)\,N(\beta)$ (by Proposition 2.16.5). However, $N(\alpha)$ and $N(\beta)$ are nonnegative integers (since N is a map $\mathbb{Z}[i] \to \mathbb{N}$). Since p is prime, the only ways to write p^2 as a product of two nonnegative integers are $p^2 = 1 \cdot p^2$ and $p^2 = p^2 \cdot 1$ and $p^2 = p \cdot p$ (by the classical prime factorization theorem from number theory). Hence, the equality $p^2 = N(\alpha)\,N(\beta)$ (with $N(\alpha)$ and $N(\beta)$ being nonnegative integers) entails that we must be in one of the following two cases:

Case 1: One of the two numbers $N(\alpha)$ and $N(\beta)$ is 1, and the other is p^2.

Case 2: Both numbers $N(\alpha)$ and $N(\beta)$ are p.

Let us consider Case 1. In this case, one of the two numbers $N(\alpha)$ and $N(\beta)$ is 1. We WLOG assume that $N(\alpha) = 1$ and $N(\beta) = p^2$ (since the other possibility can be transformed into this one by swapping α with β). Now, recall that $N(\alpha) = 1$ is equivalent to α being a unit (because of Corollary 2.16.7). However, α is not a unit. This is a contradiction. Hence, Case 1 is impossible.

Thus, we must be in Case 2. In other words, $N(\alpha) = p$ and $N(\beta) = p$.

Now, α is a Gaussian integer, so we can write it as $\alpha = x+yi$ for some $x, y \in \mathbb{Z}$. Therefore, using these x, y, we have $N(\alpha) = x^2+y^2$. Hence, $x^2+y^2 = N(\alpha) = p$. Thus, p is a sum of two perfect squares; Theorem 2.16.1 is proven. □

We note that Theorem 2.16.1 has a converse as well (which, however, is rather easy):

Exercise 2.16.1. Let p be a prime. Prove that p can be written as a sum of two perfect squares if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

[92] This is easiest to see using Lemma 2.16.8: Indeed, if we had $p \mid u!-i$, then Lemma 2.16.8 would entail that $\dfrac{u!-i}{p}$ is a Gaussian integer; however, $\dfrac{u!-i}{p} = \dfrac{u!}{p} + \dfrac{-1}{p}i$ is not a Gaussian integer (since its imaginary part $\dfrac{-1}{p}$ is not an integer). Thus, we don't have $p \mid u!-i$. For a similar reason, we don't have $p \mid u!+i$.

2.16.2. Non-primes and numbers of representations

Theorem 2.16.1 is the beginning of a long sequence of more and more complex results, whose discovery and proof spanned several centuries. First of all, one can ask which integers (rather than which primes) can be written as sums of two perfect squares. The answer is not too hard at this point:

Theorem 2.16.9. Let n be a positive integer with prime factorization $n = 2^a p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes larger than 2, and where $a, b_1, b_2, \ldots, b_k$ are nonnegative integers. (In particular, if n is odd, then $a = 0$.)

Then:

(a) The number n can be written as a sum of two perfect squares if and only if the following condition holds: For each $i \in \{1, 2, \ldots, k\}$ satisfying $p_i \equiv 3 \bmod 4$, the exponent b_i is even.

(b) If this condition holds, then the number of ways to write n as a sum of two perfect squares (to be more precise: the number of pairs $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ satisfying $n = x^2 + y^2$) is $4 \cdot \prod_{\substack{i \in \{1,2,\ldots,k\}; \\ p_i \equiv 1 \bmod 4}} (b_i + 1)$.

For a proof of this theorem, see [Grinbe19, Theorem 4.2.62] or [DumFoo04, §8.1, Corollary 19]. (The proof again uses Gaussian integers in a rather neat way.)

Exercise 2.16.2. Prove the "if" part of Theorem 2.16.9 **(a)**. (Keep in mind that 0 counts as a perfect square.)

More about decompositions of integers into sums of perfect squares can be found

- in [DumFoo04, §8.3];
- in Keith Conrad's `https://kconrad.math.uconn.edu/math5230f12/handouts/Zinotes.pdf` ;
- in [Grinbe19, §4.2].

2.16.3. Other forms $x^2 + ny^2$

Instead of writing integers n in the form $n = x^2 + y^2$, we can try to write them in the form $x^2 + 2y^2$ or $x^2 + 3y^2$ or $x^2 + 4y^2$ or $x^2 + 5y^2$ or $x^2 + xy + y^2$ or $\left|x^2 - 2y^2\right|$ or many other such forms. Each time, we can ask when this is possible, and how many ways there are. These questions vary widely in difficulty,

and even their most basic variants (which prime numbers can be written in a given form?) can be extremely hard. After having answered the x^2+y^2 question for primes, the x^2+4y^2 question becomes quite easy (see Exercise 2.16.3 below), but the x^2+2y^2 question will have to wait until a later chapter (see Exercise 5.8.6 below). A whole book [Cox22] has been written entirely about the question of writing prime(!) numbers in the form x^2+ny^2 for positive integers n; just answering these questions for different n requires rather advanced mathematics. Here is a summary of answers for certain values of n (see [Cox22] for proofs of these and many more results):

Theorem 2.16.10. Let p be a prime number.

(a) We can write p in the form $p = x^2+y^2$ with $x, y \in \mathbb{Z}$ if and only if $p = 2$ or $p \equiv 1 \bmod 4$.

(b) We can write p in the form $p = x^2+2y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 3 \bmod 8$. (The notation "$p \equiv 1, 3 \bmod 8$" is shorthand for "p is congruent to 1 or to 3 modulo 8". Similar shorthands will be used in the following parts.)

(c) We can write p in the form $p = x^2+3y^2$ with $x, y \in \mathbb{Z}$ if and only if $p = 3$ or $p \equiv 1 \bmod 3$.

(d) We can write p in the form $p = x^2+4y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \bmod 4$.

(e) We can write p in the form $p = x^2+5y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 9 \bmod 20$.

(f) We can write p in the form $p = x^2+6y^2$ with $x, y \in \mathbb{Z}$ if and only if $p \equiv 1, 7 \bmod 24$.

(g) We can write p in the form $p = x^2+14y^2$ with $x, y \in \mathbb{Z}$ if and only if we have $p \equiv 1, 9, 15, 23, 25, 39 \bmod 56$ and there exists some integer z satisfying $\left(z^2+1\right)^2 \equiv 8 \bmod p$.

(h) We can write p in the form $p = x^2+27y^2$ with $x, y \in \mathbb{Z}$ if and only if we have $p \equiv 1 \bmod 3$ and there exists some integer z satisfying $z^3 \equiv 2 \bmod p$.

Part **(a)** of Theorem 2.16.10 follows from Theorem 2.16.1 and Exercise 2.16.1. As we said, parts **(b)** and **(d)** follow easily from Exercise 5.8.6 and Exercise 2.16.3. Part **(c)** is similar, but the proof is trickier since $\mathbb{Z}\left[\sqrt{-3}\right]$ is not a PID (or even a UFD); nevertheless, fairly elementary proofs exist, and one such

proof is outlined in Exercise 5.8.7[93]. Part **(e)** is proved using genus theory of quadratic forms in [Cox22, (2.22)], and using elementary techniques (quadratic reciprocity) in [Zhang07]. Part **(f)** requires class field theory ([Cox22, Theorem 5.33]). Parts **(g)** and **(h)** can be proved using elliptic functions from complex analysis ([Cox22, Chapters 2 and 3]). Note the additional "there exists some integer z" conditions in parts **(g)** and **(h)**; such conditions can be avoided for $x^2 + ny^2$ when n is small, but eventually become necessary. See `https://mathoverflow.net/questions/79342/` for more about the need for such conditions, and see [Cox22, Chapters 2 and 3] for their exact nature.

We can also ask about sums of more than two squares. Lagrange proved that every nonnegative integer can be written as a sum of **four** squares (that is, each $n \in \mathbb{N}$ can be written as $n = x^2 + y^2 + z^2 + w^2$ for some $x, y, z, w \in \mathbb{Z}$). These days, one of the shortest proofs of this fact uses the so-called *Hurwitz quaternions* – a quaternion analogue of Gaussian integers. See `https://en.wikipedia.org/wiki/Lagrange's_four-square_theorem` or [Haensc16] or [Schwar14] for the proof.

2.16.4. Coda

Exercise 2.16.3. Let p be a prime. Prove that p can be written in the form $p = x^2 + 4y^2$ for some $x, y \in \mathbb{Z}$ if and only if $p \equiv 1 \bmod 4$.

Exercise 2.16.4.

(a) Let $z = a + bi \in \mathbb{Z}[i]$ with $a, b \in \mathbb{Z}$. Assume that $z \neq 0$. Let $n = \lfloor |z| \rfloor = \left\lfloor \sqrt{a^2 + b^2} \right\rfloor$. Prove that every divisor of z in $\mathbb{Z}[i]$ has the form $c + di$ with $c, d \in \{-n, -n+1, \ldots, n\}$.

(b) Without recourse to the general theory of PIDs and UFDs, prove that every nonzero element of $\mathbb{Z}[i]$ has an irreducible factorization.

Exercise 2.16.5. Let R be the ring $\mathbb{Z}[i]$ of Gaussian integers. Let S be the ring

$$\begin{aligned}\mathbb{Z}[2i] &= \{a + b \cdot 2i \mid a, b \in \mathbb{Z}\} \\ &= \{\text{Gaussian integers with an even imaginary part}\}.\end{aligned}$$

This ring S is a subring of R.

Define two elements $x, y \in S$ by $x = 2 + 2i$ and $y = 2 - 2i$.

(a) Find the units of S.

(b) Prove that we have $x \sim y$ in R, but we don't have $x \sim y$ in S.

(c) Prove that the ideal $xS + yS$ of S is not principal.

[93] See, e.g., `https://math.stackexchange.com/a/76917/` for another proof.

(d) Conclude that S is not a PID.

(e) Show that S is not a UFD either.

[**Hint:** It may be helpful to write i' for $2i$ in order to avoid confusing i for an element of S.

For part **(c)**, argue that if $xS + yS$ was zS for some $z \in S$, then $xR + yR$ would be zR as well (why?), but this would force z to be associate to x and y in R (why?), and this would leave only four possibilities for z (why?).

For part **(e)**, ponder the equality $xy = 2 \cdot 2 \cdot 2$. Note that any divisor of an element $s \in S$ is also a divisor of the same element s in $R = \mathbb{Z}[i]$ (but not always the other way round).]

Exercise 2.16.6. Consider the ring

$$\mathbb{Z}\left[\sqrt{-3}\right] = \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\right\}.$$

This ring is a subring of $\mathbb{C}$, and thus is an integral domain.

Let $u = 2 \in \mathbb{Z}\left[\sqrt{-3}\right]$ and $v = 1 + \sqrt{-3} \in \mathbb{Z}\left[\sqrt{-3}\right]$. Further let $a = 2u = 4$ and $b = 2v$.

(a) Prove that both u and v are common divisors of a and b in $\mathbb{Z}\left[\sqrt{-3}\right]$.

(b) Prove that the only divisors of 4 in $\mathbb{Z}\left[\sqrt{-3}\right]$ are ± 1, ± 2, ± 4, $\pm\left(1 + \sqrt{-3}\right)$, and $\pm\left(1 - \sqrt{-3}\right)$.

(c) Prove that a and b have no gcd in $\mathbb{Z}\left[\sqrt{-3}\right]$.

[**Remark:** This shows that $\mathbb{Z}\left[\sqrt{-3}\right]$ is not a UFD, thus not a PID and not Euclidean.]

Exercise 2.16.7.

(a) Prove that there are no ring morphisms from $\mathbb{Z}[i]$ to $\mathbb{Z}$.

Now, let p be a prime number. Prove the following:

(b) There are no ring morphisms from $\mathbb{Z}[i]$ to $\mathbb{Z}/p$ if $p \equiv 3 \bmod 4$.

(c) There are exactly two ring morphisms from $\mathbb{Z}[i]$ to $\mathbb{Z}/p$ if $p \equiv 1 \bmod 4$.

(d) There is a unique ring morphism from $\mathbb{Z}[i]$ to $\mathbb{Z}/p$ if $p = 2$.

More generally, prove the following:

(e) If R is any ring, then the number of ring morphisms from $\mathbb{Z}[i]$ to R is the number of all elements $r \in R$ satisfying $r^2 = -1$.

[**Hint:** If f is a ring morphism from $\mathbb{Z}[i]$ to R, then what equation must $f(i)$ satisfy?]

2.17. More about ideals and quotient rings

For the sake of completeness, let me mention three more general properties of quotient rings, known respectively as the **second**, **third** and **fourth isomorphism theorems for rings**. The second and third isomorphism theorems claim isomorphisms between quotient rings; the fourth relates the ideals of a quotient ring to some ideals of the original ring. We shall not use these theorems, but they are not hard to prove and are part of an algebraist's culture.

2.17.1. The second isomorphism theorem for rings

The **second isomorphism theorem for rings** is all about the interaction between an ideal and a subring:

Theorem 2.17.1 (Second isomorphism theorem for rings)**.** Let R be a ring. Let S be a subring of R. Let I be an ideal of R. Define $S+I$ to be the subset $\{s+i \mid s \in S \text{ and } i \in I\}$ of R. Then:

(a) This subset $S+I$ is a subring of R.

(b) The set I is an ideal of the ring $S+I$.

(c) The set $S \cap I$ is an ideal of the ring S.

(d) We have $(S+I)/I \cong S/(S \cap I)$ (as rings). More concretely, there is a ring isomorphism $S/(S \cap I) \to (S+I)/I$ that sends each residue class $\overline{s} = s + (S \cap I)$ to $\overline{s} = s + I$.

Proof. See [21w, homework set #2, Exercise 9]. □

Example 2.17.2. For an example, we

- let R be the polynomial ring $\mathbb{Q}[x]$ of all univariate polynomials with rational coefficients;
- let $I = \left\{a_2x^2 + a_3x^3 + \cdots + a_nx^n \mid n \geq 0 \text{ and } a_i \in \mathbb{Q}\right\}$ be the ideal consisting of all polynomials divisible by x^2 (that is, all polynomials whose x^0-coefficient and x^1-coefficient are 0);
- let S be the subring $\mathbb{Q}$ of R (which consists of all constant polynomials).

Then, $S+I = \left\{a_0 + a_2x^2 + a_3x^3 + \cdots + a_nx^n \mid n \geq 0 \text{ and } a_i \in \mathbb{Q}\right\}$ is the set of all polynomials whose x^1-coefficient is 0. This is indeed a subring of R, as we have seen in Subsection 2.15.1 (where we have used this subring to find an irreducible element that is not prime).

Other interesting examples of $S+I$ can be obtained using upper-triangular matrix rings such as $\mathbb{Q}^{3\leq 3}$.

2.17.2. The third isomorphism theorem for rings

You might have noticed that the quotient rings R/I of a given ring R stand in an "antithetical" relationship to the ideals I that produce them: The larger the ideal I, the smaller the quotient ring R/I. (In particular, the largest ideal of R is R itself, and the corresponding quotient ring R/R is trivial, which is as small as a ring can get.)

Can we make this relationship precise? To some extent, we can. Namely, when two ideals I and J of a ring R satisfy $I \subseteq J$, the corresponding quotient rings R/I and R/J are related as well, and specifically, R/J is isomorphic to a quotient ring of R/I. In other words, the quotient R/J by the "large" ideal J can be obtained by first quotienting out a "smaller" ideal I and then "quotienting further". The **third isomorphism theorem for rings** states this relationship in a more concrete way:

Theorem 2.17.3 (Third isomorphism theorem for rings)**.** Let R be a ring. Let I and J be two ideals of R such that $I \subseteq J$. Let J/I denote the set of all cosets $j + I \in R/I$ where $j \in J$. Then:

(a) This set J/I is an ideal of R/I.

(b) We have $(R/I)\,/\,(J/I) \cong R/J$ (as rings). More concretely, there is a ring isomorphism $R/J \to (R/I)\,/\,(J/I)$ that sends each residue class $\overline{r} = r + J$ to $\overline{r+I} = (r+I) + (J/I)$.

Proof. See [21w, homework set #2, Exercise 8]. □

Example 2.17.4. For an example, take $R = \mathbb{Z}$ and $I = 6\mathbb{Z}$ and $J = 2\mathbb{Z}$. In this case, J/I consists of the "even" residue classes $\overline{0}, \overline{2}, \overline{4}$ in $R/I = \mathbb{Z}/6$. Theorem 2.17.3 **(b)** says that if we "quotient them out" of $\mathbb{Z}/6$, then we are left with (an isomorphic copy of) $R/J = \mathbb{Z}/2$.

2.17.3. The inverse image of an ideal

The following easy fact gives yet another way to construct ideals of rings:

Proposition 2.17.5. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Let K be an ideal of S.

Then,

$$f^{-1}(K) := \{r \in R \mid f(r) \in K\}$$

is an ideal of R that satisfies $\operatorname{Ker} f \subseteq f^{-1}(K)$.

Exercise 2.17.1. Prove Proposition 2.17.5.

Here is an example:

- Let S be the ring $\mathbb{Z}$. Let R be the ring $\mathbb{Z}^{2\leq 2}$ of all upper-triangular 2×2-matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with integer entries $a, b, d \in \mathbb{Z}$. Let $f : R \to S$ be the map that sends each such matrix $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ to its entry d. It is easy to see that this map f is a ring morphism. Let K be the ideal of S consisting of all even integers (that is, $K = 2\mathbb{Z}$). Thus, $f^{-1}(K)$ (as defined in Proposition 2.17.5) is the set of all upper-triangular 2×2-matrices $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ with integer entries $a, b, d \in \mathbb{Z}$ such that d is even. Proposition 2.17.5 shows that this set $f^{-1}(K)$ is an ideal of R (which the reader can easily check).

2.17.4. The fourth isomorphism theorem for rings

What is the relation between the ideals of a quotient ring R/I and the ideals of the original ring R ? More generally, what is the relation between the ideals of two rings S and R when there is a surjective ring morphism $f : R \to S$? (This is "more general" since there is always a surjective morphism $\pi : R \to R/I$ from a ring R to a quotient ring R/I.) The **fourth isomorphism theorem for rings** answers this question:

Theorem 2.17.6 (Fourth isomorphism theorem for rings)**.** Let R and S be two rings. Let $f : R \to S$ be a **surjective** ring morphism. Then:

(a) If J is an ideal of R, then $f(J) := \{f(j) \mid j \in J\}$ is an ideal of S.

(b) The maps

$$\{\text{ideals } J \text{ of } R \text{ satisfying } \operatorname{Ker} f \subseteq J\} \to \{\text{ideals of } S\}, \quad J \mapsto f(J)$$

and

$$\{\text{ideals of } S\} \to \{\text{ideals } J \text{ of } R \text{ satisfying } \operatorname{Ker} f \subseteq J\}, \quad K \mapsto f^{-1}(K)$$

(where $f^{-1}(K)$ is defined as in Proposition 2.17.5) are mutually inverse.

Exercise 2.17.2. Prove Theorem 2.17.6.

We note that Theorem 2.17.6 **(a)** becomes false if we drop the "f is surjective" assumption.

2.17.5. Prime and maximal ideals

The following definition is rather important for the deeper study of ideals in commutative rings (and, by extension, for algebraic geometry). We will only touch on it briefly in this little subsection.

Definition 2.17.7. Let R be a commutative ring. Let I be an ideal of R.

(a) The ideal I is said to be **proper** if it is a proper subset of R (that is, $I \neq R$).

(b) The ideal I is said to be **prime** if it is proper and has the following property: If $a, b \in R$ satisfy $ab \in I$, then $a \in I$ or $b \in I$.

(c) The ideal I is said to be **maximal** if it is proper and the only ideals J of R satisfying $I \subseteq J \subseteq R$ are I and R.

We note that a principal ideal aR of a commutative ring R (with $a \in R$ nonzero) is prime if and only if a is a prime element of R. Thus, the notion of prime ideals generalizes the notion of prime elements (and, ultimately, that of prime numbers).

Exercise 2.17.3. Let R be a commutative ring. Let I be an ideal of R. Prove the following:

(a) The ideal I is prime if and only if the quotient ring R/I is an integral domain.

(b) The ideal I is maximal if and only if the quotient ring R/I is a field.

(c) Any maximal ideal I of R is prime.

[**Hint:** Theorem 2.17.6 and Exercise 2.8.1 are helpful for part **(b)**.]

3. Modules ([DumFoo04, Chapter 10])

We now move on from studying rings themselves to studying **modules** over rings. In many ways, modules are even more important than rings, as their definition offers more freedom (and this freedom is widely used throughout mathematics). Some would argue that the notion of a ring is merely an ancillary character to that of a module.

3.1. Definition and examples ([DumFoo04, §10.1])

Before we define modules rigorously, let me give a rough idea of what they stand for.

We can think of a ring is a system of "number-like objects" that can be "added" (with one another) and "multiplied" (with one another).[94]

In contrast, a **module** (over a given ring R) can be thought of a system of "vector-like objects" that can be "added" (with one another) and "scaled" (by elements of R). In particular, if R is a field, then the modules over R are just the vector spaces over R (as defined in any textbook on abstract linear algebra).

To turn this into a proper definition of a module, we just need to decide what properties of "adding" and "scaling" we want to require as axioms.

3.1.1. Definition of modules

For every ring R, there are two notions of an "R-module": the "left R-modules" and the "right R-modules". Let us first define the left ones:

Definition 3.1.1. Let R be a ring. A **left R-module** (or a **left module over** R) means a set M equipped with

- a binary operation $+$ (that is, a map from $M \times M$ to M) that is called **addition**;
- an element $0_M \in M$ that is called the **zero element** or the **zero vector** or just the **zero**, and is just denoted by 0 when there is no ambiguity;
- a map from $R \times M$ to M that is called the **action of R on M**, and is written as multiplication (i.e., we denote the image of a pair $(r, m) \in R \times M$ under this map by rm or $r \cdot m$)

such that the following properties (the "**module axioms**") hold:

- $(M, +, 0)$ is an abelian group.
- The **right distributivity law** holds: We have $(r + s)\, m = rm + sm$ for all $r, s \in R$ and $m \in M$.

[94] Here I am leaving the zero and the unity unmentioned, for the sake of brevity.

- The **left distributivity law** holds: We have $r(m+n) = rm + rn$ for all $r \in R$ and $m, n \in M$.
- The **associativity law** holds: We have $(rs)\,m = r\,(sm)$ for all $r, s \in R$ and $m \in M$.
- We have $0_R m = 0_M$ for every $m \in M$.
- We have $r \cdot 0_M = 0_M$ for every $r \in R$.
- We have $1m = m$ for every $m \in M$. (Here, "1" means the unity of R.)

When M is a left R-module, the elements of M are called **vectors**, and the elements of R are called **scalars**.

As the name "left R-module" suggests, there is an analogous notion of a **right R-module**:

Definition 3.1.2. Let R be a ring. A **right R-module** is defined just as a left R-module was defined in Definition 3.1.1, but with the following changes:

- For a right R-module M, the action is not a map from $R \times M$ to M, but rather a map from $M \times R$ to M.
- Accordingly, we use the notation mr (rather than rm) for the image of a pair (m, r) under this map.
- The axioms for a right R-module are similar to the module axioms for a left R-module, accounting for the different form of the action. For example, the associativity law for a right R-module is saying that $m\,(rs) = (mr)\,s$ for all $r, s \in R$ and $m \in M$.

When R is commutative, any left R-module becomes a right R-module in a natural way:

Proposition 3.1.3. Let R be a commutative ring. Then, we can make any left R-module M into a right R-module by setting

$$mr = rm \qquad \text{for all } r \in R \text{ and } m \in M. \tag{42}$$

Similarly, we can make any right R-module M into a left R-module by setting

$$rm = mr \qquad \text{for all } r \in R \text{ and } m \in M. \tag{43}$$

These two transformations are mutually inverse, so we shall use them to identify left R-modules with right R-modules. Thus, we can use the words "left R-module" and "right R-module" interchangeably, and just speak of

"R**-modules**" instead (without specifying whether they are left or right). We shall liberally do so in what follows. (Note that this is not allowed when R is not commutative!)

When R is a field, the R-modules are also known as the R**-vector spaces**. These are precisely the vector spaces you have seen in a linear algebra class. A left R-module over an arbitrary ring R is just the natural generalization of a vector space. But while vector spaces have a very predictable structure (in particular, a vector space is uniquely determined up to isomorphism by its dimension), modules can be wild (although the "nice" families of modules, like R^n for $n \in \mathbb{N}$, still exist for every ring). The wilder a ring is, the more diverse are its modules.

One more remark about Definition 3.1.1: The "$0_R m = 0_M$" and "$r \cdot 0_M = 0_M$" axioms are actually redundant (i.e., they follow from the other axioms). I leave it to you to check this.

Exercise 3.1.1. Check this!

3.1.2. Submodules and scaling

We will soon see some examples of R-modules; but let us first define R-submodules. If you have seen subspaces of a vector space, this definition won't surprise you:

Definition 3.1.4. Let R be a ring. Let M be a left R-module. An R**-submodule** (or, to be more precise, a **left** R**-submodule**) of M means a subset N of M such that

- we have $a + b \in N$ for any $a, b \in N$;
- we have $ra \in N$ for any $r \in R$ and $a \in N$;
- we have $0 \in N$ (where 0 means 0_M).

All three axioms in Definition 3.1.4 have names: The "$a + b \in N$" axiom is called "N is closed under addition"; the "$ra \in N$" axiom is called "N is closed under scaling"; the "$0 \in N$" axiom is called "N contains the zero vector". The word "scaling" that we have just used refers to the following operation:

Definition 3.1.5. Let R be a ring. Let M be a left R-module. Let $r \in R$ be a scalar. Then, **scaling** by r (on the module M) means the map

$$\begin{aligned} M &\to M, \\ m &\mapsto rm. \end{aligned}$$

This map is a group homomorphism from the additive group $(M, +, 0)$ to itself (since any $m, n \in M$ satisfy $r(m+n) = rm + rn$ and $r \cdot 0_M = 0_M$). In particular, scaling by 1 is the identity map $\mathrm{id}_M : M \to M$ (since $1m = m$ for each $m \in M$), whereas scaling by 0 sends each vector $m \in M$ to the zero vector 0_M.

The "$ra \in N$" axiom in Definition 3.1.4 is saying that N is closed under scaling by every scalar $r \in R$. We will soon see that an R-submodule of M is the same as a subgroup of the additive group $(M, +, 0)$ that is closed under scaling by every scalar $r \in R$.

Everything we have said about left R-modules can be equally said (mutatis mutandis) for right R-modules.

3.1.3. Examples

Here are some examples of modules:

- Let R be any ring. Then, R itself becomes a left R-module: Just define the action to be the multiplication of R. In this R-module, the elements of R play both the role of vectors and the role of scalars. Scaling a vector m by a scalar r just means multiplying m by r (that is, taking the product rm inside R).

  The R-submodules of this left R-module R are the subsets L of R that are closed under addition and contain 0 and satisfy $ra \in L$ for all $r \in R$ and $a \in L$. These subsets are called the **left ideals** of R. When R is commutative, these are precisely the ideals of R. For general R, however, the notion of an ideal is more restrictive than the notion of a left ideal (since an ideal L has to satisfy not only $ra \in L$ but also $ar \in L$ for all $r \in R$ and $a \in L$).

  For example, if R is the matrix ring $\mathbb{Q}^{2\times 2}$, then the only ideals of R are $\{0_{2\times 2}\}$ and R itself, but R has infinitely many left ideals (for example, the set of all matrices of the form $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix}$ is a left ideal).

- Let R be any ring. An R-module (left or right) is said to be **trivial** if it has only one element. The one-element set $\{0\}$ is a trivial left R-module (with addition given by $0 + 0 = 0$, action given by $r \cdot 0 = 0$, and zero vector 0) and a trivial right R-module (likewise).

- Let R be any ring, and let $n \in \mathbb{N}$. Then, the Cartesian product
$$R^n = \{(a_1, a_2, \ldots, a_n) \mid \text{all } a_i \text{ belong to } R\}$$
is a left R-module, where addition and action are defined entrywise: i.e., the addition is defined by
$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1,\ a_2 + b_2,\ \ldots,\ a_n + b_n)$$
$$\text{for all } a_1, a_2, \ldots, a_n \in R \text{ and } b_1, b_2, \ldots, b_n \in R,$$

and the action is defined by

$$r \cdot (a_1, a_2, \ldots, a_n) = (ra_1, ra_2, \ldots, ra_n) \text{ for all } r \in R \text{ and } a_1, a_2, \ldots, a_n \in R.$$

The zero vector of this R-module R^n is $(0, 0, \ldots, 0)$.

If $n = 0$, then the left R-module R^n is trivial, and its only element is the 0-tuple $()$.

- Let R be any ring, and let $n, m \in \mathbb{N}$. Consider the set $R^{n \times m}$ of all $n \times m$-matrices with entries in R. This set $R^{n \times m}$ is not a ring unless $n = m$ (since two $n \times m$-matrices cannot be multiplied unless $n = m$). However, it is always a left R-module, where addition and action are defined entrywise: e.g., the action is defined by

$$r \cdot \begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{pmatrix} = \begin{pmatrix} ra_{1,1} & ra_{1,2} & \cdots & ra_{1,m} \\ ra_{2,1} & ra_{2,2} & \cdots & ra_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ ra_{n,1} & ra_{n,2} & \cdots & ra_{n,m} \end{pmatrix}$$

for any $r, a_{i,j} \in R$.

The zero vector of this R-module $R^{n \times m}$ is the zero matrix $0_{n \times m}$.

The set $R^{n \times m}$ is also a right R-module (where addition and action are again defined entrywise, but the action now results in a matrix whose entries are $a_{i,j}r$ rather than $ra_{i,j}$).

According to Definition 3.1.1, the elements of this R-module $R^{n \times m}$ can thus be called "vectors", even though they are matrices. This shows that our concept of a "vector" is much more general than the classical notion of "vectors" from introductory linear algebra classes (i.e., row vectors and column vectors). This generality might be an acquired taste, but it is quite useful. For example, we will soon define linear combinations and linear independence of vectors; thus we will automatically obtain these notions for matrices.

Note that the zero vector of an R-module is uniquely determined by its addition (in fact, this is true for any group); thus, we don't even need to specify it explicitly when we define an R-module.

Exercise 3.1.2. Let R be a ring, and $n \in \mathbb{N}$. Consider the left R-module R^n.

(a) Prove that the set

$$\begin{aligned} A &:= \{(a_1, a_2, \ldots, a_n) \in R^n \mid a_1 = a_2 = \cdots = a_n\} \\ &= \left\{ \left(\underbrace{a, a, \ldots, a}_{n \text{ times}} \right) \mid a \in R \right\} \end{aligned}$$

is an R-submodule of R^n.

(b) Prove that the set

$$B := \{(a_1, a_2, \ldots, a_n) \in R^n \mid 1a_1 = 2a_2 = 3a_3 = \cdots = na_n\}$$

is an R-submodule of R^n.

(c) Prove that the set

$$C := \{(a_1, a_2, \ldots, a_n) \in R^n \mid a_1 a_2 \cdots a_n = 0\}$$

is an R-submodule of R^n only if R is trivial or $n = 1$.

(d) Prove that the set

$$D := \{(a_1, a_2, \ldots, a_n) \in R^n \mid a_i = a_{i-1} + a_{i-2} \text{ for all } i \geq 3\}$$

is an R-submodule of R^n.

3.1.4. Left vs. right R-modules in general

As we said above, the notion of a left R-module is not equivalent to the notion of a right R-module when R is a noncommutative ring. However, the general notion of a "left module over a ring" is equivalent to the general notion of a "right module over a ring". Indeed, the next exercise ([21w, homework set #2, Exercise 2 **(d)**]) provides a way to convert right modules into left modules (over a different ring):

Exercise 3.1.3. Let R be a ring. Define the opposite ring R^{op} as in Exercise 2.7.6.

Let M be a right R-module. Prove that M becomes a left R^{op}-module if we define an action of R^{op} on M by

$$rm = mr \qquad \text{for all } r \in R^{\mathrm{op}} \text{ and } m \in M.$$

(Here, the left hand side is to be understood as the image of (r, m) under the new action of R^{op} on M, whereas the right hand side is the image of (m, r) under the original action of R on M.)

Similarly, we can translate left R-modules into right R^{op}-modules. (This is just a generalization of Proposition 3.1.3 to arbitrary – i.e., not necessarily commutative – rings R.)

Thus, for any ring R, we can translate left R-modules into right R^{op}-modules and vice versa. As a consequence, any property of left R-modules can be translated into a property of right R^{op}-modules, and vice versa. The same holds with the words "left" and "right" interchanged. Thus, we can focus our study on left R-modules, knowing that everything we prove about them will also hold (with analogous proofs) for right R^{op}-modules, and thus (if we replace R by R^{op}) for right R-modules.

3.2. A couple generalities

Let us next show a few general properties of modules.

3.2.1. Negation, subtraction and scaling

Recall that when a group is written additively (i.e., its operation is denoted by $+$), the inverse of an element a of this group is denoted by $-a$ (and is called its additive inverse). The following proposition says that the additive inverse of a vector in an R-module can be obtained by scaling the vector by -1:

Proposition 3.2.1. Let R be a ring. Let M be a left R-module. Then, $(-1)\, m = -m$ for each $m \in M$. (Here, "-1" stands for -1_R.)

Proof. Let $m \in M$. Then, $1m = m$ (by one of the module axioms). Thus,

$$\begin{aligned}(-1)\, m + \underbrace{m}_{=1m} &= (-1)\, m + 1m \\ &= \underbrace{((-1)+1)}_{=0_R}\, m \qquad \text{(by the right distributivity axiom)} \\ &= 0_R m = 0_M \qquad \text{(by one of the module axioms)}.\end{aligned}$$

In other words, $(-1)\, m$ is an additive inverse of m. But the additive inverse of m is $-m$. Thus, we conclude that $(-1)\, m = -m$. This proves Proposition 3.2.1. □

Further properties of negation and scaling can easily be derived from this. For example:

Proposition 3.2.2. Let R be a ring. Let M be a left R-module. Let $r \in R$ and $m \in M$. Then,

$$(-r)\, m = -(rm) = r\,(-m) \tag{44}$$

and

$$(-r)\,(-m) = rm. \tag{45}$$

Proof. Left to the reader. (Just as in the proof of Proposition 3.2.1, argue that both $(-r)\, m$ and $r\,(-m)$ are additive inverses of rm. This proves (44). To get (45), apply (44) to $-m$ instead of m.) □

Proposition 3.2.3. Let R be a ring. Let M be a left R-module. Then, any R-submodule of M is a subgroup of the additive group $(M, +, 0)$.

Proof of Proposition 3.2.3. Let N be an R-submodule of M. Then, N is closed under addition and under scaling and contains the zero vector. Since N is closed under scaling, we have $(-1)\, m \in N$ for each $m \in N$. However, each

$m \in N$ satisfies $(-1)\, m = -m$ (by Proposition 3.2.1, applied to $a = m$) and thus $-m = (-1)\, m \in N$. In other words, N is closed under negation (= taking additive inverses). Thus, N is a subgroup of $(M, +, 0)$. □

Proposition 3.2.4. Let R be a ring. Let M be a left R-module. Then, an R-submodule of M is the same as a subgroup of the additive group $(M, +, 0)$ that is closed under scaling by every scalar $r \in R$.

Proof. Any R-submodule of M is a subgroup of the additive group $(M, +, 0)$ (by Proposition 3.2.3) that is closed under scaling by every scalar $r \in R$ (by the definition of a submodule). Conversely, any subgroup of the additive group $(M, +, 0)$ that is closed under scaling by every scalar $r \in R$ is an R-submodule of M (since it satisfies all the axioms for a submodule). Thus, Proposition 3.2.4. □

Proposition 3.2.5. Let R be a ring. Let M be a left R-module. Then, any R-submodule of M becomes a left R-module in its own right (just like a subring of a ring becomes a ring).

Proof. Let N be an R-submodule of M. Then, Proposition 3.2.3 shows that N is a subgroup of the additive group $(M, +, 0)$. Hence, $(N, +, 0)$ is a group. Since N is closed under scaling, we furthermore can define an action of R on N in the obvious way (viz., inheriting it from M). This makes N into a left R-module. This proves Proposition 3.2.5. □

We also have "distributivity laws for subtraction":

Proposition 3.2.6. Let R be a ring. Let M be a left R-module. Then:

(a) We have $(r - s)\, m = rm - sm$ for all $r, s \in R$ and $m \in M$.

(b) We have $r\,(m - n) = rm - rn$ for all $r \in R$ and $m, n \in M$.

Proof. LTTR. (The fastest way is to derive these properties from the distributivity laws by strategic application of (44).) □

3.2.2. Finite sums

Next, let us recall how we defined finite sums $\sum_{s \in S} a_s$ of elements of a ring. In the same way, we can define a finite sum $\sum_{s \in S} a_s$ of elements of any additive group, and thus a finite sum $\sum_{s \in S} a_s$ of elements of any R-module (since any R-module is an additive group). Thus, in particular, if $a_1, a_2, \ldots, a_n$ are n elements of an R-module M, then the finite sum $a_1 + a_2 + \cdots + a_n \in M$ is well-defined.

The following "generalized distributivity laws" hold in any left R-module:

Proposition 3.2.7. Let R be a ring. Let M be a left R-module. Then:

(a) We have

$$(r_1 + r_2 + \cdots + r_k)\, m = r_1 m + r_2 m + \cdots + r_k m$$

for any $r_1, r_2, \ldots, r_k \in R$ and $m \in M$.

(b) We have

$$r\,(m_1 + m_2 + \cdots + m_i) = rm_1 + rm_2 + \cdots + rm_i$$

for any $r \in R$ and $m_1, m_2, \ldots, m_i \in M$.

Proof. **(a)** This follows by applying the right distributivity law (one of the module axioms) many times. (More precisely, this follows by induction on k; the right distributivity law is used in the induction step. The induction base follows from the $0_R m = 0_M$ axiom.)

(b) This follows by applying the left distributivity law (one of the module axioms) many times. (More precisely, this follows by induction on i; the left distributivity law is used in the induction step. The induction base follows from the $r \cdot 0_M = 0_M$ axiom.) □

The following convention is useful when dealing with R-modules. Essentially, it says that (just as with products of multiple elements in a ring or in a group) we can drop parentheses when we scale an element of an R-module by several elements of R:

Convention 3.2.8. Let R be a ring. Let M be a left R-module. Let $r, s \in R$ and $m \in M$. Then, $(rs)\, m$ and $r\,(sm)$ are the same vector (by the associativity axiom in the definition of a left R-module). We shall denote this vector by rsm. Likewise, expressions like $r_1 r_2 \cdots r_k m$ (for $r_1, r_2, \ldots, r_k \in R$ and $m \in M$) will be understood.

Everything we said above about left R-modules can be adapted to right R-modules in a straightforward way; we leave the details to the reader.

3.2.3. Some exercises

Exercise 3.2.1. Let R be a ring. Let M be a left R-module. Let I be an R-submodule of M.

For any two elements $a, b \in M$, we write "$a \equiv b \bmod I$" (and say that "a is congruent to b modulo I") if and only if $a - b \in I$. (This is a generalization of congruence of integers, as it is usually defined in elementary number theory. Indeed, congruence of integers modulo an integer n is recovered when $R = \mathbb{Z}$ and $I = n\mathbb{Z}$.)

Prove the following:

(a) Each $a \in M$ satisfies $a \equiv a \bmod I$.

(b) If $a, b \in M$ satisfy $a \equiv b \bmod I$, then $b \equiv a \bmod I$.

(c) If $a, b, c \in M$ satisfy $a \equiv b \bmod I$ and $b \equiv c \bmod I$, then $a \equiv c \bmod I$.

(d) If $a, b, c, d \in M$ satisfy $a \equiv b \bmod I$ and $c \equiv d \bmod I$, then $a + c \equiv b + d \bmod I$.

(e) If $a, b \in M$ and $r \in R$ satisfy $a \equiv b \bmod I$, then $ra \equiv rb \bmod I$.

Now, we claim a sort of converse:

(f) Let us drop the requirement that I be an R-submodule of M. Instead, we require that I be any subset of M for which the claims of parts **(a)**, **(c)** and **(e)** of this exercise hold. Prove that I is an R-submodule of M.

Exercise 3.2.1 can be summarized as "modular arithmetic modulo a subset I of M works if and only if I is a submodule of M". In other words, roughly speaking, the submodules of a module M are precisely the subsets I that allow "working modulo I". This is most likely the reason why modules are called "modules"[95].

Exercise 3.2.2. Let R be a ring. Let M be a left R-module.

For any subset K of M, let $\operatorname{Ann} K$ denote the subset $\{r \in R \mid rk = 0 \text{ for all } k \in K\}$ of R. (This is called the **annihilator** of K.)

(a) Prove that $\operatorname{Ann} M$ is an ideal of R.

(b) Let K be any subset of M. Prove that $\operatorname{Ann} K$ is a left ideal of R. (Recall that a **left ideal** of R means a subset L of R that is closed under addition and contains 0 and satisfies $ra \in L$ for all $r \in R$ and $a \in L$.)

(c) Find an example showing that the $\operatorname{Ann} K$ in part **(b)** is not always an ideal of R.

3.3. More operations on modules and submodules

3.3.1. Direct products and direct sums

Fix a ring R. In Subsection 3.1.1, we have defined left R-modules (recall: these are essentially additive groups whose elements can be scaled by elements of R), and afterwards we have seen a few examples of them. Let me briefly repeat the two simplest examples:

- The ring R itself becomes a left R-module: Just define the action to be the multiplication of R. This is called the **natural left R-module** R. The

[95] The name was coined by Dedekind, although in a less general context.

R-submodules of this R-module are the left ideals of R. (Every ideal of R is a left ideal of R, but usually not vice versa.)

- For any $n \in \mathbb{N}$, the set

$$R^n = \{(a_1, a_2, \ldots, a_n) \mid \text{all } a_i \text{ belong to } R\}$$

is a left R-module, with addition and action being entrywise[96] and with the zero vector $(0, 0, \ldots, 0)$. This generalizes the Euclidean space $\mathbb{R}^n$ from linear algebra, and many of its analogues.

Here are some more examples:

- The left R-modules R^n (with $n \in \mathbb{N}$) tend to have many R-submodules. When R is a field, this is well-known from linear algebra (where R-submodules are called R-vector subspaces); in particular, the solution set of any given system of homogeneous linear equations in n variables is an R-submodule of R^n. The same applies to any commutative ring R, but here we have even more freedom: Besides equations, our system can contain congruences too (as long as they are linear and have no constant term). For instance, for $R = \mathbb{Z}$, the set

$$\Big\{(x, y, z, w) \in \mathbb{Z}^4 \mid x \equiv y \bmod 2 \text{ and } x + y + z + w \equiv 0 \bmod 3 \\ \text{and } x - y + z - w = 0\Big\}$$

is a $\mathbb{Z}$-submodule of $\mathbb{Z}^4$. To prove this, you need to check the axioms ("closed under addition", "closed under scaling" and "contains the zero vector"). With a bit of practice, you can do this all in your head.

If R is noncommutative, you have to be somewhat careful with the side on which the coefficients stand in your system. If the coefficients are on the **right** of the variables, then the solution set is a **left** R-module (so, e.g., if a and b are two elements of R, then $\{(x, y) \in R^2 \mid xa + yb = 0\}$ is a left R-module); on the other hand, if the coefficients are on the **left** of the variables, then the solution set is a **right** R-module. (Again, this is not hard to check: e.g., the set $\{(x, y) \in R^2 \mid xa + yb = 0\}$ is closed under the scaling maps of a left R-module because $xa + yb = 0$ implies $rxa + ryb = r\underbrace{(xa + yb)}_{=0} = 0$. Meanwhile, in general, this set is not closed under the scaling maps of a right R-module, since $xa + yb = 0$ does not imply $xra + yrb = 0$.)

[96] e.g., the action is defined by

$$r \cdot (a_1, a_2, \ldots, a_n) = (ra_1, ra_2, \ldots, ra_n) \text{ for all } r \in R \text{ and } a_1, a_2, \ldots, a_n \in R.$$

- Just as we defined the left R-module R^n consisting of all n-tuples, we can define a left R-module "R^∞" consisting of all infinite sequences. It is commonly denoted by $R^{\mathbb{N}}$ (since there are different kinds of infinity). Explicitly, we define the left R-module $R^{\mathbb{N}}$ by

$$R^{\mathbb{N}} := \{(a_0, a_1, a_2, \ldots) \mid \text{all } a_i \text{ belong to } R\},$$

  where addition and action are defined entrywise.

  This left R-module $R^{\mathbb{N}}$ has an R-submodule

$$\begin{aligned} R^{(\mathbb{N})} &:= \left\{(a_0, a_1, a_2, \ldots) \in R^{\mathbb{N}} \mid \text{only finitely many } i \in \mathbb{N} \text{ satisfy } a_i \neq 0\right\} \\ &= \left\{(a_0, a_1, a_2, \ldots) \in R^{\mathbb{N}} \mid \text{all but finitely many } i \in \mathbb{N} \text{ satisfy } a_i = 0\right\}. \end{aligned}$$

  You can check that this is indeed an R-submodule of $R^{\mathbb{N}}$. (For instance, it is closed under addition, because if only finitely many $i \in \mathbb{N}$ satisfy $a_i \neq 0$ and only finitely many $i \in \mathbb{N}$ satisfy $b_i \neq 0$, then only finitely many $i \in \mathbb{N}$ satisfy $a_i + b_i \neq 0$.)

  For example, if $R = \mathbb{Q}$, then

$$\begin{aligned} &(1, 1, 1, \ldots) \in R^{\mathbb{N}} \setminus R^{(\mathbb{N})} \\ \text{and} \quad &(0, 0, 0, \ldots) \in R^{(\mathbb{N})} \\ \text{and} \quad &(1, 0, 0, 0, \ldots) \in R^{(\mathbb{N})} \\ \text{and} \quad &\left(1, 0, 4, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) \in R^{(\mathbb{N})} \\ \text{and} \quad &\left(\underbrace{1, 0, 1, 0, 1, 0, \ldots}_{\text{ones and zeroes in turn}}\right) \in R^{\mathbb{N}} \setminus R^{(\mathbb{N})}. \end{aligned}$$

Generalizing R^n, here is a way to build modules out of other modules:

Definition 3.3.1. Let $n \in \mathbb{N}$, and let $M_1, M_2, \ldots, M_n$ be any n left R-modules. Then, the Cartesian product $M_1 \times M_2 \times \cdots \times M_n$ becomes a left R-module itself, where addition and action are defined entrywise: e.g., the action is defined by

$$r \cdot (m_1, m_2, \ldots, m_n) = (rm_1, rm_2, \ldots, rm_n) \text{ for all } r \in R \text{ and } m_i \in M_i.$$

This left R-module $M_1 \times M_2 \times \cdots \times M_n$ is called the **direct product** of $M_1, M_2, \ldots, M_n$.

If all of $M_1, M_2, \ldots, M_n$ are the natural left R-module R, then this direct product is precisely the left R-module R^n defined above.

This direct product $M_1 \times M_2 \times \cdots \times M_n$ can be generalized further, allowing products of infinitely many modules, too. Just as for rings, the best setting for this is using families, not lists:[97]

Proposition 3.3.2. Let I be any set. Let $(M_i)_{i \in I}$ be any family of left R-modules. Then, the Cartesian product

$$\prod_{i \in I} M_i = \left\{\text{all families } (m_i)_{i \in I} \text{ with } m_i \in M_i \text{ for all } i \in I\right\}$$

becomes a left R-module if we endow it with the entrywise addition (i.e., we set $(m_i)_{i \in I} + (n_i)_{i \in I} = (m_i + n_i)_{i \in I}$ for any two families $(m_i)_{i \in I}, (n_i)_{i \in I} \in \prod_{i \in I} M_i$) and the entrywise scaling (i.e., we set $r\,(m_i)_{i \in I} = (rm_i)_{i \in I}$ for any $r \in R$ and any family $(m_i)_{i \in I} \in \prod_{i \in I} M_i$) and with the zero vector $(0)_{i \in I}$.

Definition 3.3.3. This left R-module is denoted by $\prod_{i \in I} M_i$ and called the **direct product** of the left R-modules M_i. In some special cases, there are alternative notations for it:

- If $I = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$, then this left R-module is also denoted by $M_1 \times M_2 \times \cdots \times M_n$, and we identify a family $(m_i)_{i \in I} = (m_i)_{i \in \{1,2,\ldots,n\}}$ with the n-tuple $(m_1, m_2, \ldots, m_n)$. (Thus, $M_1 \times M_2 \times \cdots \times M_n$ is precisely the direct product $M_1 \times M_2 \times \cdots \times M_n$ we defined in Definition 3.3.1.)
- If all the left R-modules M_i are equal to some left R-module M, then their direct product $\prod_{i \in I} M_i = \prod_{i \in I} M$ is also denoted M^I. Note that this generalizes the $R^{\mathbb{N}}$ defined above.
- We set $M^n = M^{\{1,2,\ldots,n\}}$ for each $n \in \mathbb{N}$ and any left R-module M. This generalizes the left R-module R^n for $n \in \mathbb{N}$ discussed above.

This was quite predictable; but there is more. Indeed, we can generalize not just $R^{\mathbb{N}}$ but also its submodule $R^{(\mathbb{N})}$, and the result is at least as important:[98]

Proposition 3.3.4. Let I be any set. Let $(M_i)_{i \in I}$ be any family of left R-modules. Define $\bigoplus_{i \in I} M_i$ to be the subset

$$\left\{(m_i)_{i \in I} \in \prod_{i \in I} M_i \;\mid\; \text{only finitely many } i \in I \text{ satisfy } m_i \neq 0\right\}$$

[97] The proof of Proposition 3.3.2 is easy and LTTR.

[98] The proof of Proposition 3.3.4 is easy and LTTR.

of $\prod_{i\in I} M_i$. Then, $\bigoplus_{i\in I} M_i$ is a left R-submodule of $\prod_{i\in I} M_i$, and thus becomes a left R-module itself (by Proposition 3.2.5).

Definition 3.3.5. This left R-module $\bigoplus_{i\in I} M_i$ is called the **direct sum** of the R-modules M_i.

If $I = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$, then this left R-module is also denoted by $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

The last part of this definition might raise some eyebrows. In fact, if the set I is finite, then $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$ (since the condition "only finitely many $i \in I$ satisfy $m_i \neq 0$" is automatically satisfied for any family $(m_i)_{i\in I}$ when I is finite). Thus, in particular,

$$M_1 \oplus M_2 \oplus \cdots \oplus M_n = M_1 \times M_2 \times \cdots \times M_n$$

for any left R-modules $M_1, M_2, \ldots, M_n$. So we have introduced two notations for the same thing (and even worse, one of the notations looks like a sum, while the other looks like a product!). Nevertheless, both are in use. Direct sums start differing from direct products when the indexing set I is infinite.

For $I = \mathbb{N}$ and $M_i = R$, the direct sum $\bigoplus_{i\in I} M_i = \bigoplus_{i\in\mathbb{N}} R$ is precisely the R-module $R^{(\mathbb{N})}$ defined above. More generally:

Definition 3.3.6. Let I be a set. Let M be any left R-module. Then, $M^{(I)}$ is defined to be the left R-module $\bigoplus_{i\in I} M$.

Exercise 3.3.1. Let I be any set. Let $(M_i)_{i\in I}$ be any family of left R-modules. Let N_i be an R-submodule of M_i for each $i \in I$.

(a) Prove that $\prod_{i\in I} N_i$ is an R-submodule of the left R-module $\prod_{i\in I} M_i$.

(b) Prove that $\bigoplus_{i\in I} N_i$ is an R-submodule of the left R-module $\bigoplus_{i\in I} M_i$.

3.3.2. Restriction of modules

Here are some more ways to construct modules over rings:

- If R is a subring of a ring S, then S is a left R-module (where the action of R on S is defined by restricting the multiplication map $S \times S \to S$ to $R \times S$) and a right R-module (in a similar way).

  Let me restate this in a more down-to-earth way: If R is a subring of a ring S, then we can multiply any element of R with any element of S (since

both elements lie in the ring S); this makes S into a left R-module (and likewise, S becomes a right R-module). Explicitly, the action of R on the left R-module S is given by

$$rs = rs \qquad \text{for all } r \in R \text{ and } s \in S$$

(where the "rs" on the left hand side means the image of (r, s) under the action, whereas the "rs" on the right hand side means the product of r and s in the ring S).

Thus, for example, $\mathbb{C}$ is an $\mathbb{R}$-module (since $\mathbb{R}$ is a subring of $\mathbb{C}$) and also a $\mathbb{Q}$-module (for similar reasons). (In this sentence, you can just as well say "vector space" instead of "module", since $\mathbb{R}$ and $\mathbb{Q}$ are fields.)

- More generally: If R and S are any two rings, and if $f : R \to S$ is a ring morphism, then S becomes a left R-module (with the action of R on S being defined by

$$rs = f(r)\, s \qquad \text{for all } r \in R \text{ and } s \in S$$

) and a right R-module (in a similar way). The proof of this is easy. These R-module structures are sometimes said to be **induced** by the morphism f.

Our previous example (in which we made S into an R-module whenever R is a subring of S) is the particular case of this construction obtained when f is the canonical inclusion[99] of R into S.

Here are some other particular cases:

  - Any quotient ring R/I of a ring R (by some ideal I) becomes a left R-module, because the canonical projection $\pi : R \to R/I$ (which sends every $r \in R$ to its residue class $\overline{r} \in R/I$) is a ring morphism. Explicitly, the action of R on R/I is given by

$$r \cdot \overline{u} = \underbrace{\pi(r)}_{=\overline{r}} \cdot \overline{u} = \overline{r} \cdot \overline{u} = \overline{ru} \qquad \text{for all } r, u \in R.$$

    Similarly, R/I becomes a right R-module.

[99] Recall what "canonical inclusion" means:

If U is a subset of a set V, then the map

$$U \to V,$$
$$u \mapsto u$$

is called the **canonical inclusion** of U into V.

If U is a subring of a ring V, then the canonical inclusion of U into V is furthermore a ring morphism. (This follows trivially from the definition of a subring.)

– Here is another particular case (a less transparent one): I claim that the abelian group $\mathbb{Z}/5$ becomes a $\mathbb{Z}[i]$-module[100], if we define the action by

$$(a+bi)\cdot m = \overline{a+2b}\cdot m \qquad \text{for all } a+bi\in\mathbb{Z}[i] \text{ and } m\in\mathbb{Z}/5.$$

To wit, the map

$$\begin{aligned} f : \mathbb{Z}[i] &\to \mathbb{Z}/5, \\ a+bi &\mapsto \overline{a+2b} \end{aligned}$$

is a ring morphism (check this![101]); and this can be used to turn $\mathbb{Z}/5$ into a $\mathbb{Z}[i]$-module by our above construction; this yields precisely the action I claimed above (because all $a+bi\in\mathbb{Z}[i]$ and $m\in\mathbb{Z}/5$ satisfy $(a+bi)\cdot m = \underbrace{f(a+bi)}_{=\overline{a+2b}}\cdot m = \overline{a+2b}\cdot m$).

This is not the only way to turn $\mathbb{Z}/5$ into a $\mathbb{Z}[i]$-module. We could just as well use the ring morphism

$$\begin{aligned} g : \mathbb{Z}[i] &\to \mathbb{Z}/5, \\ a+bi &\mapsto \overline{a+3b} \end{aligned}$$

instead of f. This would give us a $\mathbb{Z}[i]$-module $\mathbb{Z}/5$ with action given by

$$(a+bi)\cdot m = \overline{a+3b}\cdot m \qquad \text{for all } a+bi\in\mathbb{Z}[i] \text{ and } m\in\mathbb{Z}/5.$$

Thus, we have obtained two **different** $\mathbb{Z}[i]$-module structures on $\mathbb{Z}/5$ – that is, two different $\mathbb{Z}[i]$-modules that are equal as sets (and

[100] As usual, $\mathbb{Z}[i]$ denotes the ring of the Gaussian integers, with $i=\sqrt{-1}$.

[101] Indeed, it is pretty easy to see that this map f respects addition, the zero and the unity. It remains to show that this map respects multiplication. To show this, we fix any $x,y\in\mathbb{Z}[i]$. We then need to show that $f(xy)=f(x)f(y)$.

Write x and y as $x=a+bi$ and $y=c+di$ for some $a,b,c,d\in\mathbb{Z}$. Then, $xy=(a+bi)(c+di)=(ac-bd)+(ad+bc)i$ (by the rule for multiplying complex numbers). Hence,

$$f(xy)=f((ac-bd)+(ad+bc)i)=\overline{ac-bd+2(ad+bc)} \tag{46}$$

(by the definition of f). On the other hand, $x=a+bi$ entails $f(x)=f(a+bi)=\overline{a+2b}$, and similarly we find $f(y)=\overline{c+2d}$. Multiplying these two equalities, we find

$$f(x)f(y)=\overline{a+2b}\cdot\overline{c+2d}=\overline{(a+2b)(c+2d)}=\overline{ac+2^2bd+2(ad+bc)} \tag{47}$$

(since $(a+2b)(c+2d)=ac+2^2bd+2(ad+bc)$). Now, the right hand sides of the equalities (46) and (47) are identical (since $2^2\equiv -1 \bmod 5$ and thus $\overline{2}^2=\overline{-1}$, so that $\overline{2^2bd}=\overline{-bd}$); hence, so are the left hand sides. In other words, $f(xy)=f(x)f(y)$. This completes the proof that the map f respects multiplication; therefore, f is a ring morphism.

even as additive groups) but different as $\mathbb{Z}[i]$-modules (and not even isomorphic as such). None of these two module structures is more natural or otherwise better than the other. Thus, when you speak of a "$\mathbb{Z}[i]$-module $\mathbb{Z}/5$", you need to clarify which one you mean. (Such situations are rather frequent in algebra. "Natural" R-module structures – i.e., structures that are clearly "the right one" – are rare in comparison.)

- Even more generally: If R and S are two rings, and if $f : R \to S$ is a ring morphism, then any left S-module M (not just S itself) naturally becomes a left R-module, with the action defined by

$$rm = f(r)\, m \qquad \text{for all } r \in R \text{ and } m \in M.$$

(You can think of this as letting R act on M "by proxy": In order to scale a vector $m \in M$ by a scalar $r \in R$, you just scale it by the scalar $f(r) \in S$.)

This method of turning S-modules into R-modules is called **restriction of scalars** (or, more specifically, **restricting** an S-module to R via f).

If we apply this method to a canonical inclusion (i.e., if R is a subring of S and if $f : R \to S$ is the canonical inclusion), then we conclude that any module over a ring naturally becomes a module over any subring.[102] For example, any $\mathbb{C}$-module naturally becomes an $\mathbb{R}$-module (this is known as "decomplexification" in linear algebra[103]) and a $\mathbb{Q}$-module and a $\mathbb{Z}$-module.

3.3.3. More examples

Here are some more general constructions of submodules in a given R-module (similar to some of the above constructions for ideals in a given ring):

Proposition 3.3.7. Let R be a ring. Let M be a left R-module. Let I and J be two R-submodules of M. Then, $I \cap J$ is an R-submodule of M as well.

Proposition 3.3.8. Let R be a ring. Let M be a left R-module.

(a) Let I and J be two R-submodules of M. Then,

$$I + J := \{i + j \mid i \in I \text{ and } j \in J\}$$

is an R-submodule of M as well.

[102] You can think of it as forgetting how to scale vectors by scalars that don't belong to the subring.

[103] Of course, again, linear algebraists speak of vector spaces instead of modules.

From linear algebra, you might also know a procedure going in the other direction: "complexification", which turns an $\mathbb{R}$-vector space into a $\mathbb{C}$-vector space. We will later learn how to generalize this to arbitrary ring morphisms.

(b) If I, J and K are three R-submodules of M, then $(I+J)+K = I+(J+K)$.

Proposition 3.3.9. Let R be a ring. Let I be an ideal of R. Let M be a left R-module. An (I,M)**-product** shall mean a product of the form im with $i \in I$ and $m \in M$. Then,

$$IM := \{\text{finite sums of } (I,M)\text{-products}\}$$

is an R-submodule of M.

Proof. This is fairly similar to the proof of the fact that the product IJ of two ideals I and J is again an ideal (see Exercise 2.11.1 **(a)**). □

Proposition 3.3.10. Let R be a commutative ring.

(a) Let $a \in R$. Let M be an R-module. Then,

$$aM := \{am \mid m \in M\}$$

is an R-submodule of M.

(b) In particular, $0M = \{0_M\}$ and $1M = M$ are R-submodules of M.

Proof. This is a straightforward generalization of Proposition 2.8.5. The proof is LTTR. □

Exercise 3.3.2. Prove Propositions 3.3.7, 3.3.8, 3.3.9 and 3.3.10.

Proposition 3.3.10 **(b)** holds for noncommutative rings R, too: If M is a left R-module, then $\{0_M\}$ and M are R-submodules of M. These are the "book-ends" for the R-submodules of M (in the sense that every R-submodule N of M satisfies $\{0_M\} \subseteq N \subseteq M$).

Proposition 3.3.10 **(a)** holds for noncommutative rings R as well, if we assume that a is a central element of R. (Of course, "R-module" should then be replaced by "left R-module".)

Exercise 3.3.3. Prove this claim.

Here are a few more examples of modules:

- Let $n \in \mathbb{N}$, and let R be a ring. The set R^n is not only a left R-module (as we have seen), but also a right $R^{n\times n}$-module[104], where the action of $R^{n\times n}$

[104]Recall that $R^{n\times n}$ is the ring of $n \times n$-matrices over R.

on R^n is the vector-by-matrix multiplication map

$$\begin{aligned} R^n \times R^{n \times n} &\to R^n, \\ (v, M) &\mapsto vM \end{aligned}$$

(where we identify n-tuples $v \in R^n$ with row vectors).

- More generally, for any $n, m \in \mathbb{N}$, the set $R^{n \times m}$ of all $n \times m$-matrices is a left $R^{n \times n}$-module and a right $R^{m \times m}$-module[105] (since an $n \times m$-matrix can be multiplied by an $n \times n$-matrix from the left and by an $m \times m$-matrix from the right, and since the module axioms follow from the standard laws of matrix multiplication such as associativity and distributivity). Even better, this set is a so-called $(R^{n \times n}, R^{m \times m})$-bimodule (we will later define this notion; essentially it means a left and a right module structure that fit together well).

- Let us study a particular case of this.

  Namely, let R be a field F, and let $n = 2$. So F^2 is a left F-module, with the action given by

  $$\lambda (a, b) = (\lambda a, \lambda b) \qquad \text{for all } \lambda, a, b \in F,$$

  and is a right $F^{2 \times 2}$-module, with the action given by

  $$(a, b) \begin{pmatrix} x & y \\ z & w \end{pmatrix} = (ax + bz, ay + bw) \qquad \text{for all } a, b, x, y, z, w \in F.$$

  What are the F-submodules of F^2 ? These are precisely the F-vector subspaces of F^2; as you know from linear algebra, these subspaces are the whole F^2 as well as the zero subspace $\{0_{F^2}\}$ and all lines through the origin.

  What are the $F^{2 \times 2}$-submodules of F^2 ? Only F^2 and $\{0_{F^2}\}$, because any two nonzero vectors in F^2 can be mapped to one another by a 2×2-matrix.

  Now, consider the subring

  $$F^{2 \geq 2} := \left\{ \begin{pmatrix} x & 0 \\ z & w \end{pmatrix} \mid x, z, w \in F \right\}$$

  of $F^{2 \times 2}$. This is the ring of all lower-triangular 2×2-matrices over F. (Yes, it is a subring of $F^{2 \times 2}$, since the sum and the product of two lower-triangular matrices are lower-triangular and since the zero and identity matrices are lower-triangular.) Since F^2 is a right $F^{2 \times 2}$-module, F^2 must also be a right $F^{2 \geq 2}$-module (by restriction). What are the $F^{2 \geq 2}$-submodules of F^2 ? Only F^2 and $\{0_{F^2}\}$ and $\{(a, 0) \mid a \in F\}$. (You might have to prove this on a future homework set.)

[105] This is in addition to it being a left R-module and a right R-module!

Exercise 3.3.4. Let I and J be two ideals of a ring R. Let M be a left R-module. Prove that $(IJ)\,M = I\,(JM)$.

[Note that this generalizes the identity $(IJ)\,K = I\,(JK)$ in Proposition 2.11.2 **(e)**.)

3.4. Abelian groups as $\mathbb{Z}$-modules ([DumFoo04, §10.1])

Now, let us try to understand $\mathbb{Z}$-modules in particular.

3.4.1. The action of $\mathbb{Z}$ by repeated addition

Let us recall one of the most basic definitions in elementary mathematics: the definition of multiplication of integers.

Multiplication of nonnegative integers was defined by repeated addition: If $n, m \in \mathbb{N}$, then nm means $\underbrace{m+m+\cdots+m}_{n \text{ times}}$. This same formula $nm = \underbrace{m+m+\cdots+m}_{n \text{ times}}$ can be applied to negative integers m as well, but not to negative integers n, since there is no such thing as $\underbrace{m+m+\cdots+m}_{-5 \text{ times}}$. Thus, the product nm for negative n had to be defined differently; one way to define it is by setting $nm = -\left(\underbrace{m+m+\cdots+m}_{-n \text{ times}}\right)$ (thus using negation to reduce the case of negative n to the case of positive n). Thus, for arbitrary integers n and m, the product nm is defined by

$$nm = \begin{cases} \underbrace{m+m+\cdots+m}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{m+m+\cdots+m}_{-n \text{ times}}\right), & \text{if } n < 0. \end{cases}$$

The same definition can be adapted to any abelian group:

Proposition 3.4.1. Let A be an abelian group. Assume that A is written additively (i.e., the operation of A is denoted by $+$, and the neutral element by 0). For any $n \in \mathbb{Z}$ and $a \in A$, define

$$na = \begin{cases} \underbrace{a+a+\cdots+a}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{a+a+\cdots+a}_{-n \text{ times}}\right), & \text{if } n < 0. \end{cases} \tag{48}$$

Thus, we have defined a map

$$\begin{aligned} \mathbb{Z} \times A &\to A, \\ (n, a) &\mapsto na. \end{aligned}$$

We shall refer to this map as the **action of $\mathbb{Z}$ by repeated addition** (due to the way na was defined in (48)).

(a) The group A becomes a $\mathbb{Z}$-module (where we take this map as the action of $\mathbb{Z}$ on A, and the pre-existing addition of A as the addition).

(b) This is the **only** $\mathbb{Z}$-module structure on A. That is, if A is **any** $\mathbb{Z}$-module, then the action of $\mathbb{Z}$ on A is given by the formula (48) (and is therefore uniquely determined by the abelian group structure on A).

(c) The $\mathbb{Z}$-submodules of A are precisely the subgroups of A.

Proof of Proposition 3.4.1. LTTR. Here are the main ideas:

(a) You have to prove axioms like $(n+m)\,a = na + ma$ and $n\,(a+b) = na + nb$ and $(nm)\,a = n\,(ma)$ for all $n, m \in \mathbb{Z}$ and $a, b \in A$. These facts are commonly proved for $A = \mathbb{Z}$ in standard texts on the construction of the number system; if you pick the "right" proofs, then you can adapt them to the general case just by replacing $\mathbb{Z}$ by A. The main idea is "reduce to the case when n and m are nonnegative, and then prove them by induction on n and m". The details are rather laborious, as there are several cases to discuss based on the signs of n, m and $n+m$.

(b) Given **any** $\mathbb{Z}$-module structure on A, we must have

$$\begin{aligned} na &= \underbrace{(1+1+\cdots+1)}_{n \text{ times}}\, a = \underbrace{1a+1a+\cdots+1a}_{n \text{ times}} \qquad \text{(by Proposition 3.2.7 \textbf{(a)})} \\ &= \underbrace{a+a+\cdots+a}_{n \text{ times}} \qquad \text{(by the } 1a = a \text{ axiom)} \end{aligned}$$

for any $n \in \mathbb{N}$ and any $a \in A$. This proves the "top half" of (48). It is not hard to prove the "bottom half" either (use the right distributivity axiom to see that $na + (-n)\,a = \underbrace{(n+(-n))}_{=0}\,a = 0a = 0$).

(c) Proposition 3.2.3 (applied to $R = \mathbb{Z}$ and $M = A$) shows that any $\mathbb{Z}$-submodule of A is a subgroup of A. Conversely, we must prove that if B is a subgroup of A, then B is a $\mathbb{Z}$-submodule of A. So let B be a subgroup of A.

Then, any $n \in \mathbb{Z}$ and $b \in B$ satisfy

$$nb = \begin{cases} \underbrace{b+b+\cdots+b}_{n \text{ times}}, & \text{if } n \geq 0; \\ -\left(\underbrace{b+b+\cdots+b}_{-n \text{ times}}\right), & \text{if } n < 0 \end{cases} \in B$$

(since B is closed under addition and negation and contains 0). In other words, B is closed under scaling. Hence, B is a $\mathbb{Z}$-submodule of A (since B is a subgroup of A and therefore closed under addition and contains 0), qed. □

Proposition 3.4.1 reveals what $\mathbb{Z}$-modules really are: In general, when R is a ring, an R-module is an abelian group A with an extra structure (namely, an action of R on A); however, for $R = \mathbb{Z}$, this extra structure is redundant (in the sense that it can always be constructed in a unique way from the abelian group structure), and so a $\mathbb{Z}$-module is just an abelian group in fancy clothes.[106] Thus, we shall identify abelian groups with $\mathbb{Z}$-modules (at least when the abelian groups are written additively).

This has a rather convenient consequence: The theory of R-modules is a generalization of the theory of abelian groups. In particular, anything we have proved or will prove for R-modules can therefore be applied to abelian groups (by setting $R = \mathbb{Z}$).

3.4.2. A few words on $\mathbb{Q}$-modules and $\mathbb{R}$-modules

Thus, we have understood what $\mathbb{Z}$-modules are. What about $\mathbb{Q}$-modules? Not every abelian group can be made into a $\mathbb{Q}$-module:

Example 3.4.2. There is no $\mathbb{Q}$-module structure on $\mathbb{Z}/2$ (that is, there is no $\mathbb{Q}$-module whose additive group is $\mathbb{Z}/2$).

Proof. This follows from linear algebra (since $\mathbb{Q}$-modules are $\mathbb{Q}$-vector spaces and thus have dimensions; but $\mathbb{Z}/2$ is too large to have dimension 0 and yet too small to have dimension > 0). Alternatively, you can do it by hand: Assume that $\mathbb{Z}/2$ is a $\mathbb{Q}$-module in some way. Then,

$$\frac{1}{2} \cdot \left(2 \cdot \overline{1}\right) = \underbrace{\left(\frac{1}{2} \cdot 2\right)}_{=1} \cdot \overline{1} = 1 \cdot \overline{1} = \overline{1},$$

so that

$$\overline{1} = \frac{1}{2} \cdot \underbrace{\left(2 \cdot \overline{1}\right)}_{=\overline{0}} = \frac{1}{2} \cdot \overline{0} = \overline{0},$$

[106] Don't get me wrong: "redundant" and "in fancy clothes" doesn't mean "useless"; it just means that the scaling is determined by the abelian group structure.

which contradicts $\overline{1} \neq \overline{0}$. □

Thus we see that not every abelian group can be made into a $\mathbb{Q}$-module (unlike for $\mathbb{Z}$-modules). However, any abelian group that can be made into a $\mathbb{Q}$-module can only be made so in one way:

Exercise 3.4.1. Let A be an abelian group (written additively). Prove that there is at most one map $\mathbb{Q} \times A \to A$ that makes A into a $\mathbb{Q}$-module (where we take this map as the action of $\mathbb{Q}$ on A, and the pre-existing addition of A as the addition).

[**Hint:** Let $*_1$ and $*_2$ denote two such maps. Let $r, s \in \mathbb{Z}$ and $a \in A$ with $s \neq 0$. Your goal is to show that $\frac{r}{s} *_1 a = \frac{r}{s} *_2 a$. First prove that if two elements $u, v \in A$ satisfy $s *_1 u = s *_1 v$, then $u = v$.]

What about $\mathbb{R}$-modules? Here, we get neither existence nor uniqueness: There are abelian groups that cannot be made into $\mathbb{R}$-modules; there are also abelian groups that can be made into $\mathbb{R}$-modules in multiple different ways. So the action of $\mathbb{R}$ on an $\mathbb{R}$-module cannot be reconstructed from the underlying group of the latter (unlike for $\mathbb{Z}$ and $\mathbb{Q}$). "Most" rings behave more like $\mathbb{R}$ than like $\mathbb{Z}$ and $\mathbb{Q}$ in this regard.

Exercise 3.4.2.

(a) Prove that any nontrivial $\mathbb{R}$-module is uncountable as a set.

(b) Conclude that $\mathbb{Q}$ cannot be an $\mathbb{R}$-module (no matter how we define an action of $\mathbb{R}$ on $\mathbb{Q}$).

[**Hint:** If M is a nontrivial $\mathbb{R}$-module, and if $m \in M$ is nonzero, then argue that the elements rm for all $r \in \mathbb{R}$ have to be distinct.]

3.4.3. Repeated addition vs. scaling

If R is any ring and M is any R-module, then M is (in particular) an additive abelian group, and thus (by Proposition 3.4.1 **(a)**) becomes a $\mathbb{Z}$-module in a natural way (using the action of $\mathbb{Z}$ by repeated addition). How does this $\mathbb{Z}$-module structure relate to the original R-module structure on M ? The following proposition shows a certain consistency between the two:

Proposition 3.4.3. Let R be a ring. Let M be a left R-module. Then,

$$(nr)\, a = r\,(na) = n\,(ra) \qquad \text{for all } n \in \mathbb{Z},\ r \in R \text{ and } a \in M.$$

Here, we are using both the action of R on M (to make sense of expressions like ra) and the action of $\mathbb{Z}$ by repeated addition (to make sense of expressions like na).

Proof. LTTR. (For $n \geq 0$, this is just saying that

$$\underbrace{(r+r+\cdots+r)}_{n \text{ times}} a = r \underbrace{(a+a+\cdots+a)}_{n \text{ times}} = \underbrace{ra+ra+\cdots+ra}_{n \text{ times}},$$

which easily follows from Proposition 3.2.7. The case of $n < 0$ can be reduced to the case of $n > 0$ using (44).) □

3.5. Module morphisms ([DumFoo04, §10.2])

3.5.1. Definition

Module morphisms are defined similarly to ring morphisms, but you probably already know their definition from linear algebra: they are also known as linear maps. Let me recall the definition:

Definition 3.5.1. Let R be a ring. Let M and N be two left R-modules.

(a) A **left R-module homomorphism** (or, for short, **left R-module morphism**, or **left R-linear map**) from M to N means a map $f : M \to N$ that

- **respects addition** (i.e., satisfies $f(a+b) = f(a) + f(b)$ for all $a, b \in M$);
- **respects scaling** (i.e., satisfies $f(ra) = rf(a)$ for all $r \in R$ and $a \in M$);
- **respects the zero** (i.e., satisfies $f(0_M) = 0_N$).

You can drop the word "left" (and, e.g., just say "R-module morphism") when it is clear from the context.

(b) A **left R-module isomorphism** (or, informally, **left R-module iso**) from M to N means an invertible left R-module morphism $f : M \to N$ whose inverse $f^{-1} : N \to M$ is also a left R-module morphism.

(c) The left R-modules M and N are said to be **isomorphic** (this is written $M \cong N$) if there exists a left R-module isomorphism $f : M \to N$.

(d) We let $\mathrm{Hom}_R(M, N)$ be the set of all left R-module morphisms from M to N.

(e) Right R-module morphisms (and isomorphisms) are defined similarly.

It is not hard to show that the "respects the zero" axiom in Definition 3.5.1 **(a)** is redundant. (In fact, it is "doubly redundant": It follows from each of the other two axioms!)

3.5.2. Simple examples

Here are some examples of R-module morphisms:

- You have seen linear maps between vector spaces in linear algebra. These are precisely the left R-module morphisms when R is a field.
- Let $k \in \mathbb{Z}$. The map
$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}, \\ a &\mapsto ka \end{aligned}$$
is always a $\mathbb{Z}$-module morphism. (For comparison: It is a ring morphism only when $k = 1$.)
- More generally: Let R be a **commutative** ring. Let $k \in R$. Let M be any R-module. Then, the map
$$\begin{aligned} M &\to M, \\ a &\mapsto ka \end{aligned}$$
is an R-module morphism. (This is the map that we have called "scaling by k".)
- Even more generally: Let R be any ring (commutative or not), and let k be a central element of R. Let M be any left R-module. Then, the map
$$\begin{aligned} M &\to M, \\ a &\mapsto ka \end{aligned}$$
is a left R-module morphism. Indeed, this map respects scaling because we have
$$k(ra) = \underbrace{(kr)}_{\substack{=rk \\ \text{(since } k \text{ is central)}}} a = (rk)\, a = r(ka) \qquad \text{for all } r \in R \text{ and } a \in M.$$
It respects addition and the zero for similar reasons.
However, if k is not central, then this map is **not** a left R-module morphism in general.
- Let R be a ring. Let $n \in \mathbb{N}$. For any $i \in \{1, 2, \ldots, n\}$, the map
$$\begin{aligned} \pi_i : R^n &\to R, \\ (a_1, a_2, \ldots, a_n) &\mapsto a_i \end{aligned}$$
is a left R-module morphism.

More generally: If $(M_i)_{i \in I}$ is a family of left R-modules, and if $j \in I$, then the map

$$\begin{aligned} \pi_j : \prod_{i \in I} M_i &\to M_j, \\ (m_i)_{i \in I} &\mapsto m_j \end{aligned}$$

is a left R-module morphism. This follows immediately from the fact that the structure of $\prod_{i \in I} M_i$ (addition, action and zero) is defined entrywise.

- Let R be a ring. If M and N are two left R-modules, then the map

$$\begin{aligned} M \times N &\to N \times M, \\ (m, n) &\mapsto (n, m) \end{aligned}$$

is an R-module isomorphism.

- If R is any ring, and $n, m \in \mathbb{N}$ are arbitrary, then the map

$$\begin{aligned} R^{n \times m} &\to R^{m \times n}, \\ A &\mapsto A^T \end{aligned}$$

(which sends each matrix A to its transpose) is a left R-module isomorphism. (Indeed, it is an R-module morphism because of the formulas $(A+B)^T = A^T + B^T$ and $(rA)^T = rA^T$ and $0_{n \times m}^T = 0_{m \times n}$. It is an isomorphism because its inverse is the analogous map from $R^{m \times n}$ to $R^{n \times m}$.)

The $\mathbb{Z}$-module morphisms (i.e., the $\mathbb{Z}$-linear maps) are simply the group morphisms of additive groups:

Proposition 3.5.2. Let M and N be two $\mathbb{Z}$-modules. Then, the $\mathbb{Z}$-module morphisms from M to N are precisely the group morphisms from $(M, +, 0)$ to $(N, +, 0)$. In other words,

$$\operatorname{Hom}_{\mathbb{Z}}(M, N) = \{\text{group morphisms } (M, +, 0) \to (N, +, 0)\}.$$

Proof. We have to show that any group morphism $f : (M, +, 0) \to (N, +, 0)$ automatically respects the scaling – i.e., that it satisfies $f(na) = nf(a)$ for all $n \in \mathbb{Z}$ and $a \in M$. This is LTTR. □

Exercise 3.5.1. Let R be any ring. Consider the map

$$\begin{aligned} S : R^{\mathbb{N}} &\to R^{\mathbb{N}}, \\ (a_0, a_1, a_2, \ldots) &\mapsto (a_0,\ a_0 + a_1,\ a_0 + a_1 + a_2,\ a_0 + a_1 + a_2 + a_3,\ \ldots) \\ &= (b_0, b_1, b_2, \ldots) \text{ where } b_i = a_0 + a_1 + \cdots + a_i. \end{aligned}$$

Consider furthermore the map

$$\begin{aligned}\Delta : R^{\mathbb{N}} &\to R^{\mathbb{N}}, \\ (a_0, a_1, a_2, \ldots) &\mapsto (a_0,\ a_1 - a_0,\ a_2 - a_1,\ a_3 - a_2,\ \ldots) \\ &= (c_0, c_1, c_2, \ldots) \text{ where } c_0 = a_0 \text{ and } c_i = a_i - a_{i-1} \text{ for all } i \geq 1.\end{aligned}$$

(a) Prove that S and Δ are R-linear maps and are mutually inverse.

(b) Recall the R-submodule

$$R^{(\mathbb{N})} = \left\{ (a_0, a_1, a_2, \ldots) \in R^{\mathbb{N}} \mid \text{only finitely many } i \in \mathbb{N} \text{ satisfy } a_i \neq 0 \right\}$$

of $R^{\mathbb{N}}$. Define a further R-submodule $R^{(\mathbb{N})+}$ of $R^{\mathbb{N}}$ by

$$R^{(\mathbb{N})+} := \left\{ (a_0, a_1, a_2, \ldots) \in R^{\mathbb{N}} \mid \text{there exists a } c \in R \text{ such that only finitely many } i \in \mathbb{N} \text{ satisfy } a_i \neq c \right\}.$$

(Thus, a sequence $(a_0, a_1, a_2, \ldots) \in R^{\mathbb{N}}$ belongs to $R^{(\mathbb{N})+}$ if and only if starting from some point on, all its entries are equal.)

Clearly, $R^{(\mathbb{N})}$ is a proper subset of $R^{(\mathbb{N})+}$ (unless R is trivial).

Prove that $R^{(\mathbb{N})} \cong R^{(\mathbb{N})+}$ as left R-modules, and in fact the restriction of the map S to $R^{(\mathbb{N})}$ is a left R-module isomorphism from $R^{(\mathbb{N})}$ to $R^{(\mathbb{N})+}$.

3.5.3. Ring morphisms as module morphisms

Let me give one more, slightly confusing example of module morphisms. Namely, I claim that any ring morphism is a module morphism, as long as the module structures are defined correctly (warning: these are often not the module structures you expect!). To wit:

- Let R and S be two rings. Let $f : R \to S$ be a ring morphism. As we have seen in Subsection 3.3.2, the ring S then becomes a left R-module, with the action of R on S being defined by

$$rs = f(r)\, s \qquad \text{for all } r \in R \text{ and } s \in S.$$

  This action is called the action on S induced by f. It is now easy to see that f is a left R-module morphism from R to S.

  Here is an example. There is a ring morphism $f : \mathbb{C} \to \mathbb{C}$ that sends each complex number $z = a + bi$ (with $a, b \in \mathbb{R}$) to its complex conjugate $\overline{z} = a - bi$. Thus, from the previous paragraph, we can conclude that this morphism f is a $\mathbb{C}$-module morphism from $\mathbb{C}$ to $\mathbb{C}$. But this is only true if the $\mathbb{C}$-module structure on the target (but not on the domain) is the one induced by f (so it is given by $rs = f(r)\, s = \overline{r}s$ for all $r \in \mathbb{C}$ and $s \in \mathbb{C}$),

which is of course a rather nonstandard choice of a $\mathbb{C}$-module structure on $\mathbb{C}$. So f is indeed a $\mathbb{C}$-module morphism from $\mathbb{C}$ to $\mathbb{C}$, but these are two different $\mathbb{C}$-modules $\mathbb{C}$!

Of course, writing things like this is just inviting confusion. To avoid this confusion, you need to introduce a new notation for the nonstandard $\mathbb{C}$-module $\mathbb{C}$ (the one induced by f). Namely, let us denote this new $\mathbb{C}$-module by $\overline{\mathbb{C}}$, while the unadorned symbol $\mathbb{C}$ will always mean the old, obvious $\mathbb{C}$-module structure on $\mathbb{C}$ (in which the action is just the multiplication). Thus, what we said in the previous paragraph can be restated as follows: The map f is a $\mathbb{C}$-module morphism from $\mathbb{C}$ to $\overline{\mathbb{C}}$. Actually, it is easy to see that f is a $\mathbb{C}$-module **isomorphism** from $\mathbb{C}$ to $\overline{\mathbb{C}}$. Thus, the $\mathbb{C}$-modules $\mathbb{C}$ and $\overline{\mathbb{C}}$ are isomorphic (but still should not be identified to prevent confusion).

More generally, since $f : \mathbb{C} \to \mathbb{C}$ is a ring morphism, we can restrict any $\mathbb{C}$-module M to $\mathbb{C}$ via f. This means the following: If M is a $\mathbb{C}$-module, then we define a new $\mathbb{C}$-module structure on M by

$$rm = f(r)\, m = \overline{r}m \qquad \text{for all } r \in \mathbb{C} \text{ and } m \in M$$

(where the "rm" on the left hand side refers to the new $\mathbb{C}$-module structure, whereas the "$f(r)\, m$" and "$\overline{r}m$" refer to the old one). This new $\mathbb{C}$-module is called $\overline{M}$ (since calling it M would be asking for trouble). It is a "twisted version" of M: It is identical to M as an abelian group, but the action of $\mathbb{C}$ on it has been "twisted" (in the sense that scaling by z on $\overline{M}$ is the same as scaling by $\overline{z}$ on M).

Here is a nice thing about these twisted $\mathbb{C}$-modules: If V and W are two $\mathbb{C}$-modules (i.e., $\mathbb{C}$-vector spaces), then a $\mathbb{C}$-module morphism $g : V \to \overline{W}$ is what is known as an **antilinear map** from V to W in linear algebra. Thus, antilinear maps are "secretly" just linear maps, once you have twisted the vector space structure on the target.

3.5.4. General properties of linearity

We shall now state a bunch of general facts about module morphisms that are analogous to some facts we have previously stated for ring morphisms. I won't distract you with the proofs, as they are all straightforward.

We fix a ring R.

Proposition 3.5.3. Let M and N be two left R-modules. Let $f : M \to N$ be an invertible left R-module morphism. Then, f is a left R-module isomorphism.

Proposition 3.5.4. Let M, N and P be three left R-modules. Let $f : N \to P$ and $g : M \to N$ be two left R-module morphisms. Then, $f \circ g : M \to P$ is a left R-module morphism.

Proposition 3.5.5. Let M, N and P be three left R-modules. Let $f : N \to P$ and $g : M \to N$ be two left R-module isomorphisms. Then, $f \circ g : M \to P$ is a left R-module isomorphism.

Proposition 3.5.6. Let M and N be two left R-modules. Let $f : M \to N$ be a left R-module isomorphism. Then, $f^{-1} : N \to M$ is a left R-module isomorphism.

Corollary 3.5.7. The relation $\cong$ for left R-modules is an equivalence relation.

Left R-module isomorphisms preserve all "intrinsic" properties of left R-modules (just like ring isomorphisms do for properties of rings). For example, if M and N are two isomorphic left R-modules, then M has as many R-submodules as N does (and there is a one-to-one correspondence between the R-submodules of M and those of N).

All of this holds just as well for right R-modules; by now this is so obvious that we don't even need to say it. (Besides, as you have seen in Exercise 3.1.3, right R-modules can be transformed into left R^{op}-modules for a certain ring R^{op}. This can also be done in reverse, and thus provides a dictionary between left modules and right modules, which can always be used to translate a statement about one kind of modules into a statement about the other. Module morphisms behave as one would expect under this dictionary: When we use this dictionary to turn two right R-modules M and N into left R^{op}-modules, the right R-module morphisms from M to N become the left R^{op}-module morphisms from M to N. This gives you all excuses you might ever need to ignore right R-modules and only work with left R-modules, until you actually need certain "hybrid" modules with both left and right structures.)

3.5.5. Adding, subtracting and scaling R-linear maps

In a way, R-linear maps (i.e., R-module morphisms) behave even better than ring morphisms: If you add two ring morphisms f and g pointwise (i.e., form the map that sends every r to $f(r) + g(r)$), then the resulting map will not usually be a ring morphism. Meanwhile, R-linear maps can be added and sometimes scaled:

Exercise 3.5.2. Let R be a ring. Let M and N be two left R-modules. Recall that $\mathrm{Hom}_R(M, N)$ is the set of all left R-module morphisms from M to N.

Prove the following:

(a) The map

$$M \to N,$$
$$m \mapsto 0_N$$

is an R-module morphism (i.e., is R-linear). We shall call it the **zero morphism** and denote it by $\mathbf{0}$ (a boldfaced zero).

(b) If $f \in \mathrm{Hom}_R(M,N)$ and $g \in \mathrm{Hom}_R(M,N)$ are two R-linear maps from M to N, then the map

$$\begin{aligned} M &\to N, \\ m &\mapsto f(m) + g(m) \end{aligned}$$

is also an R-module morphism. We shall denote the latter map by $f+g$, and we shall call it the **(pointwise) sum** of f and g.

(c) The set $\mathrm{Hom}_R(M,N)$ becomes an additive abelian group if we define addition pointwise (i.e., for any $f \in \mathrm{Hom}_R(M,N)$ and $g \in \mathrm{Hom}_R(M,N)$, we define $f+g$ as in part **(b)** of this exercise). Its neutral element is the zero morphism $\mathbf{0} : M \to N$ defined in part **(a)** of this exercise. This group $\mathrm{Hom}_R(M,N)$ is called the **Hom group** of M and N.

(d) If r is a central element of R (see Definition 2.3.7 **(a)** for the meaning of "central"), and if $f \in \mathrm{Hom}_R(M,N)$ is an R-linear map from M to N, then the map

$$\begin{aligned} M &\to N, \\ m &\mapsto rf(m) \end{aligned}$$

is again R-linear (i.e., belongs to $\mathrm{Hom}_R(M,N)$). We shall denote this latter map by rf.

(e) Find an example where the claim of part **(d)** can go wrong if r is not assumed to be central.

(f) If R is commutative, then the Hom group $\mathrm{Hom}_R(M,N)$ (defined in part **(c)**) becomes an R-module, where the action is defined as follows: For any $r \in R$ and any $f \in \mathrm{Hom}_R(M,N)$, we define $rf \in \mathrm{Hom}_R(M,N)$ as in part **(d)**. (This is allowed because in a commutative ring R, every element r is central.)

3.5.6. Kernels and images

Next, we shall study kernels and images of module morphisms.

Again, we fix a ring R.

Definition 3.5.8. Let M and N be two left R-modules. Let $f : M \to N$ be a left R-module morphism. Then, the **kernel** of f (denoted $\ker f$ or $\mathrm{Ker}\, f$) is defined to be the subset

$$\mathrm{Ker}\, f := \{a \in M \mid f(a) = 0_N\}$$

of M.

Some examples:

- Let R be a commutative ring. Let $b \in R$. Then, the map

$$\begin{aligned} R &\to R, \\ r &\mapsto br \end{aligned}$$

is an R-module morphism (check this!). The kernel of this map is

$$\{r \in R \mid br = 0\}.$$

Assuming that $b \neq 0$, we thus conclude that this kernel is $\{0\}$ if and only if b is not a zero divisor.

- Both $\mathbb{Z}^3$ and $\mathbb{Z} \times (\mathbb{Z}/2)$ are $\mathbb{Z}$-modules (since we have seen in Proposition 3.4.1 that every additive group is a $\mathbb{Z}$-module). The map

$$\begin{aligned} \mathbb{Z}^3 &\to \mathbb{Z} \times (\mathbb{Z}/2), \\ (a,b,c) &\mapsto \left(a-b,\ \overline{b-c}\right) \end{aligned}$$

is a $\mathbb{Z}$-module morphism. Its kernel is

$$\begin{aligned} &\left\{(a,b,c) \in \mathbb{Z}^3 \mid \left(a-b,\ \overline{b-c}\right) = 0_{\mathbb{Z}\times(\mathbb{Z}/2)}\right\} \\ &= \left\{(a,b,c) \in \mathbb{Z}^3 \mid a-b=0 \text{ and } \overline{b-c}=0\right\} \\ &= \left\{(a,b,c) \in \mathbb{Z}^3 \mid a-b=0 \text{ and } b-c \equiv 0 \bmod 2\right\} \\ &= \left\{(a,b,c) \in \mathbb{Z}^3 \mid a=b \text{ and } b \equiv c \bmod 2\right\}. \end{aligned}$$

Kernels are a standard concept in linear algebra, where they are also called **nullspaces**. The following facts should be familiar from abstract linear algebra (but are also pretty easy to prove):

Theorem 3.5.9. Let M and N be two left R-modules. Let $f : M \to N$ be a left R-module morphism. Then, the kernel $\operatorname{Ker} f$ of f is a left R-submodule of M, whereas the image $\operatorname{Im} f = f(M)$ of f is a left R-submodule of N.

Lemma 3.5.10. Let M and N be two left R-modules. Let $f : M \to N$ be a left R-module morphism. Then, f is injective if and only if $\operatorname{Ker} f = \{0_M\}$.

Note that Lemma 3.5.10 is an analogue of Lemma 2.9.7.

Exercise 3.5.3. Prove Theorem 3.5.9 and Lemma 3.5.10.

3.6. Quotient modules

We fix a ring R for the entirety of Section 3.6.

3.6.1. Definition

We shall next define quotient modules of left R-modules, in more or less the same way as we defined quotient rings of rings (but this time we need to establish an action instead of a multiplication on the quotient):

Definition 3.6.1. Let I be a left R-submodule of a left R-module M. Thus, I is a subgroup of the additive group $(M, +, 0)$, hence a normal subgroup (since $(M, +, 0)$ is abelian). Therefore, the quotient group M/I itself becomes an abelian group. Its elements are the cosets $a + I$ of I in M.

Note that the addition on M/I is given by

$$(a + I) + (b + I) = (a + b) + I \qquad \text{for all } a, b \in M. \tag{49}$$

We now define an action of R on M/I by setting

$$r\,(a + I) = ra + I \qquad \text{for all } r \in R \text{ and } a \in M. \tag{50}$$

(See below for a proof that this is well-defined.)

The set M/I, equipped with the addition and the action we just defined and with the element $0 + I$ as zero vector, is a left R-module. This left R-module is called the **quotient left R-module** of M by the submodule I; it is also pronounced "M **modulo** I". It is denoted M/I (so when you hear "the left R-module M/I", it always means the set M/I equipped with the structure just mentioned).

The cosets $a + I$ are called **residue classes** modulo I, and are often denoted $a \bmod I$ or $[a]_I$ or $[a]$ or $\overline{a}$. (The last two notations are used when I is clear from the context.)

Theorem 3.6.2. Let M and I be as in Definition 3.6.1. Then, the action of R on M/I is well-defined, and M/I does indeed become a left R-module when endowed with the operations and elements just described.

Theorem 3.6.2 is an analogue of Theorem 2.9.2 for modules instead of rings, and its proof is analogous as well.

Using the notation $\overline{a}$ for the coset $a + I$, we can rewrite the formulas (49) and (50) as

$$\overline{a} + \overline{b} = \overline{a + b} \qquad \text{for all } a, b \in M \tag{51}$$

and

$$r \cdot \overline{a} = \overline{ra} \qquad \text{for all } r \in R \text{ and } a \in M. \tag{52}$$

The zero vector $0 + I$ of the quotient R-module M/I can, of course, be written as $\overline{0}$.

Remark 3.6.3. Note that the residue classes $\overline{a} = a + I$ in Definition 3.6.1 are precisely the equivalence classes of the "congruent modulo I" relation defined in Exercise 3.2.1. Thus, the quotient R-module M/I generalizes the classical notion of modular arithmetic in $\mathbb{Z}/n$.

Theorem 2.9.3, too, has an analogue for modules:

Theorem 3.6.4. Let I be a left R-submodule of a left R-module M. Consider the map

$$\begin{aligned} \pi : M &\to M/I, \\ a &\mapsto a + I. \end{aligned}$$

Then, π is a surjective R-module morphism with kernel I.

Definition 3.6.5. This morphism π is called the **canonical projection** from M onto M/I.

The proof of Theorem 3.6.4 is analogous to the proof of Theorem 2.9.3.

3.6.2. Examples

Examples of quotient modules can be easily created from various sources:

- Quotients of abelian groups are instances of quotient modules, since abelian groups are $\mathbb{Z}$-modules.
- Quotients of vector spaces are instances of quotient modules, since vector spaces are modules over a field.

  For instance, consider the 3-dimensional vector space (i.e., $\mathbb{R}$-module) $\mathbb{R}^3$ over the ring $\mathbb{R}$ of real numbers. This vector space $\mathbb{R}^3$ is typically viewed as a model for three-dimensional space. Define a vector subspace (i.e., $\mathbb{R}$-submodule) I of $\mathbb{R}^3$ by

  $$I = \left\{ (x,y,z) \in \mathbb{R}^3 \mid x + y + z = 0 \right\}.$$

  Geometrically, this is a hyperplane through the origin of $\mathbb{R}^3$. Now, consider the quotient $\mathbb{R}$-module (i.e., quotient vector space) $\mathbb{R}^3/I$. Its elements are residue classes of the form $\overline{(x,y,z)}$, where two vectors (x,y,z) and (x',y',z') belong to the same residue class if and only if their entrywise difference $(x-x',\ y-y',\ z-z')$ belongs to I (that is, if we have $(x-x') + (y-y') + (z-z') = 0$). For instance, the two residue classes $\overline{(3,0,0)}$ and $\overline{(1,1,1)}$ are identical (since $(3-1) + (0-1) + (0-1) = 0$), but the two residue classes $\overline{(1,0,0)}$ and $\overline{(2,0,0)}$ are not. It is not hard to see that each element of $\mathbb{R}^3/I$ can be uniquely written in the form $\overline{(r,0,0)}$ for some $r \in \mathbb{R}$. This shows that the vector space $\mathbb{R}^3/I$ is 1-dimensional.

- If R is any ring, and M is any left R-module, then the two obvious R-submodules $\{0_M\}$ and M of M lead to uninteresting quotient modules: The quotient module $M/\{0_M\}$ is isomorphic to M, whereas the quotient module M/M is trivial (i.e., has only one element).
- Let R be a ring. As we recall from Subsection 3.3.1, the left R-module $R^{\mathbb{N}}$ has an R-submodule $R^{(\mathbb{N})}$. How does the quotient module $R^{\mathbb{N}}/R^{(\mathbb{N})}$ look like? Its elements are residue classes of the form $\overline{(a_0, a_1, a_2, \ldots)}$, where two infinite sequences $(a_0, a_1, a_2, \ldots)$ and $(b_0, b_1, b_2, \ldots)$ belong to the same residue class if and only if their entrywise difference $(a_0 - b_0,\ a_1 - b_1,\ a_2 - b_2,\ \ldots)$ belongs to $R^{(\mathbb{N})}$ (that is, if the two sequences $(a_0, a_1, a_2, \ldots)$ and $(b_0, b_1, b_2, \ldots)$ agree at all but finitely many positions). Thus, we can view an element $\overline{(a_0, a_1, a_2, \ldots)}$ of $R^{\mathbb{N}}/R^{(\mathbb{N})}$ as an "infinite sequence determined up to finite change" (where "finite change" means changing finitely many entries). This kind of construction is frequent in analysis: For instance, the limit $\lim\limits_{n\to\infty} a_n$ of a sequence $(a_0, a_1, a_2, \ldots)$ of real numbers does not depend on finite changes (i.e., it does not change if we change finitely many entries of our sequence), and thus (if it exists) can be viewed as a property of the residue class $\overline{(a_0, a_1, a_2, \ldots)} \in R^{\mathbb{N}}/R^{(\mathbb{N})}$ (for $R = \mathbb{R}$).

3.6.3. The universal property of quotient modules

The universal property of quotient rings (Theorem 2.9.5), too, has an analogue for modules:

Theorem 3.6.6 (Universal property of quotient modules, elementwise form)**.** Let M be a left R-module. Let I be a left R-submodule of M.

Let N be a left R-module. Let $f : M \to N$ be a left R-module morphism. Assume that $f(I) = 0$ (this is shorthand for saying that $f(a) = 0$ for all $a \in I$). Then, the map

$$\begin{aligned} f' : M/I &\to N, \\ \overline{m} &\mapsto f(m) \qquad \text{(for all } m \in M\text{)} \end{aligned}$$

is well-defined (i.e., the value $f(m)$ depends only on the residue class $\overline{m}$, not on m itself) and is a left R-module morphism.

The proof of Theorem 3.6.6 is analogous to the proof of Theorem 2.9.5.

The abstract form of the universal property of quotient rings (Theorem 2.9.6) has an analogue for modules as well:

Theorem 3.6.7 (Universal property of quotient modules, abstract form)**.** Let M be a left R-module. Let I be a left R-submodule of M. Consider the canonical projection $\pi : M \to M/I$.

Let N be a left R-module. Let $f : M \to N$ be a left R-module morphism. Assume that $f(I) = 0$ (this is shorthand for saying that $f(a) = 0$ for all $a \in I$). Then, there is a unique left R-module morphism $f' : M/I \to N$ satisfying $f = f' \circ \pi$.

Just to unravel the abstract definition: This morphism f' is exactly the morphism f' from Theorem 3.6.6, i.e., it sends each coset (= residue class) $\overline{m} = m + I \in M/I$ to $f(m)$.

The proof of Theorem 3.6.7 is analogous to the proof of Theorem 2.9.6.

The equality $f = f' \circ \pi$ in Theorem 3.6.7 is oftentimes restated as follows: The diagram

$$\begin{array}{ccc} M & & \\ {\scriptstyle\pi}\downarrow & \searrow^{f} & \\ M/I & \xrightarrow[f']{} & N \end{array}$$

commutes.

3.6.4. The First Isomorphism Theorem for modules

The First Isomorphism Theorem for rings (Theorem 2.9.9) also has a counterpart for R-modules (with an equally straightforward proof):

Theorem 3.6.8 (First Isomorphism Theorem for modules, elementwise form)**.** Let M and N be two left R-modules, and let $f : M \to N$ be a left R-module morphism. Then:

(a) The kernel $\operatorname{Ker} f$ is an R-submodule of M. Thus, $M/\operatorname{Ker} f$ is a quotient module of M. As a set, $M/\operatorname{Ker} f$ is precisely the set M/f defined in Theorem 2.9.8 (applied to M and N instead of R and S). The f-classes (as defined in Theorem 2.9.8) are precisely the cosets of $\operatorname{Ker} f$.

(b) The image $f(M) := \{f(m) \mid m \in M\}$ of f is an R-submodule of N.

(c) The map

$$\begin{aligned} f' : M/\operatorname{Ker} f &\to f(M), \\ \overline{a} &\mapsto f(a) \end{aligned}$$

is well-defined and is a left R-module isomorphism.

(d) This map f' is precisely the map f' defined in Theorem 2.9.8 **(c)** (applied to M and N instead of R and S).

(e) Let $\pi : M \to M/\operatorname{Ker} f$ denote the **canonical projection** (i.e., the map that sends each $m \in M$ to its coset $\overline{m}$). Let $\iota : f(M) \to N$ denote the **canonical inclusion** (i.e., the map that sends each $n \in f(M)$ to n). Then, the map f' defined in part **(c)** satisfies

$$f = \iota \circ f' \circ \pi.$$

In other words, the diagram

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ {\scriptstyle\pi}\downarrow & & \uparrow{\scriptstyle\iota} \\ M/\operatorname{Ker} f & \xrightarrow[f']{} & f(M) \end{array} \tag{53}$$

is commutative.

(f) We have $M/\operatorname{Ker} f \cong f(M)$ as left R-modules.

All results we have stated so far about modules are analogues of known results about rings. So are their proofs (which is why we have omitted them). The Second and the Third isomorphism theorem for rings (which you have seen in Section 2.17) also have analogues for modules.

Remark 3.6.9. If you have done some abstract linear algebra, the formula $M/\operatorname{Ker} f \cong f(M)$ in Theorem 3.6.8 **(f)** might remind you of something.

Indeed, let R be a field. Thus, R-modules are R-vector spaces. Let M and N be two finite-dimensional R-vector spaces. Let $f : M \to N$ be a linear map. Thus, Theorem 3.6.8 **(f)** yields that $M/\operatorname{Ker} f \cong f(M)$ as R-modules (i.e., as R-vector spaces). However, isomorphic vector spaces have equal dimension. Hence, from $M/\operatorname{Ker} f \cong f(M)$, we obtain

$$\dim(M/\operatorname{Ker} f) = \dim(f(M)). \tag{54}$$

However, it is not hard to see (we will see it soon) that $\dim(M/I) = \dim M - \dim I$ whenever I is a vector subspace of M. (The idea behind this formula is that when you pass from M to M/I, you are "collapsing" the "dimensions" contained in I (since you are equating any vector in I with 0), and thus the dimension of the vector space should go down by $\dim I$. Formally speaking, this can be shown using bases. We will do so below.)

As a consequence of the $\dim(M/I) = \dim M - \dim I$ formula, we have

$$\dim(M/\operatorname{Ker} f) = \dim M - \dim(\operatorname{Ker} f).$$

Hence,

$$\dim M - \dim(\operatorname{Ker} f) = \dim(M/\operatorname{Ker} f) = \dim(f(M)) \qquad (\text{by (54)}).$$

This is the **rank-nullity formula** from linear algebra (indeed, $\dim(\operatorname{Ker} f)$ is called the **nullity** of f, whereas $\dim(f(M))$ is called the **rank** of f).

Here are some more exercises related to quotient modules:[107]

Exercise 3.6.1. Let R be a commutative ring. Let N be any R-module. For any R-module M, we define the R-module $\operatorname{Hom}_R(M, N)$ as in Exercise 3.5.2 **(f)**.

(a) Prove that $\operatorname{Hom}_R(R, N) \cong N$ as R-modules. More precisely, prove that the map

$$\begin{aligned} \operatorname{Hom}_R(R, N) &\to N, \\ f &\mapsto f(1) \end{aligned}$$

(which sends every R-linear map $f : R \to N$ to its value $f(1)$) is an R-module isomorphism.

(b) Let I be an ideal of R. Let N_I be the subset $\{a \in N \mid ia = 0 \text{ for all } i \in I\}$ of N. Prove that N_I is an R-submodule of N, and that the map

$$\begin{aligned} \operatorname{Hom}_R(R/I,\ N) &\to N_I, \\ f &\mapsto f(1) \end{aligned}$$

is an R-module isomorphism.

Exercise 3.6.2. For any two integers n and m with $m \neq 0$, prove that $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n,\ \mathbb{Z}/m) \cong \mathbb{Z}/\gcd(n, m)$ as $\mathbb{Z}$-modules. (Here, the $\mathbb{Z}$-module $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n,\ \mathbb{Z}/m)$ is defined as in Exercise 3.5.2 **(f)**.)

Exercise 3.6.3. Let I be any set. Let $(M_i)_{i \in I}$ be any family of left R-modules. Let N_i be an R-submodule of M_i for each $i \in I$.

(a) Prove that $\left(\prod_{i \in I} M_i\right) / \left(\prod_{i \in I} N_i\right) \cong \prod_{i \in I} (M_i / N_i)$ as left R-modules. (The left hand side is well-defined by Exercise 3.3.1 **(a)**.)

(b) Prove that $\left(\bigoplus_{i \in I} M_i\right) / \left(\bigoplus_{i \in I} N_i\right) \cong \bigoplus_{i \in I} (M_i / N_i)$ as left R-modules. (The left hand side is well-defined by Exercise 3.3.1 **(b)**.)

An analogue of the Chinese Remainder Theorem (Theorem 2.12.12 and Theorem 2.12.13) also exists for modules, although it still involves ideals:

[107] Recall once again that a commutative ring R is an R-module itself, and that its R-submodules are precisely its ideals.

Exercise 3.6.4. Prove the **Chinese Remainder Theorem for Modules**:

Let R be a commutative ring. Let $I_1, I_2, \ldots, I_k$ be k mutually comaximal ideals of R. Let M be a R-module. Then:

(a) We have $I_1M \cap I_2M \cap \cdots \cap I_kM = I_1I_2 \cdots I_kM$. (See Proposition 3.3.9 for the definition of IM for any ideal I of R. The notation "$I_1M \cap I_2M \cap \cdots \cap I_kM$" means "$(I_1M) \cap (I_2M) \cap \cdots \cap (I_kM)$".)

(b) There is an R-module isomorphism[108]

$$M/\left(I_1I_2 \cdots I_kM\right) \to (M/I_1M) \times (M/I_2M) \times \cdots \times (M/I_kM)$$

that sends each coset $m + I_1I_2 \cdots I_kM$ to the k-tuple $(m + I_1M,\ m + I_2M,\ \ldots,\ m + I_kM)$.

3.7. Spanning, linear independence, bases and free modules ([DumFoo04, §10.3])

Again, let us fix a ring R for the entirety of Section 3.7.

3.7.1. Definitions

We shall now generalize some classical notions from linear algebra (spanning, linear independence and bases) to arbitrary R-modules.

Definition 3.7.1. Let M be a left R-module. Let $m_1, m_2, \ldots, m_n$ be finitely many vectors in M.

(a) A **linear combination** of $m_1, m_2, \ldots, m_n$ means a vector of the form

$$r_1m_1 + r_2m_2 + \cdots + r_nm_n \qquad \text{with } r_1, r_2, \ldots, r_n \in R.$$

(b) The set of all linear combinations of $m_1, m_2, \ldots, m_n$ is called the **span** of $(m_1, m_2, \ldots, m_n)$, and is denoted by $\operatorname{span}(m_1, m_2, \ldots, m_n)$. (Note that [DumFoo04] calls it $R\{m_1, m_2, \ldots, m_n\}$.)

(c) If the span of $(m_1, m_2, \ldots, m_n)$ is M, then we say that the vectors $m_1, m_2, \ldots, m_n$ **span** M (or **generate** M).

(d) We say that the vectors $m_1, m_2, \ldots, m_n$ are **linearly independent** if the following holds: If $r_1, r_2, \ldots, r_n \in R$ satisfy

$$r_1m_1 + r_2m_2 + \cdots + r_nm_n = 0,$$

[108] The notation "M/IM" (where I is an ideal of R) means "$M/(IM)$".

then $r_1 = r_2 = \cdots = r_n = 0$. (In other words, the vectors $m_1, m_2, \ldots, m_n$ are said to be linearly independent if the only way to write 0 as a linear combination of them is $0 = 0m_1 + 0m_2 + \cdots + 0m_n$.)

(e) We say that the n-tuple $(m_1, m_2, \ldots, m_n)$ is a **basis** of the R-module M if $m_1, m_2, \ldots, m_n$ are linearly independent and span M.

(f) All of this terminology depends on R. Thus, if R is not clear from the context, we will clarify it by saying "R-linear combination" (or "linear combination over R") instead of just "linear combination", and likewise saying "R-span" or "R-linearly independent" or "R-basis".

Fine print: The property of n vectors $m_1, m_2, \ldots, m_n$ to span M is a joint property (i.e., it is a property of the **list** $(m_1, m_2, \ldots, m_n)$, not of each single vector). The same applies to linear independence. Sometimes, we do say that a single vector m spans M (for example, the vector $1 \in \mathbb{Z}$ spans the $\mathbb{Z}$-module $\mathbb{Z}$); this means that the one-element list (m) spans M.

Definition 3.7.1 was tailored to finite lists of vectors, but we can extend it to arbitrary (possibly infinite) families of vectors:

Definition 3.7.2. Let M be a left R-module. Let $(m_i)_{i \in I}$ be a family of vectors in M (with I being any set).

(a) A **linear combination** of $(m_i)_{i \in I}$ means a vector of the form

$$\sum_{i \in I} r_i m_i$$

for some family $(r_i)_{i \in I}$ of scalars (i.e., for some choice of $r_i \in R$ for each $i \in I$) with the property that

$$\text{all but finitely many } i \in I \text{ satisfy } r_i = 0. \tag{55}$$

Here, the sum $\sum_{i \in I} r_i m_i$ is an infinite sum, but all but finitely many of its addends are zero (thanks to the condition (55)). Such a sum is simply defined to be the sum of the nonzero addends. For example, $3 + 2 + 0 + 0 + 0 + \cdots = 3 + 2 = 5$.

(b) The set of all linear combinations of $(m_i)_{i \in I}$ is called the **span** of $(m_i)_{i \in I}$, and is denoted by $\operatorname{span}(m_i)_{i \in I}$. (Note that [DumFoo04] calls it $R\{m_i \mid i \in I\}$.)

(c) If the span of $(m_i)_{i \in I}$ is M, then we say that the family $(m_i)_{i \in I}$ **spans** M (or **generates** M).

(d) We say that the family $(m_i)_{i \in I}$ is **linearly independent** if the following holds: If some family $(r_i)_{i \in I}$ of scalars $r_i \in R$ has the properties that

$$\text{all but finitely many } i \in I \text{ satisfy } r_i = 0 \tag{56}$$

and that

$$\sum_{i \in I} r_i m_i = 0,$$

then $r_i = 0$ for all $i \in I$.

(e) We say that the family $(m_i)_{i \in I}$ is a **basis** of the R-module M if $(m_i)_{i \in I}$ is linearly independent and spans M.

(f) All of this terminology depends on R. Thus, if R is not clear from the context, we will clarify it by saying "R-linear combination" (or "linear combination over R") instead of just "linear combination", etc..

The infinite sums in this definition are a bit of a distraction, but a necessary one. Fortunately, when studying these notions, it is often sufficient to work with finite families (i.e., finite sets I), since they are in some sense representative of the general case. To wit:

Proposition 3.7.3. Let M be a left R-module. Let $(m_i)_{i \in I}$ be a family of vectors in M (with I being any set).

(a) Any linear combination of $(m_i)_{i \in I}$ is already a linear combination of some finite subfamily of $(m_i)_{i \in I}$. (That is: If m is a linear combination of $(m_i)_{i \in I}$, then there exists some finite subset J of I such that m is a linear combination of $(m_i)_{i \in J}$.)

(b) The family $(m_i)_{i \in I}$ is linearly independent if and only if all its finite subfamilies (i.e., all families of the form $(m_i)_{i \in J}$ with J being a finite subset of I) are linearly independent.

Proof. **(a)** Let m be a linear combination of $(m_i)_{i \in I}$. Thus, m has the form

$$m = \sum_{i \in I} r_i m_i$$

for some family $(r_i)_{i \in I}$ of scalars (i.e., for some choice of $r_i \in R$ for each $i \in I$) with the property that

$$\text{all but finitely many } i \in I \text{ satisfy } r_i = 0.$$

The latter property can be rewritten as follows: There exists a **finite** subset J of I such that all $i \in I \setminus J$ satisfy $r_i = 0$. Consider this J. Then, in the sum $\sum_{i \in I} r_i m_i$,

all the addends with $i \notin J$ are 0 (since these addends satisfy $i \notin J$, thus $i \in I \setminus J$, hence $r_i = 0$ and therefore $r_i m_i = 0 m_i = 0$). Hence, we can throw these addends away and are left with the finite sum $\sum_{i \in J} r_i m_i$. Therefore, $\sum_{i \in I} r_i m_i = \sum_{i \in J} r_i m_i$, so that $m = \sum_{i \in I} r_i m_i = \sum_{i \in J} r_i m_i$. This shows that m is a linear combination of the finite subfamily $(m_i)_{i \in J}$ of our original family $(m_i)_{i \in I}$. This proves Proposition 3.7.3 **(a)**.

(b) This is similar to part **(a)**. The details are left to the reader. (Again, the key is that the condition (56) allows us to restrict ourselves to a finite subset of I.) □

3.7.2. Spans are submodules

Next, we show that the span of a family of vectors is always a submodule:

Proposition 3.7.4. Let M be a left R-module. Let $(m_i)_{i \in I}$ be a family of vectors in M. Then, the span of this family is an R-submodule of M.

Proof. You have to show the following three statements:

1. The sum of two linear combinations of $(m_i)_{i \in I}$ is a linear combination of $(m_i)_{i \in I}$.
2. Scaling a linear combination of $(m_i)_{i \in I}$ by an $r \in R$ gives a linear combination of $(m_i)_{i \in I}$.
3. The zero vector is a linear combination of $(m_i)_{i \in I}$.

All three of these statements are easy. For example, let me show the first statement: Let v and w be two linear combinations of $(m_i)_{i \in I}$. Thus, we can write v and w as

$$v = \sum_{i \in I} a_i m_i \qquad \text{and} \qquad w = \sum_{i \in I} b_i m_i \tag{57}$$

for some two families $(a_i)_{i \in I}$ and $(b_i)_{i \in I}$ of scalars (i.e., for some choices of $a_i \in R$ and $b_i \in R$ for each $i \in I$) with the property that

$$\text{all but finitely many } i \in I \text{ satisfy } a_i = 0 \tag{58}$$

and that

$$\text{all but finitely many } i \in I \text{ satisfy } b_i = 0. \tag{59}$$

Now, adding the two equalities in (57) together, we obtain

$$\begin{aligned} v + w &= \sum_{i \in I} a_i m_i + \sum_{i \in I} b_i m_i = \sum_{i \in I} \left(a_i m_i + b_i m_i\right) \\ &= \sum_{i \in I} \left(a_i + b_i\right) m_i. \end{aligned} \tag{60}$$

Moreover, combining (58) with (59), we see that all but finitely many $i \in I$ satisfy $a_i = 0$ and $b_i = 0$ at the same time (since the union of two finite sets is still a finite set). Therefore, all but finitely many $i \in I$ satisfy $a_i + b_i = 0$ (because if $a_i = 0$ and $b_i = 0$, then $a_i + b_i = 0 + 0 = 0$). Hence, (60) shows that $v + w$ is a linear combination of $(m_i)_{i \in I}$. This proves Statement 1 above. The proofs of Statements 2 and 3 are even easier. □

3.7.3. Free modules

Definition 3.7.5.

(a) A left R-module is said to be **free** if it has a basis.

(b) Let $n \in \mathbb{N}$. A left R-module is said to be **free of rank** n if it has a basis of size n (i.e., a basis consisting of n vectors).

Note that a free R-module does not necessarily have a rank, since its basis could be infinite.[109]

Let us see some examples of modules that are free and modules that aren't.

You might want to look at $\mathbb{Q}$-modules at first; but they make for boring examples, because of the following fact:

Theorem 3.7.6. If F is a field, then every F-module (= F-vector space) is free.

Proof. This is just the famous fact from linear algebra that every vector space has a basis. In the most important case (which is when the vector space admits a finite spanning set – i.e., there is a finite list $(m_1, m_2, \ldots, m_n)$ of vectors that spans it[110]), this has fairly neat elementary proofs (see, e.g., Theorem 2.1 in Keith Conrad's `https://kconrad.math.uconn.edu/blurbs/linmultialg/dimension.pdf` , or [LaNaSc16, Theorem 5.3.4] or [Treil21, Chapter 1, Proposition 2.8]). In the general case, the proof is tricky and requires the Axiom of Choice (see Theorem 4.1 in Keith Conrad's `https://kconrad.math.uconn.edu/blurbs/zorn1.pdf`, or [Siksek21, Corollary 212] or [Philip23, Theorem 5.23 **(b)**]). □

For example, Theorem 3.7.6 shows that the $\mathbb{Q}$-vector space $\mathbb{R}$ is free, i.e., has a basis. Such bases are called **Hamel bases** and theoretically exist (if you believe in the Axiom of Choice). Practically, there is no way to construct one.

To find more interesting examples, we need to consider rings that are not fields. First of all, let us discuss a family of examples that exists for an arbitrary ring R:

[109] For some rings R, there also exist R-modules that are free of several ranks at the same time – e.g., an R-module can be free of rank 1 and free of rank 2 simultaneously. The simplest such example is when R is the trivial ring (in which case any R-module is trivial and free of any rank). More interesting examples exist for certain noncommutative rings – see, e.g., `https://math.stackexchange.com/questions/72723/` .

[110] Such vector spaces are called **finite-dimensional**.

- Consider the left R-module

$$R^2 = \{(a,b) \mid a \in R \text{ and } b \in R\}.$$

This R-module R^2 is free of rank 2, since the list $((1,0), (0,1))$ is a basis of it. Indeed:

  - The vectors $(1,0)$, $(0,1)$ span R^2 (because any vector (a,b) can be written as $a(1,0) + b(0,1)$, and thus is a linear combination of $(1,0)$, $(0,1)$).
  - The vectors $(1,0)$, $(0,1)$ are linearly independent, since $a(1,0) + b(0,1) = (a,b)$ can only be 0 if $a = b = 0$.

- Likewise, the left R-module R^3 has basis $((1,0,0), (0,1,0), (0,0,1))$.

- More generally: If $n \in \mathbb{N}$, then the left R-module R^n has basis

$$\begin{aligned}&((1,0,0,\ldots,0),\\ &\ (0,1,0,\ldots,0),\\ &\ (0,0,1,\ldots,0),\\ &\ \ \ldots,\\ &\ (0,0,0,\ldots,1)).\end{aligned}$$

This basis is called the **standard basis** of R^n, and its n vectors are called $e_1, e_2, \ldots, e_n$ (in this order). To make this more rigorous: For each $i \in \{1,2,\ldots,n\}$, we define e_i to be the vector in R^n whose i-th entry is 1 and whose all remaining entries are 0 (it is an n-tuple, like any vector in R^n). Then, the list $(e_1, e_2, \ldots, e_n)$ is a basis of the left R-module R^n. Thus, the R-module R^n is free of rank n.

- As a particular case, the left R-module R^1 is free of rank 1. Note that $R^1 \cong R$, because the map $R \to R^1$, $r \mapsto (r)$ (which merely wraps each scalar into a list to turn it into a vector) is an R-module isomorphism. Hence, the left R-module R is free of rank 1. Of course, you can see this directly as well: The one-element list (1) is a basis of it.

  Likewise, the left R-module R^0 is free of rank 0. Note that R^0 is a trivial R-module (it consists of just the zero vector); the empty list is a basis for it (since the only vector in R^0 is the zero vector and thus is a linear combination of nothing). Some authors (e.g., Keith Conrad in the above-mentioned references) avoid trivial R-modules[111], but there is no natural reason to do so except for the slight weirdness of dealing with empty lists and empty sums.

[111] A **trivial** R**-module** means an R-module that consists only of the zero vector.

- More generally: If I is a set, then[112]

$$R^{(I)} = \bigoplus_{i \in I} R = \left\{ (r_i)_{i \in I} \in R^I \ \mid \ \text{all but finitely many } i \in I \text{ satisfy } r_i = 0 \right\}$$

is a free R-module. It has a standard basis $(e_i)_{i \in I}$, where each e_j is the family that has a 1 in its j-th position and 0s in all other positions. (That is, $e_j = \left(\delta_{i,j}\right)_{i \in I}$, where $\delta_{i,j} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j \end{cases}$.)

This R-module $R^{(I)}$ is an R-submodule of

$$R^I = \prod_{i \in I} R = \left\{ (r_i)_{i \in I} \ \mid \ \text{all } r_i \text{ belong to } R \right\}.$$

When I is finite, we actually have $R^{(I)} = R^I$ (since the condition "all but finitely many $i \in I$ satisfy $r_i = 0$" is automatically true when I is finite). In general, however, $R^{(I)}$ is smaller than R^I, and the R-module $R^I = \prod_{i \in I} R$ is usually not free. (For example, the $\mathbb{Z}$-module $\mathbb{Z}^{\mathbb{N}}$ is not free. This is actually not easy to prove! A proof is sketched in [DumFoo04, §10.3, Exercise 24]. It is easy to see that the standard basis $(e_i)_{i \in \mathbb{N}}$ of $\mathbb{Z}^{(\mathbb{N})}$ is not a basis of $\mathbb{Z}^{\mathbb{N}}$, since (e.g.) the vector $(1, 1, 1, 1, \ldots)$ is not a linear combination of this family[113]. But it is much harder to show that there is no basis at all.)

- Let R be a ring. Let $n, m \in \mathbb{N}$. Then, the left R-module $R^{n \times m}$ of all $n \times m$-matrices is free. It has a basis $\left(E_{i,j}\right)_{(i,j) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}}$, which consists of the so-called **elementary matrices** $E_{i,j}$. For each $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, m\}$, the respective elementary matrix $E_{i,j}$ is defined to be the $n \times m$-matrix whose (i, j)-th entry is 1 while all its other entries are 0.

For example, for $n = 2$ and $m = 3$, this basis consists of the six elementary matrices

$$E_{1,1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad E_{1,2} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad E_{1,3} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix},$$

$$E_{2,1} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \qquad E_{2,2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \qquad E_{2,3} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

There are, of course, many other bases of $R^{n \times m}$ too.

[112] See Definition 3.3.6 for the meaning of the notation $R^{(I)}$ we are using here.

[113] Of course, you could write

$$(1, 1, 1, 1, \ldots) = 1e_0 + 1e_1 + 1e_2 + 1e_3 + 1e_4 + \cdots;$$

however, the sum on the right is properly infinite (with infinitely many nonzero coefficients) and thus does not count as a linear combination (as it fails the condition (55) from Definition 3.7.2).

- Let R be a ring. Let $n \in \mathbb{N}$. The set of all symmetric $n \times n$-matrices forms a left R-submodule $R^{n\times n}_{\text{symm}}$ of the left R-module $R^{n\times n}$. It, too, is free. For example, for $n = 2$, it has a basis consisting of the three matrices

$$E_{1,1} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad E_{1,2} + E_{2,1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad E_{2,2} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let us now look at $\mathbb{Z}$-modules. Recall that $\mathbb{Z}$-modules are the same as abelian groups (see Proposition 3.4.1), so free $\mathbb{Z}$-modules are also known as **free abelian groups** (this is not the same as free groups).

- Consider the $\mathbb{Z}$-submodule

$$U := \left\{ (a,b,c) \in \mathbb{Z}^3 \mid a+b+c = 0 \right\} \text{ of } \mathbb{Z}^3.$$

  Is U free? Can we find a basis for U ?

  So we are trying to find a basis for a submodule of $\mathbb{Z}^3$ that is determined by a set of linear equations (in our case, only one linear equation – namely, $a+b+c=0$). If we were using a field (e.g., $\mathbb{Q}$ or $\mathbb{R}$) instead of $\mathbb{Z}$, then this would be an instance of a classical problem from linear algebra (solving a system of homogeneous linear equations[114]), which can be solved by Gaussian elimination (see, e.g., [LaNaSc16, §A.3.2]). If we try to perform Gaussian elimination over $\mathbb{Z}$, we might run into trouble: Denominators may appear; as a result, we might not actually get vectors with integer entries. However, for the submodule U above, this does not happen, and we obtain the basis

$$((-1,1,0),\ (-1,0,1)).$$

  So U is indeed free.[115]

  What if we have a more complicated submodule and we do run into denominators? Thus, we do not get a basis using Gaussian elimination. Does this mean that no basis exists, or does it mean that we have to try something else? We will soon see.

- The $\mathbb{Z}$-module $\mathbb{Z}/2$ is not free (i.e., does not have a basis). Indeed, if it had a basis, then this basis would contain at least one vector (since $\mathbb{Z}/2$ is not trivial), but this vector would not be linearly independent, since scaling it by 2 would give 0.

- More generally, if M is any **finite** abelian group of size larger than 1, then M is not free (as a $\mathbb{Z}$-module), since a free $\mathbb{Z}$-module must be either trivial or infinite.

[114] more precisely: finding a basis for the solution space of such a system

[115] See Exercise 3.7.1 for a generalization of this.

- The $\mathbb{Z}$-module $\mathbb{Q}$ is not free (i.e., does not have a basis).

  Proof. Assume the contrary. Thus, there exists a $\mathbb{Z}$-basis $(m_i)_{i\in I}$ of $\mathbb{Q}$. The set I must be nonempty (since $\mathbb{Q}$ is not trivial); thus, we are in one of the following two cases:

  - *Case 1:* We have $|I| = 1$. In this case, I is a 1-element set, so we can rewrite our basis $(m_i)_{i\in I}$ as a list (m) that consists of a single rational number m. This single rational number m must span the entire $\mathbb{Z}$-module $\mathbb{Q}$. In other words, every element of $\mathbb{Q}$ must be a $\mathbb{Z}$-multiple of m. But this is absurd (indeed, if $m = 0$, then 1 is not a $\mathbb{Z}$-multiple of m; but otherwise, $\frac{1}{2}m$ is not a $\mathbb{Z}$-multiple of m).
  - *Case 2:* We have $|I| > 1$. In this case, there are at least two vectors m_u and m_v in this basis $(m_i)_{i\in I}$. However, two rational numbers are never $\mathbb{Z}$-linearly independent[116]. Thus, a fortiori, the whole family $(m_i)_{i\in I}$ cannot be $\mathbb{Z}$-linearly independent (since a subfamily of a linearly independent family of vectors must always be linearly independent). This contradicts the assumption that this family is a basis.

  Thus, in each case, we have found a contradiction, and our proof is complete.

- Now, consider the $\mathbb{Z}$-submodule

$$V := \left\{(a,b) \in \mathbb{Z}^2 \ \mid \ a \equiv b \bmod 2\right\} \text{ of } \mathbb{Z}^2.$$

  This $\mathbb{Z}$-submodule V contains the vectors $(0,2)$ and $(1,1)$ and $(1,-1)$ and $(4,-2)$ and many others. Is V free? Can we find a basis for V ?

  Let's try the pair $((2,0),\ (0,2))$. Is this pair a basis for V ? Its span is

$$\begin{aligned}\operatorname{span}((2,0),\ (0,2)) &= \{c\,(2,0) + d\,(0,2) \ \mid \ c,d \in \mathbb{Z}\} \\ &= \{(2c,2d) \ \mid \ c,d \in \mathbb{Z}\} \\ &= \left\{(a,b) \in \mathbb{Z}^2 \ \mid \ a \equiv b \equiv 0 \bmod 2\right\}.\end{aligned}$$

  This is a $\mathbb{Z}$-submodule of V, but not the entire V, since (for example) $(1,1)$ belongs to V but not to $\operatorname{span}((2,0),\ (0,2))$. So we have "undershot" our V (by finding a linearly independent family that does not span V).

[116] Indeed, let p and q be two rational numbers. We claim that there exist integers $a, b \in \mathbb{Z}$ that are not both 0 but still satisfy $ap + bq = 0$. (This will clearly prove that p and q are not $\mathbb{Z}$-linearly independent.)

Indeed, if $p = 0$, then we set $a = 1$ and $b = 0$ and are done. Something similar works if $q = 0$. So we WLOG assume that $p \neq 0$ and $q \neq 0$. Write p and q as $p = \frac{n}{d}$ and $q = \frac{m}{e}$ for some nonzero integers n, d, m, e (we can do this, since p and q are nonzero rational numbers). Then, $dmp + (-en)\,q = 0$ (check this!), so we have found our a and b (namely, $a = dm$ and $b = -en$).

Let's try the triple $((2,0),\ (0,2),\ (1,1))$. This triple does span V (check this!), but is not linearly independent, since

$$1 \cdot (2,0) + 1 \cdot (0,2) + (-2) \cdot (1,1) = 0.$$

So we have "overshot" V now (by finding a family that spans V but is not linearly independent).

Let us try to correct this by throwing away $(0,2)$. So we are left with the pair $((2,0),\ (1,1))$. And this pair is indeed a basis of V, as can easily be checked. Indeed, it is linearly independent (you can check this using linear algebra, since it clearly suffices to prove its $\mathbb{Q}$-linear independence[117]), and furthermore spans V because each $(a,b) \in V$ can be written as a linear combination of $(2,0),\ (1,1)$ as follows:

$$(a,b) = \underbrace{\frac{a-b}{2}}_{\substack{\in \mathbb{Z} \\ (\text{since } a \equiv b \bmod 2)}} \cdot (2,0) + b \cdot (1,1).$$

Another basis for V is the pair $((1,1),\ (1,-1))$. Indeed, this pair is linearly independent (check this!), and it spans V, because each $(a,b) \in V$ can be written as

$$(a,b) = \underbrace{\frac{a+b}{2}}_{\in \mathbb{Z}} \cdot (1,1) + \underbrace{\frac{a-b}{2}}_{\in \mathbb{Z}} \cdot (1,-1) \in \operatorname{span}((1,1),\ (1,-1)).$$

(See Exercise 3.7.2 for a generalization of V.)

Exercise 3.7.1. Let R be any ring. Let n be a positive integer. Let U be the subset

$$\{(a_1, a_2, \ldots, a_n) \in R^n \mid a_1 + a_2 + \cdots + a_n = 0\}$$

of the left R-module R^n.

(a) Prove that U is an R-submodule of R^n.

(b) Show that U is free, and prove that the $n-1$ vectors

$$\begin{aligned} &(1,-1,0,0,\ldots,0), \\ &(0,1,-1,0,\ldots,0), \\ &\ldots, \\ &(0,0,\ldots,0,1,-1) \end{aligned}$$

(that is, the $n-1$ vectors that consist of a number of 0's, followed by a 1, followed by a -1, followed again by a number of 0's) form a basis of U.

[117] Or you can check this directly: If $a, b \in \mathbb{Z}$ satisfy $a(2,0) + b(1,1) = 0$, then $0 = a(2,0) + b(1,1) = (2a+b,\ b)$, so that $(2a+b,\ b) = 0 = (0,0)$, and therefore $2a+b = 0$ and $b = 0$; but this quickly yields $a = b = 0$.

Exercise 3.7.2. Let n and k be two positive integers. Let V be the subset

$$\{(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n \mid a_1 \equiv a_2 \equiv \cdots \equiv a_n \bmod k\}$$

of the $\mathbb{Z}$-module $\mathbb{Z}^n$.

(a) Prove that V is a $\mathbb{Z}$-submodule of $\mathbb{Z}^n$.

(b) Show that V is free, and find a basis of V.

Exercise 3.7.3. Let R be any ring. Let $n \geq 2$ be an integer. Let W be the subset

$$\{(a_1, a_2, \ldots, a_n) \in R^n \mid a_i - a_{i-1} = a_{i+1} - a_i \text{ for each } i \in \{2, 3, \ldots, n-1\}\}$$

of the left R-module R^n. (This set W consists of all vectors $(a_1, a_2, \ldots, a_n) \in R^n$ whose entries "form an arithmetic progression", i.e., satisfy $a_2 - a_1 = a_3 - a_2 = a_4 - a_3 = \cdots = a_n - a_{n-1}$.)

(a) Prove that W is an R-submodule of R^n.

(b) Let $a = (1, 1, \ldots, 1) \in R^n$ and $b = (1, 2, \ldots, n) \in R^n$. Prove that (a, b) is a basis of W.

Exercise 3.7.4.

(a) Let X be the $\mathbb{Z}$-submodule

$$\left\{(a, b, c) \in \mathbb{Z}^3 \mid a \equiv b \bmod 2 \text{ and } b \equiv c \bmod 3\right\}$$

of $\mathbb{Z}^3$. Prove that X is free, and find a basis of X.

(b) Let Y be the $\mathbb{Z}$-submodule

$$\left\{(a, b, c) \in \mathbb{Z}^3 \mid a \equiv b \bmod 2 \text{ and } b \equiv c \bmod 3 \text{ and } c \equiv a \bmod 5\right\}$$

of $\mathbb{Z}^3$. Prove that Y is free, and find a basis of Y.

Exercise 3.7.5. Let R be any ring. A square matrix $A \in R^{n \times n}$ is said to be **antisymmetric** (or **skew-symmetric**) if $A^T = -A$ (where A^T is the transpose of A). For each $n \in \mathbb{N}$, we let $R^{n \times n}_{\text{asym}}$ denote the set of all antisymmetric $n \times n$-matrices in $R^{n \times n}$.

(a) Prove that $R^{n \times n}_{\text{asym}}$ is a left R-submodule of $R^{n \times n}$ for each $n \in \mathbb{N}$.

(b) Find a basis of the $\mathbb{Q}$-module $\mathbb{Q}^{2 \times 2}_{\text{asym}}$.

(c) Find a basis of the $\mathbb{Z}/2$-module $(\mathbb{Z}/2)^{2 \times 2}_{\text{asym}}$.

(d) Prove that the $\mathbb{Z}/4$-module $(\mathbb{Z}/4)^{2\times 2}_{\text{asym}}$ is not free (i.e., has no basis).

(This is somewhat surprising when compared to the R-module $R^{n\times n}_{\text{symm}}$ of symmetric $n \times n$-matrices, which module always has a basis. In a sense, it shows that antisymmetric matrices behave more wildly than symmetric matrices.)

[**Hint:** What exactly does the condition $A^T = -A$ say about the diagonal entries of a matrix A ?]

Exercise 3.7.6. Let R be any ring. A square matrix $A \in R^{n\times n}$ is said to be **alternating** if it is antisymmetric (i.e., satisfies $A^T = -A$) and its diagonal entries all equal 0. For each $n \in \mathbb{N}$, we let $R^{n\times n}_{\text{alt}}$ denote the set of all alternating $n \times n$-matrices in $R^{n\times n}$.

(a) Prove that $R^{n\times n}_{\text{alt}}$ is a left R-submodule of $R^{n\times n}$ for each $n \in \mathbb{N}$.

(b) Prove that this R-module $R^{n\times n}_{\text{alt}}$ is always free, and find a basis of this R-module. (This shows that $R^{n\times n}_{\text{alt}}$ is a "better-behaved" variant of the R-module $R^{n\times n}_{\text{asym}}$ from Exercise 3.7.5.)

(c) What (fairly simple) condition must R satisfy in order for this R-module $R^{n\times n}_{\text{alt}}$ to be identical to the R-module $R^{n\times n}_{\text{asym}}$ from Exercise 3.7.5?

Remark 3.7.7. Let $n \in \mathbb{N}$. A nontrivial theorem says that every $\mathbb{Z}$-submodule of $\mathbb{Z}^n$ is free, i.e., has a basis, and is isomorphic to $\mathbb{Z}^m$ for some $m \in \{0, 1, \ldots, n\}$. For a proof, see (e.g.) [Knapp16, Theorem 8.25] (which proves more and in greater generality). Note that the proof is non-constructive, and there is no general method for finding a basis (or even the rank) of a given $\mathbb{Z}$-submodule of $\mathbb{Z}^n$.

More generally, if R is a PID, then any R-submodule of R^n is free and isomorphic to R^m for some $m \in \{0, 1, \ldots, n\}$. This does not generalize to arbitrary rings, though. For example, if R is the polynomial ring $\mathbb{Z}[x]$, then R^1 has an R-submodule consisting of the polynomials with an even constant term. This R-submodule is not free (check this!).

Let us now return to the general case to state a few theorems:

Theorem 3.7.8. Let M be a left R-module. Let $n \in \mathbb{N}$. The left R-module M is free of rank n if and only if $M \cong R^n$ (as left R-modules).

More concretely:

Theorem 3.7.9. Let M be a left R-module. Let $m_1, m_2, \ldots, m_n$ be n vectors in M. Consider the map

$$f : R^n \to M,$$
$$(r_1, r_2, \ldots, r_n) \mapsto r_1 m_1 + r_2 m_2 + \cdots + r_n m_n.$$

Then:

(a) This map f is always a left R-module morphism.

(b) The map f is injective if and only if $m_1, m_2, \ldots, m_n$ are linearly independent.

(c) The map f is surjective if and only if $m_1, m_2, \ldots, m_n$ span M.

(d) The map f is an isomorphism[118] if and only if $(m_1, m_2, \ldots, m_n)$ is a basis of M.

Note that the map f in Theorem 3.7.9 takes an n-tuple $(r_1, r_2, \ldots, r_n)$ of scalars, and uses these scalars as coefficients to form a linear combination of $m_1, m_2, \ldots, m_n$. Thus, the values of f are precisely the linear combinations of $m_1, m_2, \ldots, m_n$.

Proof of Theorem 3.7.9. This is commonly done in linear algebra texts (albeit usually under the assumption that R is a field, but the proof is the same); thus I will be brief.

(a) We must prove that f respects addition, respects scaling and respects the zero. I will only show that it respects addition, since the other two statements are analogous.

So we must prove that $f(a+b) = f(a) + f(b)$ for all $a, b \in R^n$. Indeed, let $a, b \in R^n$. Write a and b as

$$a = (a_1, a_2, \ldots, a_n) \qquad \text{and} \qquad b = (b_1, b_2, \ldots, b_n).$$

Then, the definition of R^n (as the direct product $\underbrace{R \times R \times \cdots \times R}_{n \text{ times}}$) yields $a + b = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$. Hence, the definition of f yields

$$\begin{aligned} f(a+b) &= (a_1+b_1)\, m_1 + (a_2+b_2)\, m_2 + \cdots + (a_n+b_n)\, m_n \\ &= (a_1 m_1 + b_1 m_1) + (a_2 m_2 + b_2 m_2) + \cdots + (a_n m_n + b_n m_n) \\ &\qquad \text{(by right distributivity)} \\ &= \underbrace{(a_1 m_1 + a_2 m_2 + \cdots + a_n m_n)}_{\substack{= f(a) \\ \text{(by the definition of } f\text{, since } a=(a_1,a_2,\ldots,a_n))}} + \underbrace{(b_1 m_1 + b_2 m_2 + \cdots + b_n m_n)}_{\substack{= f(b) \\ \text{(by the definition of } f\text{, since } b=(b_1,b_2,\ldots,b_n))}} \\ &= f(a) + f(b), \end{aligned}$$

which is what we wanted to show.

[118] Of course, "isomorphism" means "left R-module isomorphism" here.

(b) The map f is an R-module morphism (by part **(a)**). Thus, it is injective if and only if $\operatorname{Ker} f = \{0_{R^n}\}$ (by Lemma 3.5.10). Hence, we have the following chain of logical equivalences:

$$
\begin{aligned}
&(f \text{ is injective}) \\
&\iff (\operatorname{Ker} f = \{0_{R^n}\}) \\
&\iff (\operatorname{Ker} f \subseteq \{0_{R^n}\}) \qquad (\text{since } \{0_{R^n}\} \text{ is clearly a subset of } \operatorname{Ker} f) \\
&\iff (\{a \in R^n \mid f(a) = 0\} \subseteq \{0_{R^n}\}) \\
&\qquad\qquad (\text{since } \operatorname{Ker} f = \{a \in R^n \mid f(a) = 0\} \text{ by the definition of } \operatorname{Ker} f) \\
&\iff (\text{the only } a \in R^n \text{ satisfying } f(a) = 0 \text{ is } 0_{R^n}) \\
&\iff \left(\begin{array}{c} \text{the only } (a_1, a_2, \ldots, a_n) \in R^n \text{ satisfying } f(a_1, a_2, \ldots, a_n) = 0 \\ \text{is } (0, 0, \ldots, 0) \end{array} \right) \\
&\qquad\qquad \left(\begin{array}{c} \text{since any } a \in R^n \text{ can be written in the form } (a_1, a_2, \ldots, a_n), \\ \text{and since } 0_{R^n} = (0, 0, \ldots, 0) \end{array} \right) \\
&\iff \left(\begin{array}{c} \text{the only } (a_1, a_2, \ldots, a_n) \in R^n \text{ satisfying } a_1 m_1 + a_2 m_2 + \cdots + a_n m_n = 0 \\ \text{is } (0, 0, \ldots, 0) \end{array} \right) \\
&\qquad\qquad \left(\begin{array}{c} \text{since } f(a_1, a_2, \ldots, a_n) = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n \\ \text{for any } (a_1, a_2, \ldots, a_n) \in R^n \end{array} \right) \\
&\iff \left(\begin{array}{c} \text{if } a_1, a_2, \ldots, a_n \in R \text{ satisfy } a_1 m_1 + a_2 m_2 + \cdots + a_n m_n = 0, \\ \text{then } a_1 = a_2 = \cdots = a_n = 0 \end{array} \right) \\
&\iff (m_1, m_2, \ldots, m_n \text{ are linearly independent})
\end{aligned}
$$

(by the definition of linear independence). This proves part **(b)** of the theorem.

(c) We have the following chain of logical equivalences:

$$
\begin{aligned}
&(f \text{ is surjective}) \\
&\iff (\text{each } m \in M \text{ can be written as } f(a) \text{ for some } a \in R^n) \\
&\iff \left(\begin{array}{c} \text{each } m \in M \text{ can be written as } f(a_1, a_2, \ldots, a_n) \\ \text{for some } (a_1, a_2, \ldots, a_n) \in R^n \end{array} \right) \\
&\qquad\qquad (\text{since any } a \in R^n \text{ can be written in the form } (a_1, a_2, \ldots, a_n)) \\
&\iff \left(\begin{array}{c} \text{each } m \in M \text{ can be written as } a_1 m_1 + a_2 m_2 + \cdots + a_n m_n \\ \text{for some } (a_1, a_2, \ldots, a_n) \in R^n \end{array} \right) \\
&\qquad\qquad \left(\begin{array}{c} \text{since } f(a_1, a_2, \ldots, a_n) = a_1 m_1 + a_2 m_2 + \cdots + a_n m_n \\ \text{for any } (a_1, a_2, \ldots, a_n) \in R^n \end{array} \right) \\
&\iff (\text{each } m \in M \text{ is a linear combination of } m_1, m_2, \ldots, m_n) \\
&\qquad\qquad (\text{by the definition of a linear combination}) \\
&\iff (m_1, m_2, \ldots, m_n \text{ span } M).
\end{aligned}
$$

This proves part **(c)** of the theorem.

(d) We have the following chain of logical equivalences:

$$
\begin{aligned}
&(f \text{ is an } R\text{-module isomorphism}) \\
&\iff (f \text{ is invertible}) \\
&\qquad\qquad \left(\begin{array}{c} \text{since we know from Proposition 3.5.3 that any} \\ \text{invertible } R\text{-module morphism is an isomorphism} \end{array} \right) \\
&\iff (f \text{ is bijective}) \\
&\iff \underbrace{(f \text{ is injective})}_{\substack{\iff (m_1,m_2,\ldots,m_n \text{ are linearly independent}) \\ \text{(by part \textbf{(b)})}}} \wedge \underbrace{(f \text{ is surjective})}_{\substack{\iff (m_1,m_2,\ldots,m_n \text{ span } M) \\ \text{(by part \textbf{(c)})}}} \\
&\iff (m_1, m_2, \ldots, m_n \text{ are linearly independent}) \wedge (m_1, m_2, \ldots, m_n \text{ span } M) \\
&\iff ((m_1, m_2, \ldots, m_n) \text{ is a basis of } M)
\end{aligned}
$$

(by the definition of a basis). This proves part **(d)** of the theorem. □

Proof of Theorem 3.7.8. $\Longrightarrow$: Assume that M is free of rank n. That is, M has a basis $(m_1, m_2, \ldots, m_n)$ of size n. Consider this basis. Consider the map $f : R^n \to M$ defined in Theorem 3.7.9. Thus, Theorem 3.7.9 **(d)** yields that f is an isomorphism. Hence, $R^n \cong M$ as left R-modules. In other words, $M \cong R^n$ as left R-modules. This proves the "$\Longrightarrow$" direction of Theorem 3.7.8.

$\Longleftarrow$: Assume that $M \cong R^n$ as left R-modules. But the left R-module R^n is free of rank n (as we have seen above). Hence, I claim that the left R-module M is also free of rank n, since $M \cong R^n$. Indeed, this follows from the "isomorphism principle" for modules – i.e., from the "meta-theorem" that says that module isomorphisms preserve all "intrinsic" properties of modules (in this case, this property is "being free of rank n").

Here is a more pedestrian way to get to the same conclusion: We have $M \cong R^n$, thus $R^n \cong M$. In other words, there exists a left R-module isomorphism $g : R^n \to M$. Consider this g. Now, consider the standard basis $(e_1, e_2, \ldots, e_n)$ of the left R-module R^n. Applying g to each vector in this basis, we obtain a list $(g(e_1), g(e_2), \ldots, g(e_n))$ of vectors in M. It is straightforward to see that this new list is a basis of M (indeed, when we apply g to a linear combination $a_1e_1 + a_2e_2 + \cdots + a_ne_n$ of the standard basis $(e_1, e_2, \ldots, e_n)$ in R^n, then we obtain

$$
\begin{aligned}
g(a_1e_1 + a_2e_2 + \cdots + a_ne_n) = a_1g(e_1) + a_2g(e_2) + \cdots + a_ng(e_n) \\
(\text{since } g \text{ is } R\text{-linear}),
\end{aligned}
$$

which is the corresponding linear combination of $(g(e_1), g(e_2), \ldots, g(e_n))$; thus, linear independence of $(e_1, e_2, \ldots, e_n)$ translates into linear independence of $(g(e_1), g(e_2), \ldots, g(e_n))$ (since g sends only 0 to 0), and the same holds for spanning (since g is bijective)). Hence, M has a basis of size n. In other words, M is free of rank n.

Either way, the "$\Longleftarrow$" direction of Theorem 3.7.8 is now proved. □

Theorem 3.7.9 can be generalized to bases of arbitrary size:

Theorem 3.7.10. Let M be a left R-module. Let $(m_i)_{i\in I}$ be any family of vectors in M. Consider the map[119]

$$f : R^{(I)} \to M,$$
$$(r_i)_{i\in I} \mapsto \sum_{i\in I} r_i m_i.$$

(This is well-defined, since any $(r_i)_{i\in I} \in R^{(I)}$ automatically satisfies the condition (55) because of the definition of $R^{(I)}$.)

Then:

(a) This map f is always a left R-module morphism.

(b) The map f is injective if and only if the family $(m_i)_{i\in I}$ is linearly independent.

(c) The map f is surjective if and only if the family $(m_i)_{i\in I}$ spans M.

(d) The map f is an isomorphism if and only if the family $(m_i)_{i\in I}$ is a basis of M.

Note that the map f here has domain $R^{(I)}$, not R^I, since the infinite sum $\sum_{i\in I} r_i m_i$ is well-defined for all $(r_i)_{i\in I} \in R^{(I)}$ but not (in general) for all $(r_i)_{i\in I} \in R^I$.

The map f in Theorem 3.7.10 takes a family $(r_i)_{i\in I}$ of scalars, and uses it to build a linear combination of $(m_i)_{i\in I}$.

Proof of Theorem 3.7.10. Analogous to Theorem 3.7.9, with the usual caveats about infinite sums. □

Remark 3.7.11. As you will have noticed by now, "free module of rank n" is a generalization of "vector space of dimension n" to arbitrary rings.

We have been careful to speak of "free modules of rank n", but never of "the rank of a free module". This is due to the somewhat perverse-sounding fact that there can be modules that are free of several ranks simultaneously (i.e., modules that have bases of different sizes). One way to get such modules is by taking R to be a trivial ring (in which case, any R-module is trivial and is free of every rank simultaneously – seriously). If this was the only example, one could discount the issue as a formality, but there are less trivial (pardon) examples as well: [DumFoo04, §10.3, exercise 27] constructs a ring

[119] Recall that $R^{(I)}$ denotes the direct sum $\bigoplus_{i\in I} R$ here. This is the left R-module that consists of all families $(r_i)_{i\in I} \in R^I$ such that only finitely many $i \in I$ satisfy $r_i \neq 0$.

R over which $R^n \cong R$ as left R-modules for each $n \in \{1,2,3,\ldots\}$ (so R itself is a free R-module of rank n for each $n \in \{1,2,3,\ldots\}$).

If R is a nontrivial commutative ring, then things are nice: The R-modules $R^0, R^1, R^2, \ldots$ are mutually non-isomorphic, so a free R-module can never have two different ranks at the same time. This is not obvious (see [DumFoo04, §10.3, exercise 2]). We can actually say more: If R is a nontrivial commutative ring, then an R-module morphism $R^m \to R^n$ cannot be injective unless $m \leq n$ (see, e.g., `https://math.stackexchange.com/questions/106786` or [Richma88, Theorem 2]), and cannot be surjective unless $m \geq n$ (see, e.g., `https://math.stackexchange.com/questions/20178` or [Richma88, Theorem 1]). These facts are in line with the intuition you should have from linear algebra (injective maps cannot quash dimensions; surjective maps cannot create dimensions) and also with the Pigeonhole Principles from combinatorics (a map between two finite sets M and N cannot be injective unless $|M| \leq |N|$, and cannot be surjective unless $|M| \geq |N|$). But actually proving them takes real work!

3.8. The universal property of a free module ([DumFoo04, §10.3])

As before, we fix a ring R.

The next proposition shows that linear maps respect linear combinations (in the sense that if you apply a linear map to a linear combination of some vectors, then you get the same linear combination of their images):

Proposition 3.8.1. Let M and P be two left R-modules. Let $f : M \to P$ be an R-linear map. Let $(m_i)_{i \in I}$ be any family of vectors in M, and let $(r_i)_{i \in I}$ be a family of scalars in R with the property that

$$\text{all but finitely many } i \in I \text{ satisfy } r_i = 0. \tag{61}$$

Then,

$$f\left(\sum_{i \in I} r_i m_i\right) = \sum_{i \in I} r_i f\left(m_i\right).$$

Proof of Proposition 3.8.1. We give a proof by example: We assume that $I = \{1,2,3\}$. Thus, the claim we need to prove is saying that

$$f\left(r_1 m_1 + r_2 m_2 + r_3 m_3\right) = r_1 f\left(m_1\right) + r_2 f\left(m_2\right) + r_3 f\left(m_3\right).$$

But this is a consequence of the linearity of f (applied several times):

$$\begin{aligned}
&f\left(r_1m_1+r_2m_2+r_3m_3\right)\\
&=f\left(r_1m_1+r_2m_2\right)+f\left(r_3m_3\right) && \text{(since } f \text{ respects addition)}\\
&=f\left(r_1m_1\right)+f\left(r_2m_2\right)+f\left(r_3m_3\right) && \text{(since } f \text{ respects addition)}\\
&=r_1f\left(m_1\right)+r_2f\left(m_2\right)+r_3f\left(m_3\right) && \text{(since } f \text{ respects scaling)}.
\end{aligned}$$

The same reasoning applies to an arbitrary finite set I. (To be fully rigorous, this is a proof by induction on $|I|$.)

The case when I is infinite can be reduced to the case when I is finite using the assumption (61). Indeed, because of (61), there is a finite subset J of I such that all $i \in I \setminus J$ satisfy $r_i = 0$. Choosing such a J, we then have

$$\sum_{i\in I} r_i m_i = \sum_{i\in J} r_i m_i \qquad \text{and} \qquad \sum_{i\in I} r_i f\left(m_i\right) = \sum_{i\in J} r_i f\left(m_i\right), \tag{62}$$

since vanishing addends in a sum can be discarded. But since we have already proved Proposition 3.8.1 in the case of a finite set I, we can apply Proposition 3.8.1 to J, and thus obtain $f\left(\sum_{i\in J} r_i m_i\right) = \sum_{i\in J} r_i f\left(m_i\right)$. In view of (62), this rewrites as $f\left(\sum_{i\in I} r_i m_i\right) = \sum_{i\in I} r_i f\left(m_i\right)$, so we are done. □

One useful feature of bases is that they make it easy to define linear maps out of a free module: Namely, if M is a module with a basis $\left(m_i\right)_{i\in I}$, and you want to define a linear map f out of M, then it suffices to specify the values $f\left(m_i\right)$ of the map on each vector of the basis. These values can be specified arbitrarily; each possible specification yields a unique linear map f. Here is the theorem that underlies this strategy:

Theorem 3.8.2 (Universal property of free modules)**.** Let M be a free left R-module with basis $\left(m_i\right)_{i\in I}$. Let P be a further left R-module (not necessarily free). Let $p_i \in P$ be a vector for each $i \in I$. Then, there exists a **unique** R-linear map $f : M \to P$ such that

$$\text{each } i \in I \text{ satisfies } f\left(m_i\right) = p_i. \tag{63}$$

Proof. **Uniqueness:** If $f : M \to P$ is an R-linear map satisfying (63), then any R-linear combination $\sum_{i\in I} a_i m_i$ of $\left(m_i\right)_{i\in I}$ (where $a_i \in R$ and where all but finitely many $i \in I$ satisfy $a_i = 0$) satisfies

$$\begin{aligned}
f\left(\sum_{i\in I} a_i m_i\right) &= \sum_{i\in I} a_i \underbrace{f\left(m_i\right)}_{\substack{=p_i \\ \text{(by (63))}}} && \text{(by Proposition 3.8.1)}\\
&= \sum_{i\in I} a_i p_i.
\end{aligned} \tag{64}$$

This equality uniquely determines the value of f on each R-linear combination of $(m_i)_{i\in I}$. But each element of M can be written as an R-linear combination of $(m_i)_{i\in I}$ (since $(m_i)_{i\in I}$ is a basis of M and thus spans M). Thus, the equality (64) uniquely determines the value of f on each element of M. In other words, it uniquely determines f. Hence, the R-linear map f satisfying (63) is unique.

Existence: Consider the map

$$\begin{aligned} g : R^{(I)} &\to M, \\ (r_i)_{i\in I} &\mapsto \sum_{i\in I} r_i m_i. \end{aligned}$$

This is the map we called f in Theorem 3.7.10 (of course, we cannot call it f right now, since we need the letter for something else). Theorem 3.7.10 **(d)** yields that the map g is an isomorphism (since the family $(m_i)_{i\in I}$ is a basis of M). In particular, this means that g is bijective. Hence, any element of M can be written as an R-linear combination $\sum_{i\in I} r_i m_i$ of $(m_i)_{i\in I}$ for a **unique** family $(r_i)_{i\in I} \in R^{(I)}$.

Thanks to this, we can define a map

$$\begin{aligned} f : M &\to P, \\ \sum_{i\in I} r_i m_i &\mapsto \sum_{i\in I} r_i p_i \qquad \left(\text{for } (r_i)_{i\in I} \in R^{(I)}\right). \end{aligned}$$

Now, it is easy to see that this map f is R-linear and satisfies (63). Hence, the R-linear map f satisfying (63) exists.

Having proved both existence and uniqueness, we are now done proving Theorem 3.8.2. □

In the proof of the "Uniqueness" part above, we have not used the assumption that the family $(m_i)_{i\in I}$ is a basis of M; we have only used that it spans M. Thus, the uniqueness of f holds even under this weaker condition. Let us isolate this into a separate theorem:

Theorem 3.8.3 (Linear maps are determined on a spanning set)**.** Let M be a left R-module. Let $(m_i)_{i\in I}$ be a family of vectors in M that spans M. Let P be a further left R-module. Let $f, g : M \to P$ be two R-linear maps such that

$$\text{each } i \in I \text{ satisfies } f(m_i) = g(m_i).$$

Then, $f = g$.

This theorem is often used to prove that two linear maps are equal.

3.9. Bilinear maps

When R is a commutative ring, the addition map

$$\text{add} : R \times R \to R, \qquad (a,b) \mapsto a+b$$

is R-linear (where the domain is the direct product of two copies of the left R-module R). In fact, if $(a,b) \in R \times R$ and $(c,d) \in R \times R$ are any two pairs, then

$$\text{add}\left(\underbrace{(a,b)+(c,d)}_{=(a+c,b+d)}\right) = \text{add}\left((a+c,b+d)\right) = (a+c)+(b+d) \qquad \text{and}$$
$$\text{add}\left((a,b)\right) + \text{add}\left((c,d)\right) = (a+b)+(c+d) = (a+c)+(b+d)$$

are clearly the same thing. (This just shows that add respects addition; but the other axioms are just as easy.)

In contrast, the multiplication map

$$\text{mul} : R \times R \to R, \qquad (a,b) \mapsto ab$$

is **not** R-linear. However, it is linear in the first argument if we fix the second. In other words, for any given $b \in R$, the map

$$R \to R, \qquad a \mapsto ab$$

is R-linear. Likewise, the multiplication map $\text{mul} : R \times R \to R$ is linear in the second argument if we fix the first. Such maps have a name:

Definition 3.9.1. Let R be a commutative ring. Let M, N and P be three R-modules. A map $f : M \times N \to P$ is said to be **R-bilinear** (or just **bilinear**) if it satisfies the following two conditions:

- For any $n \in N$, the map
$$\begin{aligned} M &\to P, \\ m &\mapsto f(m,n) \end{aligned}$$
is R-linear. That is, for any $n \in N$, we have
$$\begin{aligned} f(m_1+m_2,n) &= f(m_1,n)+f(m_2,n) \qquad &&\text{for all } m_1,m_2 \in M; \\ f(rm,n) &= rf(m,n) \qquad &&\text{for all } r \in R,\ m \in M; \\ f(0,n) &= 0. \end{aligned}$$
This is called **linearity in the first argument**.

- For any $m \in M$, the map

$$\begin{aligned} N &\to P, \\ n &\mapsto f(m,n) \end{aligned}$$

is R-linear. That is, for any $m \in M$, we have

$$\begin{aligned} f(m, n_1+n_2) &= f(m,n_1) + f(m,n_2) && \text{for all } n_1, n_2 \in N; \\ f(m, rn) &= rf(m,n) && \text{for all } r \in R \text{ and } n \in N; \\ f(m,0) &= 0. \end{aligned}$$

This is called **linearity in the second argument**.

Here are some examples of bilinear maps:[120]

- As I said, the multiplication map $R \times R \to R$, $(a,b) \mapsto ab$ is R-bilinear.
- For any $n \in \mathbb{N}$, the map

$$\begin{aligned} R^n \times R^n &\to R, \\ ((a_1, a_2, \ldots, a_n),\ (b_1, b_2, \ldots, b_n)) &\mapsto a_1b_1 + a_2b_2 + \cdots + a_nb_n \end{aligned}$$

is R-bilinear. This map is known as the **standard scalar product** (also known as the **dot product**) on R^n.

- Consider the field $\mathbb{C}$ of complex numbers. For any $n \in \mathbb{N}$, the **standard inner product**

$$\begin{aligned} \mathbb{C}^n \times \mathbb{C}^n &\to \mathbb{C}, \\ ((a_1, a_2, \ldots, a_n),\ (b_1, b_2, \ldots, b_n)) &\mapsto a_1\overline{b_1} + a_2\overline{b_2} + \cdots + a_n\overline{b_n} \end{aligned}$$

(where $\overline{z}$ denotes the complex conjugate of a $z \in \mathbb{C}$) is $\mathbb{R}$-bilinear but not $\mathbb{C}$-bilinear (since it is antilinear rather than linear in the second argument). However, it becomes $\mathbb{C}$-bilinear if you view it as a map $\mathbb{C}^n \times \overline{\mathbb{C}}^n \to \mathbb{C}$ (with $\overline{\mathbb{C}}$ being the "twisted" $\mathbb{C}$-module $\mathbb{C}$ from Subsection 3.5.3).

- The determinant map

$$\begin{aligned} \det : R^2 \times R^2 &\to R, \\ ((a,b),\ (c,d)) &\mapsto ad - bc \end{aligned}$$

is R-bilinear. (This is called the determinant map because it sends a 2×2-matrix – encoded as pair of pairs – to its determinant.)

[120] In all these examples, R is assumed to be a commutative ring.

- Matrix multiplication is bilinear. That is: For any $m, n, p \in \mathbb{N}$, the map
$$\begin{aligned} R^{m\times n} \times R^{n\times p} &\to R^{m\times p}, \\ (A, B) &\mapsto AB \end{aligned}$$
is R-bilinear.

- The **cross product** map
$$\begin{aligned} R^3 \times R^3 &\to R^3, \\ ((a,b,c),\ (x,y,z)) &\mapsto (bz-cy,\ cx-az,\ ay-bx) \end{aligned}$$
is R-bilinear.

- For any R-module M, the action map
$$\begin{aligned} R \times M &\to M, \\ (r, m) &\mapsto rm \end{aligned}$$
is R-bilinear. In fact, it is linear in its first argument since every $m \in M$ satisfies
$$\begin{aligned} (r_1 + r_2)\, m &= r_1 m + r_2 m && \text{for all } r_1, r_2 \in R; \\ (rs)\, m &= r\,(sm) && \text{for all } r, s \in R; \\ 0_R \cdot m &= 0_M; \end{aligned}$$
and it is linear in its second argument since every $r \in R$ satisfies
$$\begin{aligned} r\,(m_1 + m_2) &= rm_1 + rm_2 && \text{for all } m_1, m_2 \in M; \\ r\,(sm) &= s\,(rm) && \text{for all } s \in R \text{ and } m \in M; \\ r \cdot 0_M &= 0_M. \end{aligned}$$
(Here, the equality $r\,(sm) = s\,(rm)$ follows from $r\,(sm) = \underbrace{(rs)}_{=sr} m = (sr)\, m = s\,(rm)$. Note how we relied on the commutativity of R here!)

We have always been assuming that R is commutative in this section. Non-commutative rings R would be a distraction at this point, but might appear later on.

Theorem 3.8.2 gave us a way to construct linear maps out of a free module by specifying their values on a basis. We can do the same for bilinear maps:

Theorem 3.9.2 (Universal property of free modules wrt bilinear maps)**.** Let R be a commutative ring. Let M be a free R-module with basis $(m_i)_{i\in I}$. Let N be a free R-module with basis $(n_j)_{j\in J}$. Let P be a further R-module (not necessarily free). Let $p_{i,j} \in P$ be a vector for each pair $(i,j) \in I \times J$. Then, there exists a **unique** R-bilinear map $f : M \times N \to P$ such that
$$\text{each } (i,j) \in I \times J \text{ satisfies } f\left(m_i, n_j\right) = p_{i,j}. \tag{65}$$

Proof. This is similar to the proof of Theorem 3.8.2. Here are the details:

Uniqueness: If $f : M \times N \to P$ is an R-bilinear map satisfying (65), then any R-linear combination $\sum_{i \in I} a_i m_i$ of $(m_i)_{i \in I}$ (where $a_i \in R$ and where all but finitely many $i \in I$ satisfy $a_i = 0$) and any R-linear combination $\sum_{j \in J} b_j n_j$ of $\left(n_j\right)_{j \in J}$ (where $b_j \in R$ and where all but finitely many $j \in J$ satisfy $b_j = 0$) satisfy

$$
\begin{aligned}
& f\left(\sum_{i \in I} a_i m_i, \ \sum_{j \in J} b_j n_j\right) \\
&= \sum_{i \in I} a_i \ \underbrace{f\left(m_i, \ \sum_{j \in J} b_j n_j\right)}_{\substack{= \sum_{j \in J} b_j f\left(m_i, n_j\right) \\ \text{(by Proposition 3.8.1,} \\ \text{since } f \text{ is } R\text{-linear} \\ \text{in its second argument)}}} \qquad \left(\begin{array}{c} \text{by Proposition 3.8.1,} \\ \text{since } f \text{ is } R\text{-linear} \\ \text{in its first argument} \end{array}\right) \\
&= \sum_{i \in I} a_i \sum_{j \in J} b_j \underbrace{f\left(m_i, n_j\right)}_{\substack{= p_{i,j} \\ \text{(by (65))}}} \qquad \text{(by Proposition 3.8.1)} \\
&= \sum_{i \in I} a_i \sum_{j \in J} b_j p_{i,j} = \sum_{(i,j) \in I \times J} a_i b_j p_{i,j}. \qquad (66)
\end{aligned}
$$

This equality uniquely determines the value of f on each pair (x, y), where x is an R-linear combination of $(m_i)_{i \in I}$ and y is an R-linear combination of $\left(n_j\right)_{j \in J}$.

But each element of M can be written as an R-linear combination of $(m_i)_{i \in I}$ (since $(m_i)_{i \in I}$ is a basis of M and thus spans M), and every element of N can be written as an R-linear combination of $\left(n_j\right)_{j \in J}$ (for similar reasons). Thus, the equality (66) uniquely determines the value of f on each pair $(x, y) \in M \times N$. In other words, it uniquely determines f. Hence, the R-bilinear map f satisfying (65) is unique.

Existence: As in the above proof of Theorem 3.8.2, we can see that any element of M can be written as an R-linear combination $\sum_{i \in I} r_i m_i$ of $(m_i)_{i \in I}$ for a **unique** family $(r_i)_{i \in I} \in R^{(I)}$. Likewise, any element of N can be written as an R-linear combination $\sum_{j \in J} s_j n_j$ of $\left(n_j\right)_{j \in J}$ for a **unique** family $\left(s_j\right)_{j \in J} \in R^{(J)}$. Hence, each pair $(x, y) \in M \times N$ can be written in the form $\left(\sum_{i \in I} r_i m_i, \ \sum_{j \in J} s_j n_j\right)$ for a **unique** pair of families $(r_i)_{i \in I} \in R^{(I)}$ and $\left(s_j\right)_{j \in J} \in R^{(J)}$.

Thanks to this, we can define a map

$$f : M \times N \to P,$$
$$\left(\sum_{i\in I} r_i m_i,\ \sum_{j\in J} s_j n_j\right) \mapsto \sum_{(i,j)\in I\times J} r_i s_j p_{i,j} \qquad \left(\text{for } (r_i)_{i\in I} \in R^{(I)} \text{ and } (s_j)_{j\in J} \in R^{(J)}\right).$$

Now, it is easy to see that this map f is R-bilinear and satisfies (65). Hence, the R-bilinear map f satisfying (65) exists.

Having proved both existence and uniqueness, we are now done proving Theorem 3.9.2. □

3.10. Multilinear maps

Linear and bilinear maps are the first two links in a chain of notions. Here is the general case:

Definition 3.10.1. Let R be a commutative ring. Let $M_1, M_2, \ldots, M_n$ be finitely many R-modules. Let P be any R-module. A map $f : M_1 \times M_2 \times \cdots \times M_n \to P$ is said to be **R-multilinear** (or just **multilinear**) if it satisfies the following condition:

- For any $i \in \{1, 2, \ldots, n\}$ and any $m_1, m_2, \ldots, m_{i-1}, m_{i+1}, m_{i+2}, \ldots, m_n$ in the respective modules (meaning that $m_k \in M_k$ for each $k \neq i$), the map
$$M_i \to P,$$
$$m_i \mapsto f(m_1, m_2, \ldots, m_n)$$
is R-linear. That is, if we fix all arguments of f other than the i-th argument, then f is R-linear as a function of the i-th argument. This is called **linearity in the i-th argument**.

Thus, "bilinear" is just "multilinear for $n = 2$", whereas "linear" is "multilinear for $n = 1$".

Here are some examples of multilinear maps:

- One of the simplest examples of an R-multilinear map is the map
$$\operatorname{prod}_n : \underbrace{R \times R \times \cdots \times R}_{n \text{ times}} \to R,$$
$$(a_1, a_2, \ldots, a_n) \mapsto a_1 a_2 \cdots a_n.$$
More generally, for any $r \in R$, the map
$$\underbrace{R \times R \times \cdots \times R}_{n \text{ times}} \to R,$$
$$(a_1, a_2, \ldots, a_n) \mapsto r a_1 a_2 \cdots a_n$$

is R-multilinear.

- The most famous example of an R-multilinear map is the determinant function

$$\det : \underbrace{R^n \times R^n \times \cdots \times R^n}_{n \text{ times}} \to R,$$
$$(v_1, v_2, \ldots, v_n) \mapsto \det(v_1, v_2, \ldots, v_n),$$

where $\det(v_1, v_2, \ldots, v_n)$ means the determinant of the $n \times n$-matrix whose columns are $v_1, v_2, \ldots, v_n$. (See, e.g., [Knapp16, Chapter II, Section 7], [Ford22, §4.7] or [Leeb20] for a treatment of determinants based on the concept of multilinearity[121].)

There is a universal property of free modules with respect to multilinear maps (extending Theorem 3.8.2 and Theorem 3.9.2), which says that a multilinear map from a product of free R-modules can be defined by specifying its values on all combinations of basis elements (i.e., on all n-tuples whose all entries belong to the respective bases). I leave it to you to state and prove it.

3.11. Algebras over commutative rings ([DumFoo04, §10.1])

Convention 3.11.1. In this section, we fix a **commutative** ring R.

3.11.1. Definition

The notion of an R**-algebra** combines the notions of a ring and of an R-module, as well as connecting them by an extra axiom:

Definition 3.11.2. An R**-algebra** is a set A that is endowed with

- two binary operations (i.e., maps from $A \times A$ to A) that are called **addition** and **multiplication** and denoted by $+$ and $\cdot$,
- a map $\cdot$ from $R \times A$ to A that is called **action** of R on A (and should not be confused with the multiplication map, which is also denoted by $\cdot$), and
- two elements of A that are called **zero** and **unity** and denoted by 0 and 1,

such that the following properties (the "**algebra axioms**") hold:

[121] Note that [Knapp16] is rather terse and abstract, but it covers the subject almost painlessly if one is familiar with the advanced viewpoint he is using. More down-to-earth methods are used in [Ford22, §4.7], and [Leeb20] is even more elementary (covering only the case when R is a field; but the same argument can be used in the general case).

- The addition, the multiplication, the zero and the unity satisfy all the ring axioms (so that A becomes a ring when equipped with them).
- The addition, the action and the zero satisfy all the module axioms (so that A becomes an R-module when equipped with them).
- **Scale-invariance of multiplication:** We have

$$r\left(ab\right) = \left(ra\right)b = a\left(rb\right) \qquad \text{for all } r \in R \text{ and } a, b \in A.$$

  Here (and in the following), we omit the $\cdot$ signs for multiplication and action (so "ab" means "$a \cdot b$", and "$r\left(ab\right)$" means "$r \cdot \left(ab\right)$").

Thus, an R-algebra is an R-module that is also a ring at the same time, with the same addition (i.e., the addition of the R-module must be identical with the addition of the ring) and the same zero, and satisfying the "scale-invariance" axiom. In other words, you get the definition of an R-algebra by throwing the definitions of an R-module and a ring together (without duplicating the addition and the zero) and requiring that the multiplication plays nice with the scaling (in the sense that scaling a product is equivalent to scaling one of its factors). Hence, in order to specify an R-algebra, it is enough to provide a set with both a ring structure and an R-module structure and show that it satisfies the "scale-invariance" axiom.

The "scale-invariance" axiom can be restated as "the multiplication map

$$\begin{aligned} A \times A &\to A, \\ \left(a, b\right) &\mapsto ab \end{aligned}$$

is R-bilinear". More precisely, requiring that the multiplication map $A \times A \to A$ be R-bilinear is tantamount to imposing both the scale-invariance axiom and a few of the ring and module axioms.

3.11.2. Examples

Examples of R-algebras include the following:

- The commutative ring R itself is an R-algebra (with both multiplication and action being the usual multiplication of R).
- The zero ring $\{0\}$ is an R-algebra.
- The matrix ring $R^{n \times n}$ is an R-algebra for any $n \in \mathbb{N}$ (since it is an R-module and a ring, and the "scale-invariance" axiom is easily seen to hold).

- The ring $\mathbb{C}$ is an $\mathbb{R}$-algebra (since it is an $\mathbb{R}$-module and a ring, and the "scale-invariance" axiom is easily seen to hold).
- The ring $\mathbb{R}$ is a $\mathbb{Q}$-algebra (for similar reasons).
- More generally: If a commutative ring R is a subring of a **commutative** ring S, then S becomes an R-algebra in a natural way. In fact, we already know from Subsection 3.3.2 that S becomes an R-module, and it is easy to see that this R-module can be combined with the ring structure on S to form an R-algebra.
- Even more generally: If R and S are two **commutative** rings, and if $f : R \to S$ is a ring morphism, then S becomes an R-algebra in a natural way. In fact, we already know from Subsection 3.3.2 that S becomes an R-module (this is the R-module structure on S induced by f), and it is easy to see that this R-module can be combined with the ring structure on S to form an R-algebra.[122] This R-algebra structure on S is said to be **induced** by the morphism f.
- Yet more generally: If R and S are two commutative rings, and if $f : R \to S$ is a ring morphism, then any S-algebra A becomes an R-algebra in a natural way. In fact, we already know from Subsection 3.3.2 that A becomes an R-module (this is the R-module obtained by restricting the S-module A to R), and it is easy to see that this R-module can be combined with the ring structure on A to form an R-algebra. This is called the R-algebra obtained by **restricting** the S-algebra A to R.

  For example, the matrix ring $\mathbb{C}^{2\times 2}$ is a $\mathbb{C}$-algebra, and thus becomes an $\mathbb{R}$-algebra (since the inclusion map $\mathbb{R} \to \mathbb{C}$ is a ring morphism).
- The quaternion ring $\mathbb{H}$ is an $\mathbb{R}$-algebra. But it is not a $\mathbb{C}$-algebra, even though it contains $\mathbb{C}$ as a subring. Indeed, the "scale-invariance" axiom for $\mathbb{H}$ to be a $\mathbb{C}$-algebra would say that

$$r\,(ab) = (ra)\,b = a\,(rb) \qquad \text{for all } r \in \mathbb{C} \text{ and } a, b \in \mathbb{H};$$

  but this is **not true** for $r = i$, $a = j$ and $b = 1$ because $ij \neq ji$.

  This does not contradict the previous bullet points! After all, $\mathbb{H}$ is not commutative.
- The polynomial ring $R[x]$ (to be defined soon) is an R-algebra.

[122] In particular, this yields that any quotient ring R/I of R becomes an R-algebra, via the canonical projection $\pi : R \to R/I$.

Exercise 3.11.1. Recall that the complex numbers were defined as pairs of real numbers, with entrywise addition and a strange-looking multiplication. Let us now generalize this construction by replacing real numbers by elements of the given commutative ring R.

Thus, we define an **R-complex number** to be a pair $(a, b) \in R \times R$. We define $\mathbb{C}_R$ to be the set of all R-complex numbers. We define an addition $+$ and a multiplication $\cdot$ on this set $\mathbb{C}_R$ by the formulas

$$(a, b) + (c, d) = (a + c,\ b + d) \qquad \text{and}$$
$$(a, b) \cdot (c, d) = (ac - bd,\ ad + bc)$$

(these are the same formulas as for the original complex numbers).

(a) Prove that the set $\mathbb{C}_R$ (equipped with these two operations, with the zero $(0, 0)$ and the unity $(1, 0)$) becomes a commutative ring.

We denote this ring by $\mathbb{C}_R$, and call it the ring of **R-complex numbers**. For $R = \mathbb{R}$, we recover the usual complex numbers: $\mathbb{C}_{\mathbb{R}} = \mathbb{C}$.

We further turn this ring $\mathbb{C}_R$ into an R-algebra by defining an action of R on $\mathbb{C}_R$ by the equation

$$r\,(a, b) = (ra, rb) \qquad \text{for any } r \in R \text{ and any } (a, b) \in \mathbb{C}_R.$$

(b) Prove that this does indeed make $\mathbb{C}_R$ into an R-algebra.

Let i denote the element $(0, 1)$ of $\mathbb{C}_R$. (This is the generalization of the imaginary unit i of $\mathbb{C}$.)

(c) Prove that $(a, b) = a \cdot 1_{\mathbb{C}_R} + bi$ for each $(a, b) \in \mathbb{C}_R$.

Now, recall that $\mathbb{C}$ is a field. What about its generalized version $\mathbb{C}_R$?

(d) Prove that $\mathbb{C}_{\mathbb{C}}$ is not a field, but rather $\mathbb{C}_{\mathbb{C}} \cong \mathbb{C} \times \mathbb{C}$ as rings.

(e) Prove that $\mathbb{C}_{\mathbb{Z}/2}$ is not a field, and in fact is isomorphic to the ring D_4 from Subsection 2.1.2.

(f) Prove that $\mathbb{C}_{\mathbb{Z}/3}$ is a field with 9 elements.

(g) Let S be the ring $\mathbb{Z}[i]$ of Gaussian integers. Prove that $\mathbb{C}_{\mathbb{Z}/n} \cong S/(nS)$ as rings for any integer n.

We can similarly generalize the dual numbers (as defined in Exercise 2.1.2):

Exercise 3.11.2. We define an **R-dual number** to be a pair $(a, b) \in R \times R$. We define $\mathbb{D}_R$ to be the set of all R-dual numbers. We define an addition $+$ and a multiplication

$\cdot$ on this set $\mathbb{D}_R$ by the formulas

$$(a,b)+(c,d)=(a+c,\ b+d) \qquad \text{and}$$
$$(a,b)\cdot(c,d)=(ac,\ ad+bc)$$

(these are the same formulas as for the original dual numbers).

(a) Prove that the set $\mathbb{D}_R$ (equipped with these two operations, with the zero $(0,0)$ and the unity $(1,0)$) becomes a commutative ring.

We denote this ring by $\mathbb{D}_R$, and call it the ring of **R-dual numbers**. For $R=\mathbb{R}$, we recover the usual dual numbers from Exercise 2.1.2: that is, $\mathbb{D}_{\mathbb{R}}=\mathbb{D}$.

We further turn this ring $\mathbb{D}_R$ into an R-algebra by defining an action of R on $\mathbb{D}_R$ by the equation

$$r\,(a,b)=(ra,rb) \qquad \text{for any } r\in R \text{ and any } (a,b)\in\mathbb{D}_R.$$

(b) Prove that this does indeed make $\mathbb{D}_R$ into an R-algebra.

Let ε denote the element $(0,1)$ of $\mathbb{D}_R$.

(c) Prove that, for any $a,b\in R$, we have $(a,b)=a\cdot 1_{\mathbb{D}_R}+b\varepsilon$ in $\mathbb{D}_R$.

(d) Prove that $\varepsilon\in\mathbb{D}_R$ is nilpotent, and in fact $\varepsilon^2=0$.

(e) Prove that $\mathbb{D}_{\mathbb{Z}/2}$ is isomorphic to the ring D_4 from Subsection 2.1.2.

Exercise 3.11.3. Let R be a ring. Let M be an R-module. Recall that the Hom group $\operatorname{Hom}_R(M,M)$ is an additive abelian group (by Exercise 3.5.2 **(a)**). Moreover, if R is commutative, then $\operatorname{Hom}_R(M,M)$ is also an R-module (by Exercise 3.5.2 **(b)**). Prove the following:

(a) The Hom group $\operatorname{Hom}_R(M,M)$ becomes a ring if we define multiplication to be composition (i.e., for any for any $f\in\operatorname{Hom}_R(M,M)$ and $g\in\operatorname{Hom}_R(M,M)$, we define fg to be the composition $f\circ g$). Its unity is the identity map $\mathrm{id}: M\to M$.

This ring $\operatorname{Hom}_R(M,M)$ is also denoted $\operatorname{End}_R(M)$ and known as the **endomorphism ring**[123] of M.

(b) If R is commutative, then the endomorphism ring $\operatorname{End}_R(M)$ becomes an R-algebra (with the R-module structure defined as in Exercise 3.5.2 **(b)**).

(c) Let $M=R^{\mathbb{N}}$; this is the left R-module of all infinite sequences $(a_0,a_1,a_2,\ldots)$ of elements of R. Define two left R-module morphisms $f: M\to M$ and $g: M\to M$ by

$$f(a_0,a_1,a_2,\ldots)=(a_1,a_2,a_3,\ldots) \qquad \text{for any } (a_0,a_1,a_2,\ldots)\in M$$

and

$$g(a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots) \qquad \text{for any } (a_0, a_1, a_2, \ldots) \in M.$$

Prove that $fg = 1$ but $gf \neq 1$ (unless R is trivial) in the ring $\mathrm{End}_R(M)$. (This gives an example of a left inverse that is not a right inverse.)

3.11.3. Rings as $\mathbb{Z}$-algebras

The most common algebras are the $\mathbb{Z}$-algebras. In fact, every ring is a $\mathbb{Z}$-algebra in a natural way:

Proposition 3.11.3. Let A be any ring. Then, A is an abelian group (with respect to addition), so A becomes a $\mathbb{Z}$-module (since we have seen in Proposition 3.4.1 that every abelian group naturally becomes a $\mathbb{Z}$-module). This $\mathbb{Z}$-module structure can be combined with the ring structure on A, turning A into a $\mathbb{Z}$-algebra.

Proof. You have to check "scale-invariance". This is easy and LTTR. □

Thus, every ring becomes a $\mathbb{Z}$-algebra (similarly to how any abelian group becomes a $\mathbb{Z}$-module). This allows us to equate rings with $\mathbb{Z}$-algebras. We shall do this whenever convenient.

3.11.4. The underlying structures

Every R-algebra A has an underlying ring (i.e., the ring obtained from A by forgetting the action) and an underlying R-module (i.e., the R-module obtained from A by forgetting the multiplication and the unity); we will refer to these simply as the "ring A" and the "R-module A". So, for example, if A and B are two R-algebras, then the "ring morphisms from A to B" will simply mean the ring morphisms from the underlying ring of A to the underlying ring of B. Similarly the "R-module morphisms from A to B" are to be understood.

Warning: There is also a notion of "base ring" which sounds similar to, but has nothing to do with, the notion of an "underlying ring"! The **base ring** of an R-algebra A is defined to be R (unlike the underlying ring of A, which is just A with its action removed).

3.11.5. Commutative R-algebras

[123] An **endomorphism** is defined to be a morphism from a structure (e.g., a ring or a module or an algebra) to itself.

Definition 3.11.4. An R-algebra is said to be **commutative** if its underlying ring is commutative (i.e., if its multiplication is commutative).

3.11.6. Subalgebras

Algebras have subalgebras; they are defined exactly as you would expect:

Definition 3.11.5. Let A be an R-algebra. An **R-subalgebra** of A means a subset of A that is simultaneously a subring and an R-submodule of A.

In pedestrian terms, this means that an R-subalgebra of A is a subset of A that is closed under addition, multiplication and scaling and contains the zero and the unity. Such an R-subalgebra of A clearly becomes an R-algebra in its own right (since we can restrict all relevant operations from A to this subalgebra).

3.11.7. R-algebra morphisms

Just as rings have ring morphisms, and R-modules have R-module morphisms, there is a notion of R-algebra morphisms:

Definition 3.11.6. Let A and B be two R-algebras.

(a) An **R-algebra morphism** (or, short, **algebra morphism**) from A to B means a map $f : A \to B$ that is both a ring morphism and an R-module morphism (i.e., that respects addition, multiplication, zero, unity and scaling).

(b) An **R-algebra isomorphism** (or, informally, **algebra iso**) from A to B means an invertible R-algebra morphism $f : A \to B$ whose inverse $f^{-1} : B \to A$ is also an R-algebra morphism.

(c) The R-algebras A and B are said to be **isomorphic** (this is written $A \cong B$) if there exists an R-algebra isomorphism from A to B.

All the fundamental properties of ring morphisms (stated in Subsection 2.7.2) and of ring isomorphisms (stated in Subsection 2.7.4) have analogues for R-algebra morphisms and isomorphisms, respectively. For example, here is the analogue of Proposition 2.7.6:

Proposition 3.11.7. Let A and B be two R-algebras. Let $f : A \to B$ be an R-algebra morphism. Then, $\operatorname{Im} f = f(A)$ is an R-subalgebra of B.

Proof. Analogous to the proof of Proposition 2.7.6. □

And here is the analogue of Proposition 2.7.7:

Proposition 3.11.8. Let A and B be two R-algebras. Let $f : A \to B$ be an invertible R-algebra morphism. Then, f is an R-algebra isomorphism.

Proof. Analogous to the proof of Proposition 2.7.7. □

An analogue to Proposition 3.5.2 is the following:

Proposition 3.11.9. Let A and B be two $\mathbb{Z}$-algebras. Then, the $\mathbb{Z}$-algebra morphisms from A to B are precisely the ring morphisms from A to B.

Proof. Analogous to the proof of Proposition 3.5.2. □

3.11.8. Direct products of algebras

The direct product of several R-algebras is defined just as you would expect: addition, multiplication and scaling are all entrywise. Just for the sake of completeness, let me give its precise definition:

Proposition 3.11.10. Let I be any set. Let $(A_i)_{i\in I}$ be any family of R-algebras. Then, their Cartesian product $\prod_{i\in I} A_i$ becomes an R-algebra if we endow it with the entrywise addition (i.e., we set $(m_i)_{i\in I} + (n_i)_{i\in I} = (m_i + n_i)_{i\in I}$ for any two families $(m_i)_{i\in I}, (n_i)_{i\in I} \in \prod_{i\in I} A_i$) and the entrywise multiplication (i.e., we set $(m_i)_{i\in I} \cdot (n_i)_{i\in I} = (m_i \cdot n_i)_{i\in I}$ for any two families $(m_i)_{i\in I}, (n_i)_{i\in I} \in \prod_{i\in I} A_i$) and the entrywise scaling (i.e., we set $r\,(m_i)_{i\in I} = (rm_i)_{i\in I}$ for any $r \in R$ and any family $(m_i)_{i\in I} \in \prod_{i\in I} A_i$) and with the zero $(0)_{i\in I}$ and the unity $(1)_{i\in I}$. The underlying ring of this R-algebra $\prod_{i\in I} A_i$ is the direct product of the rings A_i, whereas the underlying R-module of this R-algebra $\prod_{i\in I} A_i$ is the direct product of the R-modules A_i.

Definition 3.11.11. This R-algebra is denoted by $\prod_{i\in I} A_i$ and called the **direct product** of the R-algebras A_i.

The usual notations apply to these direct products: For example, if $I = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$, then the direct product $\prod_{i\in I} A_i$ is also denoted by $A_1 \times A_2 \times \cdots \times A_n$; we further set $A^I = \prod_{i\in I} A$ and $A^n = A^{\{1,2,\ldots,n\}}$ for each $n \in \mathbb{N}$.

3.12. Defining algebras: the case of $\mathbb{H}$

You can think of an R-algebra as a ring equipped with an additional piece of structure – namely, with an action of R on it. Thus, in order to define an R-algebra, it is natural to start by defining a ring and then defining an action of R on it (and showing that it satisfies the R-module axioms and scale-invariance).

Often, however, it is easier to proceed differently: First, define an R-module, and then define the multiplication and the unity to turn it into an R-algebra. If you do things in this order, you can use the R-module structure as scaffolding for defining the multiplication. This often turns out to be the simpler way.

Here is an example of how this can work:

Recall the ring $\mathbb{H}$ of quaternions, which were "defined" to be "numbers" of the form $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{R}$ and with the multiplication rules

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j.$$

It is clear how to calculate in $\mathbb{H}$ using these rules. But why does this ring $\mathbb{H}$ exist?

Here is a cautionary tale to show why this is a question: Let's replace $k^2 = -1$ by $k^2 = 1$ in our above "definition" of $\mathbb{H}$ (but still require i^2 and j^2 to be -1). Then, $j^2 \underbrace{k^2}_{=1} = j^2 = -1$, so that

$$-1 = j^2k^2 = j \underbrace{jk}_{=i} k = j \underbrace{ik}_{\substack{=-j \\ (\text{since } -ik=j)}} = j(-j) = -\underbrace{j^2}_{=-1} = -(-1) = 1.$$

Adding 1 to this equality, we find $0 = 2$, so that $0 = 1$ (upon division by 2). Therefore, the ring is trivial – i.e., all its elements are 0.

Ouch. We tried to expand our number system by introducing new "numbers" i, j, k, but instead we ended up collapsing it (making all numbers equal to 0).

It should not surprise you that this can happen; after all, the same happens if you introduce the "number" $\infty := \dfrac{1}{0}$ and start doing algebra with it. But why doesn't it happen with the quaternions? Why is $\mathbb{H}$ actually an extension of our number system rather than a collapsed version of it?

The simplest way to answer this question is to throw away the wishy-washy definition of $\mathbb{H}$ we gave above (what does "numbers of the form $a + bi + cj + dk$" really mean?), and redefine $\mathbb{H}$ rigorously.

We want $\mathbb{H}$ to be an $\mathbb{R}$-algebra. First, we introduce its underlying $\mathbb{R}$-module (i.e., $\mathbb{R}$-vector space) structure. This underlying $\mathbb{R}$-module will be a 4-dimensional $\mathbb{R}$-vector space, i.e., a free $\mathbb{R}$-module of rank 4. So let me **define** $\mathbb{H}$ to be $\mathbb{R}^4$ as an $\mathbb{R}$-module. Let me denote its standard basis by $(\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k})$ (so that $\mathbf{e} = (1, 0, 0, 0)$ and $\mathbf{i} = (0, 1, 0, 0)$ and $\mathbf{j} = (0, 0, 1, 0)$ and $\mathbf{k} = (0, 0, 0, 1)$). These four basis vectors $\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ will later become the quaternions $1, i, j, k$, but I'm being cautious for now and avoiding any names that might be too suggestive. The basis vector $\mathbf{e}$ will be the unity of $\mathbb{H}$. Next, we define the multiplication of $\mathbb{H}$ to be the

$\mathbb{R}$-bilinear map $\mu : \mathbb{H} \times \mathbb{H} \to \mathbb{H}$ that satisfies[124]

$$\begin{array}{llll} \mu(\mathbf{e},\mathbf{e}) = \mathbf{e}, & \mu(\mathbf{e},\mathbf{i}) = \mathbf{i}, & \mu(\mathbf{e},\mathbf{j}) = \mathbf{j}, & \mu(\mathbf{e},\mathbf{k}) = \mathbf{k}, \\ \mu(\mathbf{i},\mathbf{e}) = \mathbf{i}, & \mu(\mathbf{i},\mathbf{i}) = -\mathbf{e}, & \mu(\mathbf{i},\mathbf{j}) = \mathbf{k}, & \mu(\mathbf{i},\mathbf{k}) = -\mathbf{j}, \\ \mu(\mathbf{j},\mathbf{e}) = \mathbf{j}, & \mu(\mathbf{j},\mathbf{i}) = -\mathbf{k}, & \mu(\mathbf{j},\mathbf{j}) = -\mathbf{e}, & \mu(\mathbf{j},\mathbf{k}) = \mathbf{i}, \\ \mu(\mathbf{k},\mathbf{e}) = \mathbf{k}, & \mu(\mathbf{k},\mathbf{i}) = \mathbf{j}, & \mu(\mathbf{k},\mathbf{j}) = -\mathbf{i}, & \mu(\mathbf{k},\mathbf{k}) = -\mathbf{e}. \end{array}$$

Theorem 3.9.2 guarantees that there is a unique such bilinear map μ. We set $ab = \mu(a,b)$ for all $a, b \in \mathbb{H}$.

Why is this a ring? All but two of the ring axioms are obvious (they follow either from the bilinearity of μ or from the module axioms for the $\mathbb{R}$-module $\mathbb{H} = \mathbb{R}^4$). The two axioms that are not obvious are the following:

1. Associativity of multiplication.
2. Neutrality of 1 (i.e., the claim that $a \cdot \mathbf{e} = \mathbf{e} \cdot a = a$ for each $a \in \mathbb{H}$).

Fortunately, the bilinearity of μ will make both of these axioms straightforward to check. Indeed, let me explain how to check the associativity of multiplication. In other words, let me prove that the map μ is associative – i.e., that

$$\mu(\mu(a,b),c) = \mu(a,\mu(b,c)) \qquad \text{for all } a,b,c \in \mathbb{H}. \tag{67}$$

The trick to this is that when a map like μ is bilinear, its associativity can be checked on a basis – or, more generally, on a spanning set:

Lemma 3.12.1. Let R be a commutative ring. Let M be an R-module. Let $(m_i)_{i \in I}$ be a family of vectors in M that spans M. Let $f : M \times M \to M$ be an R-bilinear map. Assume that

$$f(f(m_i,m_j),m_k) = f(m_i,f(m_j,m_k)) \qquad \text{for all } i,j,k \in I. \tag{68}$$

Then, we have

$$f(f(a,b),c) = f(a,f(b,c)) \qquad \text{for all } a,b,c \in M. \tag{69}$$

Proof of Lemma 3.12.1. Let $a, b, c \in M$. Since the family $(m_i)_{i \in I}$ spans M, we can write the three vectors a, b, c as

$$a = \sum_{i \in I} a_i m_i, \qquad b = \sum_{j \in I} b_j m_j, \qquad c = \sum_{k \in I} c_k m_k$$

[124] These equations are not chosen at random, of course; they are simply the equations

$$i^2 = j^2 = k^2 = -1, \qquad ij = -ji = k, \qquad jk = -kj = i, \qquad ki = -ik = j$$

(as well as the equations $1 \cdot 1 = 1$, $1i = i$, $1j = j$, $1k = k$, $i \cdot 1 = i$, $j \cdot 1 = j$ and $k \cdot 1 = k$), with $1, i, j, k$ renamed as $\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k}$.

for some coefficients $a_i, b_j, c_k \in R$. Consider these coefficients. Then,[125]

$$\begin{aligned}
f\left(f\left(a,b\right),c\right) &= f\left(f\left(\sum_{i\in I} a_i m_i, \sum_{j\in I} b_j m_j\right), \sum_{k\in I} c_k m_k\right) \\
&= \sum_{k\in I} c_k f\left(f\left(\sum_{i\in I} a_i m_i, \sum_{j\in I} b_j m_j\right), m_k\right) \\
&\qquad \left(\text{since } f \text{ is linear in its second argument}\right) \\
&= \sum_{k\in I} c_k f\left(\sum_{i\in I} a_i f\left(m_i, \sum_{j\in I} b_j m_j\right), m_k\right) \\
&\qquad \left(\text{since } f \text{ is linear in its first argument}\right) \\
&= \sum_{k\in I} c_k f\left(\sum_{i\in I} a_i \sum_{j\in I} b_j f\left(m_i, m_j\right), m_k\right) \\
&\qquad \left(\text{since } f \text{ is linear in its second argument}\right) \\
&= \sum_{k\in I} c_k \sum_{i\in I} a_i \sum_{j\in I} b_j f\left(f\left(m_i, m_j\right), m_k\right) \\
&\qquad \left(\text{since } f \text{ is linear in its first argument}\right) \\
&= \sum_{i\in I} \sum_{j\in I} \sum_{k\in I} a_i b_j c_k f\left(f\left(m_i, m_j\right), m_k\right)
\end{aligned}$$

and similarly

$$f\left(a, f\left(b,c\right)\right) = \sum_{i\in I} \sum_{j\in I} \sum_{k\in I} a_i b_j c_k f\left(m_i, f\left(m_j, m_k\right)\right).$$

The right hand sides of these two equalities are equal by our assumption (68). Hence, the left hand sides are equal. In other words, $f\left(f\left(a,b\right),c\right) = f\left(a, f\left(b,c\right)\right)$. This proves Lemma 3.12.1. □

Let us now return to $\mathbb{H}$. We want to prove that

$$\mu\left(\mu\left(a,b\right),c\right) = \mu\left(a,\mu\left(b,c\right)\right) \qquad \text{for all } a,b,c \in \mathbb{H}.$$

By Lemma 3.12.1 (applied to $R = \mathbb{R}$, $M = \mathbb{H}$, $\left(m_i\right)_{i\in I} = \left(\mathbf{e},\mathbf{i},\mathbf{j},\mathbf{k}\right)$ and $f = \mu$), it suffices to show that

$$\mu\left(\mu\left(a,b\right),c\right) = \mu\left(a,\mu\left(b,c\right)\right) \qquad \text{for all } a,b,c \in \left\{\mathbf{e},\mathbf{i},\mathbf{j},\mathbf{k}\right\}.$$

This is a finite computation: There are only 64 triples $\left(a,b,c\right)$ with $a,b,c \in \left\{\mathbf{e},\mathbf{i},\mathbf{j},\mathbf{k}\right\}$, and we can check the equality $\mu\left(\mu\left(a,b\right),c\right) = \mu\left(a,\mu\left(b,c\right)\right)$ for each of these triples directly by computation (using the definition of μ).

[125] We will use Proposition 3.8.1 multiple times in this computation.

A computer could do this in the blink of an eye, but we can also do this by hand. There are some tricks that reduce our work. The first is to notice that $\mu(\mu(a,b),c) = \mu(a,\mu(b,c))$ is obvious when one of a,b,c is $\mathbf{e}$ (because $\mu(\mathbf{x},\mathbf{e}) = \mu(\mathbf{e},\mathbf{x}) = \mathbf{x}$ for each $\mathbf{x} \in \{\mathbf{e},\mathbf{i},\mathbf{j},\mathbf{k}\}$). Thus, it suffices to prove the equality $\mu(\mu(a,b),c) = \mu(a,\mu(b,c))$ in the case when $a,b,c \in \{\mathbf{i},\mathbf{j},\mathbf{k}\}$. This leaves 27 triples (a,b,c) to check.

The next trick is to observe a cyclic symmetry. Indeed, the definition of μ is invariant under cyclic rotation of $\mathbf{i},\mathbf{j},\mathbf{k}$, in the sense that if we replace $\mathbf{i},\mathbf{j},\mathbf{k}$ by $\mathbf{j},\mathbf{k},\mathbf{i}$ (respectively), then the definition remains unchanged (for example, $\mu(\mathbf{j},\mathbf{i}) = -\mathbf{k}$ becomes $\mu(\mathbf{k},\mathbf{j}) = -\mathbf{i}$). Thus, when we are proving $\mu(\mu(a,b),c) = \mu(a,\mu(b,c))$ for all $a,b,c \in \{\mathbf{i},\mathbf{j},\mathbf{k}\}$, we can WLOG assume that $a = \mathbf{i}$ (since otherwise, we can achieve this by rotating all of a,b,c until a becomes $\mathbf{i}$). This leaves 9 triples (a,b,c) to check.

Let me just check one of them: namely, $(a,b,c) = (\mathbf{i},\mathbf{k},\mathbf{k})$. In this case, we have

$$\begin{aligned}\mu(\mu(a,b),c) &= \mu\left(\underbrace{\mu(\mathbf{i},\mathbf{k})}_{=-\mathbf{j}},\mathbf{k}\right) = \mu(-\mathbf{j},\mathbf{k}) = -\underbrace{\mu(\mathbf{j},\mathbf{k})}_{=\mathbf{i}} \qquad \text{(since } \mu \text{ is bilinear)} \\ &= -\mathbf{i}\end{aligned}$$

and

$$\begin{aligned}\mu(a,\mu(b,c)) &= \mu\left(\mathbf{i},\underbrace{\mu(\mathbf{k},\mathbf{k})}_{=-\mathbf{e}}\right) = \mu(\mathbf{i},-\mathbf{e}) = -\underbrace{\mu(\mathbf{i},\mathbf{e})}_{=\mathbf{i}} \qquad \text{(since } \mu \text{ is bilinear)} \\ &= -\mathbf{i}.\end{aligned}$$

Thus, $\mu(\mu(a,b),c) = \mu(a,\mu(b,c))$ is proved for this triple. Similarly, the remaining $9-1=8$ triples can be checked. Thus, associativity of multiplication is proved for $\mathbb{H}$.

It remains to prove the neutrality of 1. In other words, it remains to prove that $a \cdot \mathbf{e} = \mathbf{e} \cdot a = a$ for each $a \in \mathbb{H}$. Once again, the bilinearity of the multiplication of $\mathbb{H}$ can be used to reduce this to the case when $a \in \{\mathbf{e},\mathbf{i},\mathbf{j},\mathbf{k}\}$ (here we need to use Theorem 3.8.3 instead of Lemma 3.12.1); but in this case, the claim follows from our definition of μ. The details are LTTR.

4. Monoid algebras and polynomials ([DumFoo04, Chapter 9])

Convention 4.0.1. Let R be a **commutative** ring. (This will be a standing assumption throughout this chapter.)

In Section 3.12, we have learned how to define an R-algebra the "slick" way: Define an R-module first, and then define an R-bilinear map on it, which will serve as the multiplication of the algebra. Then show that the multiplication is associative (this is best done "by linearity", i.e., using Lemma 3.12.1) and has a unity (this can again be simplified using linearity).

I illustrated this method on the example of the ring of quaternions (an $\mathbb{R}$-algebra).

Now let me apply it to define a more important class of algebras: the monoid algebras, and, as a particular case, the polynomial rings.

4.1. Monoid algebras

4.1.1. Definition

Recall the notion of a **monoid**: Roughly speaking, it is a "group without inverses". That is, a **monoid** is a triple $(M, \cdot, 1)$, where M is a set, $\cdot$ is an associative binary operation on M, and 1 is an element of M that is neutral for $\cdot$. We will write mn for $m \cdot n$ whenever $m, n \in M$. Moreover, the element mn will be called the **product** of m and n in the monoid M. We will write M for the monoid $(M, \cdot, 1)$ if $\cdot$ and 1 are clear from the context. The monoid M is said to be **abelian** if $mn = nm$ for all $m, n \in M$. (This generalizes the notion of an abelian group.) Given a monoid $(M, \cdot, 1)$, the binary operation $\cdot$ is called the **operation** of M, and the element 1 is called the **neutral element** of M. We say that the monoid M is **written multiplicatively** (or, for short, **multiplicative**) when its operation is denoted by $\cdot$, and we say that it is **written additively** (or, for short, **additive**) when its operation is denoted by $+$. Usually, the neutral element of a multiplicative monoid is denoted by 1, whereas the neutral element of an additive monoid is denoted by 0.

Here is the informal **idea** behind the notion of a monoid algebra**:** The monoid algebra $R[M]$ of a multiplicative monoid M is the R-algebra obtained by "adjoining" the monoid M to the ring R, which means "inserting" the elements of M "into" R. That is, the algebra $R[M]$ consists of "formal products" rm with $r \in R$ and $m \in M$, as well as their formal sums. These products are multiplied using the multiplications of R and M:

$$(r_1 m_1) \cdot (r_2 m_2) = (r_1 r_2) \cdot (m_1 m_2).$$

Let us formalize this:[126]

Definition 4.1.1. Let M be a monoid, written multiplicatively (so that $\cdot$ denotes its operation, and 1 denotes its neutral element).

The **monoid algebra of M over R** (also known as the **monoid ring of M over R**) is the R-algebra $R[M]$ defined as follows: As an R-module, it is the free R-module $R^{(M)}$. Its multiplication is defined to be the unique R-bilinear map $\mu : R^{(M)} \times R^{(M)} \to R^{(M)}$ that satisfies

$$\mu(e_m, e_n) = e_{mn} \qquad \text{for all } m, n \in M. \tag{70}$$

Here, $(e_m)_{m \in M}$ is the standard basis of $R^{(M)}$ (that is, $e_m \in R^{(M)}$ is the family whose m-th entry is 1 and whose all other entries are 0). The unity of this R-algebra $R[M]$ is e_1.

Theorem 4.1.2. This is indeed a well-defined R-algebra.

Proof. Theorem 3.9.2 guarantees that there is a unique R-bilinear map $\mu : R^{(M)} \times R^{(M)} \to R^{(M)}$ that satisfies (70). It remains to prove that the R-module $R^{(M)}$ (equipped with the multiplication μ and the unity e_1) is an R-algebra.

All we need to show is that μ is associative, and that e_1 is a unity. I will only show the first statement, and leave the second to you.

We need to show that $\mu(\mu(a,b),c) = \mu(a,\mu(b,c))$ for all $a, b, c \in R[M]$. According to Lemma 3.12.1, it suffices to prove that

$$\mu(\mu(e_m, e_n), e_p) = \mu(e_m, \mu(e_n, e_p)) \qquad \text{for all } m, n, p \in M$$

(since the family $(e_m)_{m \in M}$ is a basis of $R^{(M)} = R[M]$).

Let us do this: If $m, n, p \in M$, then

$$\mu\left(\underbrace{\mu(e_m, e_n)}_{=e_{mn}}, e_p\right) = \mu(e_{mn}, e_p) = e_{(mn)p} = e_{mnp}$$

[126] We recall that R is a commutative ring. Furthermore, we recall that if M is any set, then R^M is the R-module

$$\left\{(r_i)_{i \in M} \mid r_i \in R \text{ for each } i \in M\right\}$$

(consisting of all families $(r_i)_{i \in M}$ of elements of R), whereas $R^{(M)}$ is the R-submodule

$$\bigoplus_{i \in M} R = \left\{(r_i)_{i \in M} \in R^M \mid \text{all but finitely many } i \in M \text{ satisfy } r_i = 0\right\}$$

of R^M. If the set M is finite, then $R^{(M)} = R^M$.

The R-module $R^{(M)}$ is free, and the **standard basis** $(e_m)_{m \in M}$ of $R^{(M)}$ is defined as follows: For each $m \in M$, the vector $e_m \in R^{(M)}$ is the family whose m-th entry is 1 and whose all other entries are 0. (If $M = \{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$, then this recovers the classical linear-algebraic standard basis: e.g., if $M = \{1, 2, 3\}$, then $e_1 = (1, 0, 0)$ and $e_2 = (0, 1, 0)$ and $e_3 = (0, 0, 1)$.)

The standard basis $(e_m)_{m \in M}$ of $R^{(M)}$ is, of course, a basis of $R^{(M)}$.

and similarly $\mu\left(e_m, \mu\left(e_n, e_p\right)\right) = e_{mnp}$, so we indeed have $\mu\left(\mu\left(e_m, e_n\right), e_p\right) = \mu\left(e_m, \mu\left(e_n, e_p\right)\right)$ as desired. This completes the proof that μ is associative. Thus, Theorem 4.1.2 is proven. □

Since the bilinear map μ in Definition 4.1.1 is used as the multiplication of $R[M]$, we can rewrite the equality (70) as follows:

$$e_m \cdot e_n = e_{mn} \qquad \text{for all } m, n \in M. \tag{71}$$

From the way we defined monoids, it is clear that every group is a monoid. Monoid algebras of groups have a special name:

Definition 4.1.3. When a monoid M is a group, its monoid algebra $R[M]$ is called a **group algebra** (or **group ring**).

4.1.2. Examples

Let me show a few examples of monoid algebras.

Example 4.1.4. Consider the order-2 cyclic group $C_2 = \{1, u\}$ with $u^2 = 1$ (of course, we write C_2 multiplicatively). This group is better known as $\mathbb{Z}/2$, and its operation is commonly written as addition, not as multiplication; but we want to write it multiplicatively here, in order to match the way M is written in Definition 4.1.1.

How does the group algebra $\mathbb{Q}[C_2]$ look like? As a $\mathbb{Q}$-module (i.e., $\mathbb{Q}$-vector space), it has a basis $(e_m)_{m \in C_2} = (e_1, e_u)$. Thus, any element of $\mathbb{Q}[C_2]$ can be written as $a \underbrace{e_1}_{=1} + be_u = a + be_u$ for some unique $a, b \in \mathbb{Q}$. (As usual, we are writing 1 for the unity of our ring $\mathbb{Q}[C_2]$, which is e_1.)

The multiplication on $\mathbb{Q}[C_2]$ is $\mathbb{Q}$-bilinear and given on the basis by

$$e_1 e_1 = e_{1 \cdot 1} = e_1, \qquad e_1 e_u = e_{1 \cdot u} = e_u,$$
$$e_u e_1 = e_{u \cdot 1} = e_u, \qquad e_u e_u = e_{u \cdot u} = e_{u^2} = e_1.$$

Let us use this to compute some products in $\mathbb{Q}[C_2]$:

$$\begin{aligned}
(3 + 2e_u)(1 + 2e_u) &= 3 \cdot 1 + 3 \cdot 2e_u + 2e_u \cdot 1 + 2e_u \cdot 2e_u \\
&= 3 + 6e_u + 2e_u + 4 \underbrace{e_u e_u}_{=e_1=1} \\
&= 3 + 6e_u + 2e_u + 4 = 7 + 8e_u; \\
(1 + e_u)^2 &= 1 + 2e_u + \underbrace{e_u^2}_{=e_u e_u = e_1 = 1} = 1 + 2e_u + 1 = 2 + 2e_u; \\
(1 - e_u)(1 + e_u) &= 1 - \underbrace{e_u^2}_{=e_u e_u = e_1 = 1} \qquad \left(\begin{array}{c} \text{since } (1-x)(1+x) = 1 - x^2 \\ \text{for any } x \text{ in any ring} \end{array} \right) \\
&= 1 - 1 = 0.
\end{aligned}$$

The last of these computations shows that $\mathbb{Q}[C_2]$ is not an integral domain. In general, for any $a, b, c, d \in \mathbb{Q}$, we have

$$\begin{aligned}(a+be_u)(c+de_u) &= ac + ade_u + b \underbrace{e_u c}_{\substack{=ce_u \\ \text{(since the multiplication of } \mathbb{Q}[C_2] \\ \text{is } \mathbb{Q}\text{-bilinear)}}} + b \underbrace{e_u d}_{\substack{=de_u \\ \text{(since the multiplication of } \mathbb{Q}[C_2] \\ \text{is } \mathbb{Q}\text{-bilinear)}}} e_u \\ &= ac + ade_u + bce_u + bd \underbrace{e_u e_u}_{=e_1=1} = ac + ade_u + bce_u + bd \\ &= (ac+bd) + (ad+bc)\, e_u. \end{aligned} \tag{72}$$

How does $\mathbb{Q}[C_2]$ "look like"? Meaning, what known $\mathbb{Q}$-algebras is $\mathbb{Q}[C_2]$ isomorphic to (if any)?

I **claim** that

$$\mathbb{Q}[C_2] \cong \mathbb{Q}^2 = \mathbb{Q} \times \mathbb{Q} \qquad (\text{as } \mathbb{Q}\text{-algebras}). \tag{73}$$

(See Definition 3.11.11 for the meaning of $\mathbb{Q}^2$ and $\mathbb{Q} \times \mathbb{Q}$.)

[*Proof of (73):* First, we observe that $\mathbb{Q}[C_2]$ is commutative (this is easy to check), and that the element $z := \dfrac{1+e_u}{2}$ of $\mathbb{Q}[C_2]$ is idempotent (since an easy computation shows $z^2 = z$). Hence, Exercise 2.10.4 **(c)** shows that the map

$$\begin{aligned} f : (z\mathbb{Q}[C_2]) \times ((1-z)\mathbb{Q}[C_2]) &\to \mathbb{Q}[C_2], \\ (a, b) &\mapsto a + b \end{aligned}$$

is a ring isomorphism; thus, this map f is invertible. This map f is furthermore $\mathbb{Q}$-linear and thus is a $\mathbb{Q}$-algebra morphism. Since f is invertible, we thus conclude that f is a $\mathbb{Q}$-algebra isomorphism (by Proposition 3.11.8). Now, what are $z\mathbb{Q}[C_2]$ and $(1-z)\mathbb{Q}[C_2]$? A general element of $\mathbb{Q}[C_2]$ has the form $a + be_u$ for some $a, b \in \mathbb{Q}$. Thus, a general element of $z\mathbb{Q}[C_2]$ has the form $z(a+be_u)$ for some $a, b \in \mathbb{Q}$. Since

$$\begin{aligned} z(a+be_u) &= \frac{1+e_u}{2}(a+be_u) = \frac{1}{2} \underbrace{(1+e_u)(a+be_u)}_{\substack{=a+e_u a+be_u+e_u be_u \\ =a+ae_u+be_u+be_u e_u}} \\ &= \frac{1}{2}\left(a + ae_u + be_u + b\underbrace{e_u e_u}_{=e_1=1}\right) = \frac{1}{2}\left((a+b) + (a+b)\, e_u\right) \\ &= (a+b) \cdot \underbrace{\frac{1+e_u}{2}}_{=z} = \underbrace{(a+b)}_{\in \mathbb{Q}} z, \end{aligned}$$

we see that any such element is a **scalar** multiple of z (that is, an element of the form λz for some $\lambda \in \mathbb{Q}$, not just a multiple of z in the ring $\mathbb{Q}[C_2]$). In other words, any such element belongs to the $\mathbb{Q}$-submodule (= $\mathbb{Q}$-vector subspace)

$$\mathbb{Q}z := \{\lambda z \mid \lambda \in \mathbb{Q}\} \qquad \text{of } \mathbb{Q}[C_2].$$

Thus, $z\mathbb{Q}[C_2] \subseteq \mathbb{Q}z$. Since we also have $\mathbb{Q}z \subseteq z\mathbb{Q}[C_2]$ (since every $\lambda \in \mathbb{Q}$ satisfies $\lambda z = z \cdot (\lambda e_1) \in z\mathbb{Q}[C_2]$), this entails $z\mathbb{Q}[C_2] = \mathbb{Q}z$. Hence, in particular, $\mathbb{Q}z$ is a $\mathbb{Q}$-algebra with unity z. However, the map

$$\mathbb{Q} \to \mathbb{Q}z, \ \lambda \mapsto \lambda z$$

is a $\mathbb{Q}$-algebra morphism (indeed, it is clearly $\mathbb{Q}$-linear; it respects multiplication since $(\lambda z)(\mu z) = \lambda\mu \underbrace{z^2}_{=z} = \lambda\mu z$ for any $\lambda, \mu \in \mathbb{Q}$; its respects the unity since $1z = z$ is the unity of $\mathbb{Q}z$), and thus is a $\mathbb{Q}$-algebra isomorphism (since it is easily seen to be bijective). Thus, $\mathbb{Q}z \cong \mathbb{Q}$ as $\mathbb{Q}$-algebras. Combining this with $z\mathbb{Q}[C_2] = \mathbb{Q}z$, we obtain $z\mathbb{Q}[C_2] = \mathbb{Q}z \cong \mathbb{Q}$ as $\mathbb{Q}$-algebras. Similarly, we can prove that $(1-z)\mathbb{Q}[C_2] \cong \mathbb{Q}$ (indeed, a simple computation shows that $1 - z = \dfrac{1 - e_u}{2}$, and thus we can mostly repeat our above argument with $1 - z$ instead of z, with the main difference being that some plus signs become minus signs).

So the isomorphism f results in

$$\mathbb{Q}[C_2] \cong \underbrace{(z\mathbb{Q}[C_2])}_{\cong \mathbb{Q}} \times \underbrace{((1-z)\mathbb{Q}[C_2])}_{\cong \mathbb{Q}} \cong \mathbb{Q} \times \mathbb{Q} = \mathbb{Q}^2.$$

This proves (73).]

Retracing our proof of (73), we actually get an explicit $\mathbb{Q}$-algebra isomorphism

$$\begin{aligned} &\mathbb{Q}^2 \to \mathbb{Q}[C_2], \\ &(\lambda, \mu) \mapsto f(\lambda z, \mu(1-z)) = \lambda z + \mu(1-z) = \lambda \cdot \frac{1+e_u}{2} + \mu \cdot \frac{1-e_u}{2} \\ &\qquad = \frac{\lambda+\mu}{2} + \frac{\lambda-\mu}{2} e_u. \end{aligned}$$

The inverse of this isomorphism is the $\mathbb{Q}$-algebra isomorphism

$$\begin{aligned} &\mathbb{Q}[C_2] \to \mathbb{Q}^2, \\ &a + be_u \mapsto (a+b, \ a-b) \qquad (\text{for all } a, b \in \mathbb{Q}). \end{aligned}$$

Note that there are only two $\mathbb{Q}$-algebra isomorphisms from $\mathbb{Q}[C_2]$ to $\mathbb{Q}^2$: One is the one we just constructed; the other is

$$\begin{aligned} &\mathbb{Q}[C_2] \to \mathbb{Q}^2, \\ &a + be_u \mapsto (a-b, \ a+b) \qquad (\text{for all } a, b \in \mathbb{Q}) \end{aligned}$$

(which differs from the first only in $a+b$ and $a-b$ being swapped). In contrast, there are infinitely many $\mathbb{Q}$**-module** isomorphisms from $\mathbb{Q}[C_2]$ to $\mathbb{Q}^2$; the simplest one just sends each $a+be_u$ to (a,b) (for all $a,b \in \mathbb{Q}$).

Example 4.1.5.

(a) We can easily repeat Example 4.1.4 using the field $\mathbb{R}$ (or $\mathbb{C}$) instead of $\mathbb{Q}$. Everything works just as it did for $\mathbb{Q}$. For example, we get an $\mathbb{R}$-algebra isomorphism $\mathbb{R}^2 \to \mathbb{R}[C_2]$.

(b) Now, let us try to repeat Example 4.1.4 using the ring $\mathbb{Z}$ instead of $\mathbb{Q}$. The multiplication rule (72) still holds (but now for $a,b,c,d \in \mathbb{Z}$). What about the isomorphism (73) ? The idempotent z no longer exists (since we had to divide by 2 to construct it, but we cannot divide by 2 in $\mathbb{Z}$), so our proof of (73) does not work. And indeed, (73) does not hold for $\mathbb{Z}$. The $\mathbb{Z}$-algebra

$$\mathbb{Z}[C_2] = \{a+be_u \mid a,b \in \mathbb{Z}\}$$

is **not** isomorphic to any direct product of nontrivial $\mathbb{Z}$-algebras. This can be proved by showing that $\mathbb{Z}[C_2]$ has no idempotents other than 0 and 1. (In fact, if $a+be_u \in \mathbb{Z}[C_2]$ is an idempotent, then $(a+be_u)^2 = a+be_u$. But (72) yields $(a+be_u)^2 = \left(a^2+b^2\right)+2abe_u$, so this idempotency results in $\left(a^2+b^2\right)+2abe_u = a+be_u$, and thus $a^2+b^2 = a$ and $2ab = b$ (since $e_1 = 1$ and e_u are $\mathbb{Z}$-linearly independent). But the only integer solutions (a,b) of this system of two equations are $(0,0)$ and $(1,0)$ (check this!); thus, the only idempotents of $\mathbb{Z}[C_2]$ are $0+0e_u = 0$ and $1+0e_u = 1$.)

Example 4.1.6. Now, let us take the order-3 cyclic group $C_3 = \{1,u,v\}$ with $u^3 = 1$ and $v = u^2$. (Again, this group is better known as $\mathbb{Z}/3$, but we write it multiplicatively.) Then, $\mathbb{Q}[C_3]$ is again commutative, and has an idempotent $z := \dfrac{1+e_u+e_v}{3}$; this leads to a $\mathbb{Q}$-algebra isomorphism

$$\mathbb{Q}[C_3] \cong \mathbb{Q} \times S,$$

where the $\mathbb{Q}$ factor is

$$z\mathbb{Q}[C_3] = \mathbb{Q}z = \{a+ae_u+ae_v \mid a \in \mathbb{Q}\}$$

and where the S factor is

$$(1-z)\mathbb{Q}[C_3] = \{a+be_u+ce_v \mid a+b+c = 0\}.$$

The $\mathbb{Q}$ factor is 1-dimensional (as a $\mathbb{Q}$-vector space), while the S factor is 2-dimensional. Can S be decomposed further? How does S "look like"? We will later see (in Exercise 4.5.3 below).

Example 4.1.7. Here is a **non-example**: The ring of quaternions $\mathbb{H}$ is **not** a monoid algebra. It is pretty close, in that it has a basis $(1, i, j, k)$ (over $\mathbb{R}$) with the property that the product of any two basis elements is either a basis element again (for example, $ij = k$) or the negative of a basis element (for example, $ji = -k$). However, for it to be a monoid algebra, it would need a basis such that the product of any two basis elements is always a basis element (never the negative of a basis element).[127] Such a basis does not exist for $\mathbb{H}$.

If we remove all the minus signs in the definition of $\mathbb{H}$ (that is, we replace the multiplication rules by $i^2 = j^2 = k^2 = 1$ and $ij = ji = k$ and $jk = kj = i$ and $ki = ik = j$), then we actually do obtain a monoid algebra (namely, the group algebra of the Klein four-group).

We can find another group algebra closely related to $\mathbb{H}$. Indeed, we define the **quaternion group** Q_8 to be the subgroup $\{1, i, j, k, -1, -i, -j, -k\}$ of the group of units of $\mathbb{H}$. Then, consider the group algebra $\mathbb{H}' := \mathbb{R}[Q_8]$ of this group Q_8. This group algebra $\mathbb{H}'$ is 8-dimensional as an $\mathbb{R}$-vector space, whereas $\mathbb{H}$ is 4-dimensional; thus, $\mathbb{H}'$ is not quite $\mathbb{H}$ (but rather close). The main difference between $\mathbb{H}$ and $\mathbb{H}'$ is that the elements e_1 and e_{-1} of $\mathbb{H}'$ are two different basis elements (thus linearly independent), whereas the elements 1 and -1 of $\mathbb{H}$ are negatives of each other. Even though $\mathbb{H}'$ is not commutative, we can define a principal ideal $(e_1 + e_{-1})\,\mathbb{H}'$ of $\mathbb{H}'$ (by Exercise 2.8.2, since $e_1 + e_{-1}$ is a central element of $\mathbb{H}'$), and then it is not hard to show that the quotient ring $\mathbb{H}'/(e_1 + e_{-1})\,\mathbb{H}'$ is isomorphic to $\mathbb{H}$. Thus, while $\mathbb{H}$ itself is not a group ring, we can obtain $\mathbb{H}$ from the group ring $\mathbb{H}' = \mathbb{R}[Q_8]$ by "setting e_{-1} equal to the negative of e_1" (that is, quotienting out the principal ideal generated by $e_1 + e_{-1}$).

Exercise 4.1.1. Let R be a commutative ring, and n be a positive integer. In Exercise 2.10.5, we have defined the ring Circ_n of circulant $n \times n$-matrices $A \in R^{n \times n}$.

(a) Prove that this ring Circ_n is actually an R-subalgebra of $R^{n \times n}$.

(b) Prove that this R-algebra Circ_n is isomorphic to the group algebra $R[C_n]$, where C_n is the order-n cyclic group.

Exercise 4.1.2. Let R be a commutative ring. Let G be a finite group. Let s be the element $\sum_{g \in G} e_g$ of the group algebra $R[G]$.

(a) Prove that $s^2 = |G| \cdot s$.

[127] In general, you can describe a monoid algebra as an algebra that has a basis that contains the unity (i.e., the unity of the algebra belongs to the basis) and is closed under multiplication (i.e., the product of any two basis elements is again a basis element).

(b) If $|G| \cdot 1_R$ is invertible in R, then prove that $\dfrac{1}{|G|} s \in R[G]$ is idempotent.

[This generalizes the idempotents z in Example 4.1.4 and Example 4.1.6.]

Exercise 4.1.3.

(a) Prove the claim made in Example 4.1.4, saying that there are only two $\mathbb{Q}$-algebra isomorphisms from $\mathbb{Q}[C_2]$ to $\mathbb{Q}^2$.

(b) More generally: Let R be any integral domain. Prove that there are exactly $n!$ many R-algebra isomorphisms from R^n to R^n, and each of them has the form

$$R^n \to R^n,$$
$$(r_1, r_2, \ldots, r_n) \mapsto \left(r_{\sigma(1)}, r_{\sigma(2)}, \ldots, r_{\sigma(n)}\right)$$

for some permutation σ of $\{1, 2, \ldots, n\}$. (In other words, each of these isomorphisms just permutes the entries of the n-tuple.)

[**Hint:** For part **(b)**, let f be an R-algebra isomorphism $R^n \to R^n$. Consider the standard basis vectors $e_1, e_2, \ldots, e_n$ of R^n. Form the $n \times n$-matrix whose rows are the n vectors $f(e_1), f(e_2), \ldots, f(e_n)$. Show that each row of this matrix has at least one nonzero entry, but each column has at most one nonzero entry. Furthermore, what must these entries be?]

4.1.3. Pretending that the elements of M belong to $R[M]$

Convention 4.1.8. Let R be a commutative ring. Let M be a monoid. The elements e_m of the standard basis $(e_m)_{m \in M}$ of $R[M]$ will often be just denoted by m (by abuse of notation). Thus, for example, the element $a + be_u + ce_v$ of $\mathbb{Q}[C_3]$ (from Example 4.1.6) will be written as $a + bu + cv$. With this notation, an element of $R[M]$ is (at least notationally) really just a sum of products of elements of R with elements of M.

Do **not** use this convention when it can create confusion! In particular, do not use it when some elements of M include minus (or plus) signs, such as the elements $-1, -i, -j, -k$ in Example 4.1.7. (Indeed, in Example 4.1.7, it is crucial that e_1 and e_{-1} are two different basis elements of $\mathbb{H}'$, not negatives of each other. Denoting them by 1 and -1 would obscure this and risk confusing the nonzero element $e_1 + e_{-1}$ for the zero sum $1 + (-1) = 0$.)

4.1.4. General properties of monoid algebras

We shall now state some general properties of monoid algebras, and agree on some conventions that will make it easier to work in those algebras.

Proposition 4.1.9. Let M be an **abelian** monoid. Then, the monoid ring $R[M]$ is commutative.

Proof. We must prove that $ab = ba$ for all $a, b \in R[M]$. This is a typical linearity argument (just as the proof of Lemma 3.12.1): Since $(e_m)_{m \in M}$ is a basis of the R-module $R[M]$, we can write a and b as R-linear combinations of this family $(e_m)_{m \in M}$. That is, there exist scalars $a_m \in R$ and $b_m \in R$ for all $m \in M$ such that

$$a = \sum_{m \in M} a_m e_m \qquad \text{and} \qquad b = \sum_{m \in M} b_m e_m$$

(and such that $a_m = 0$ for all but finitely many $m \in M$, and likewise for the b_m). Multiplying these two equalities, we find

$$\begin{aligned} ab &= \left(\sum_{m \in M} a_m e_m \right) \left(\sum_{m \in M} b_m e_m \right) = \left(\sum_{m \in M} a_m e_m \right) \left(\sum_{n \in M} b_n e_n \right) \\ &\qquad \left(\text{here, we renamed } m \text{ as } n \text{ in the second sum}\right) \\ &= \sum_{m \in M} \sum_{n \in M} a_m b_n \underbrace{e_m e_n}_{\substack{=e_{mn} \\ \text{(by (71))}}} \\ &\qquad \left(\text{since the multiplication of the } R\text{-algebra } R[M] \text{ is } R\text{-bilinear}\right) \\ &= \sum_{m \in M} \sum_{n \in M} a_m b_n \underbrace{e_{mn}}_{\substack{=e_{nm} \\ \text{(since } M \text{ is abelian,} \\ \text{so that } mn = nm\text{)}}} = \sum_{m \in M} \sum_{n \in M} a_m b_n e_{nm} \end{aligned}$$

and (if we multiply them in the opposite order)

$$\begin{aligned} ba &= \left(\sum_{m \in M} b_m e_m \right) \left(\sum_{m \in M} a_m e_m \right) = \left(\sum_{n \in M} b_n e_n \right) \left(\sum_{m \in M} a_m e_m \right) \\ &\qquad \left(\text{here, we renamed } m \text{ as } n \text{ in the first sum}\right) \\ &= \underbrace{\sum_{n \in M} \sum_{m \in M}}_{= \sum_{m \in M} \sum_{n \in M}} \underbrace{b_n a_m}_{\substack{=a_m b_n \\ \text{(since } R \text{ is commutative)}}} \underbrace{e_n e_m}_{\substack{=e_{nm} \\ \text{(by (71))}}} \\ &\qquad \left(\text{since the multiplication of the } R\text{-algebra } R[M] \text{ is } R\text{-bilinear}\right) \\ &= \sum_{m \in M} \sum_{n \in M} a_m b_n e_{nm}. \end{aligned}$$

The right hand sides of these two equalities are equal; thus, so are the left hand sides. In other words, $ab = ba$. This completes the proof of Proposition 4.1.9. $\square$

Proposition 4.1.10. Let M be a monoid with neutral element 1. Then, the map

$$\begin{aligned} R &\to R\left[M\right], \\ r &\mapsto r \cdot e_1 \end{aligned}$$

is an injective R-algebra morphism.

Proof. First of all, this map is clearly injective, because the family $\left(e_m\right)_{m \in M}$ is a basis of $R\left[M\right]$ and thus is R-linearly independent (so $r \cdot e_1 \neq s \cdot e_1$ for any two distinct $r, s \in R$). It remains to prove that this map is an R-algebra morphism. But this is a particular case of the following general fact: If A is an R-algebra, then the map

$$\begin{aligned} R &\to A, \\ r &\mapsto r \cdot 1_A \end{aligned}$$

is an R-algebra morphism. This fact is easy to show (for example, the map respects multiplication, since any $r, s \in R$ satisfy $\left(r \cdot 1_A\right) \cdot \left(s \cdot 1_A\right) = rs \cdot 1_A \cdot 1_A = rs \cdot 1_A$), and we can apply it to $A = R\left[M\right]$ (recalling that $1_{R[M]} = e_1$) to obtain precisely the claim we are trying to prove. □

Convention 4.1.11. If M is a monoid, then we shall identify each $r \in R$ with $r \cdot e_1 \in R\left[M\right]$. This identification is harmless[128], and turns R into an R-subalgebra of $R\left[M\right]$.

An element of $R\left[M\right]$ will be called **constant** if it lies in this subalgebra (i.e., if it is of the form $r \cdot e_1$ for some $r \in R$). Thus, we have identified each constant element of $R\left[M\right]$ with the corresponding element of R.

A **warning** might be in order: In Example 4.1.4, we have seen that $\mathbb{Q}\left[C_2\right] \cong \mathbb{Q} \times \mathbb{Q}$ as $\mathbb{Q}$-algebras. Now, in Convention 4.1.11, we have identified $\mathbb{Q}$ with a $\mathbb{Q}$-subalgebra of $\mathbb{Q}\left[C_2\right]$. But this subalgebra is not one of the two $\mathbb{Q}$ factors in $\mathbb{Q}\left[C_2\right] \cong \mathbb{Q} \times \mathbb{Q}$. Indeed, as a $\mathbb{Q}$-subalgebra, it contains the unity of $\mathbb{Q}\left[C_2\right]$, but none of the two $\mathbb{Q}$ factors does.

Proposition 4.1.12. Let M be a monoid. Then, the map

$$\begin{aligned} M &\to R\left[M\right], \\ m &\mapsto e_m \end{aligned}$$

is a monoid morphism from M to $\left(R\left[M\right], \cdot, 1\right)$.

[128] Indeed, Proposition 4.1.10 shows that the map $R \to R\left[M\right]$ sending each $r \in R$ to $r \cdot e_1$ is an injective R-algebra morphism. Thus, this map keeps distinct elements of R distinct in $R\left[M\right]$ (since it is injective), and respects addition and multiplication (since it is an R-algebra morphism).

Proof. This map respects multiplication (because of (71)) and sends the neutral element of M to the unity of $R[M]$ (since e_1 is the unity of $R[M]$). Thus, it is a monoid morphism. □

Note that if we use Convention 4.1.8, then the "$m \mapsto e_m$" in Proposition 4.1.12 can be rewritten as "$m \mapsto m$", so the map from Proposition 4.1.12 looks like an inclusion map. This is merely an artefact of our notation. In truth, the element m of the monoid M is not literally the same as the corresponding basis element e_m of the monoid algebra $R[M]$; we have just agreed to call both of them m for brevity. But Proposition 4.1.12 shows that using the same letter for these two elements is a mostly harmless abuse of notation. The only possible problem it can cause is when the map in Proposition 4.1.12 fails to be injective, so we might accidentally equate two distinct elements m, n of M whose corresponding basis elements e_m and e_n are equal. Fortunately, this can only happen if the ring R is trivial (indeed, for any nontrivial ring R, the basis elements e_m for $m \in M$ are distinct), and this is not a very interesting case. (This is also an issue that rarely comes up in practice. The purpose of Convention 4.1.8 is to simplify computations in $R[M]$, not to "pull" them back into M.)

Exercise 4.1.4. Let n be a positive integer. Consider the symmetric group S_n – that is, the group of all permutations of the set $\{1, 2, \ldots, n\}$.

For any two distinct elements i and j of $\{1, 2, \ldots, n\}$, let $t_{i,j}$ be the permutation in S_n that swaps i with j while leaving the remaining elements of $\{1, 2, \ldots, n\}$ unchanged. (This is called a **transposition**.)

For each $i \in \{1, 2, \ldots, n\}$, define an element $Y_i \in \mathbb{Z}[S_n]$ of the group algebra $\mathbb{Z}[S_n]$ by

$$Y_i := \sum_{j=1}^{i-1} t_{i,j} = t_{i,1} + t_{i,2} + \cdots + t_{i,i-1}$$

(where we are using Convention 4.1.8, so that $t_{i,j}$ really means $e_{t_{i,j}}$). (Thus, $Y_1 = 0$ and $Y_2 = t_{2,1}$ and $Y_3 = t_{3,1} + t_{3,2}$ and so on.) The n elements $Y_1, Y_2, \ldots, Y_n$ are called the **Young-Jucys-Murphy elements** of $\mathbb{Z}[S_n]$.

(a) Prove that the n elements $Y_1, Y_2, \ldots, Y_n$ commute (i.e., that we have $Y_i Y_j = Y_j Y_i$ for all $i, j \in \{1, 2, \ldots, n\}$).

(b) Prove that the element $Y_1 + Y_2 + \cdots + Y_n = \sum_{1 \leq j < i \leq n} t_{i,j}$ belongs to the center of $\mathbb{Z}[S_n]$.

Exercise 4.1.5. Let G be a finite group. Let R be a nontrivial commutative ring.

Let T be a subset of G. Let s_T be the element $\sum_{t \in T} t$ of the group algebra $R[S_n]$ (where we use Convention 4.1.8, so that t means e_t).

Prove that the element s_T of $R[G]$ is central if and only if T is a union of conjugacy classes of G (that is, if every element of G that is conjugate to an element of T must itself be an element of T).

4.2. Polynomial rings

4.2.1. Univariate polynomials

Now, we can effortlessly define polynomial rings. Recall that R is a commutative ring. Recall also that $\mathbb{N} = \{0, 1, 2, \ldots\}$ (so $0 \in \mathbb{N}$).

Definition 4.2.1. Let C be the free monoid with a single generator x. This is the monoid whose elements are countably many distinct symbols named

$$x^0, \quad x^1, \quad x^2, \quad x^3, \quad \ldots,$$

and whose operation is defined by

$$x^i \cdot x^j = x^{i+j} \qquad \text{for all } i, j \in \mathbb{N}.$$

We write this monoid multiplicatively, but of course it is just the well-known monoid $(\mathbb{N}, +, 0)$ in new clothes (we have renamed each $i \in \mathbb{N}$ as x^i; we have renamed addition as multiplication). Its neutral element is x^0. We set $x = x^1$ (so that x^i really is the i-th power of x).

The elements of C are called **monomials** (in the variable x). The specific element x is called the **indeterminate** (or, somewhat imprecisely, the **variable**).

Now, the **univariate polynomial ring** over R is defined to be the monoid algebra $R[C]$. It is commonly denoted by $R[x]$. Following Convention 4.1.8, we simply write m for e_m when $m \in C$ (that is, we write x^i for the basis element e_{x^i}); thus, $R[x]$ is a free R-module with basis

$$\left(x^0, x^1, x^2, x^3, \ldots\right) = \left(1, x, x^2, x^3, \ldots\right).$$

Hence, any $p \in R[x]$ can be written as a finite R-linear combination of powers of x. In other words, any $p \in R[x]$ can be written in the form

$$p = a_0 x^0 + a_1 x^1 + a_2 x^2 + \cdots + a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

for some $n \in \mathbb{N}$ and some $a_0, a_1, \ldots, a_n \in R$. This representation is unique up to trailing zeroes (meaning that we can always add $0x^{n+1}$ addends – e.g., rewriting $4x^0 + 3x^1$ as $4x^0 + 3x^1 + 0x^2$ –, but other than that it is unique).

Elements of $R[x]$ are called **polynomials** in x over R.

Thus, up to notation, the univariate polynomial ring $R[x]$ is just the monoid ring $R[\mathbb{N}]$ of the abelian monoid $\mathbb{N} = (\mathbb{N}, +, 0)$. Hence, this ring $R[x]$ is commutative (by Proposition 4.1.9, since the monoid $\mathbb{N}$ is abelian). The unity of the R-algebra $R[x]$ is $x^0 = 1$.

Example 4.2.2.

(a) Here is an example of a polynomial:

$$1 + 3x^2 + 6x^3 = 1e_{x^0} + 3e_{x^2} + 6e_{x^3} \in R[x].$$

(b) A non-example: The infinite sum $1 + x + x^2 + x^3 + \cdots$ is **not** in $R[x]$. Indeed, polynomials are linear combinations of powers of x, and linear combinations are finite (by definition); even if you write them as infinite sums, they are de-facto finite because all but finitely many addends are 0. Infinite sums such as $1 + x + x^2 + x^3 + \cdots$ thus are not polynomials[129]; they are instead known as **formal power series**. There is a way to define an R-algebra of formal power series, too, but we won't do so now.

So we have defined **univariate** polynomial rings (i.e., polynomial rings in a single variable). Likewise, we can define **multivariate** polynomial rings – i.e., polynomial rings in several variables. For simplicity, let me restrict myself to finitely many variables.

4.2.2. Bivariate polynomials

To avoid a barrage of new notations, let me first introduce **bivariate** polynomial rings – i.e., polynomial rings in two variables. Their definition is just a particular case of the definition of multivariate polynomial rings (Definition 4.2.4) that we will give soon after, but it is somewhat easier to understand as it involves less complicated notations.

Definition 4.2.3. Let $C^{(2)}$ be the free abelian monoid with two generators x and y. This is the monoid whose elements are the distinct symbols

$$\begin{array}{llll} x^0y^0, & x^0y^1, & x^0y^2, & x^0y^3, \ \ldots, \\ x^1y^0, & x^1y^1, & x^1y^2, & x^1y^3, \ \ldots, \\ x^2y^0, & x^2y^1, & x^2y^2, & x^2y^3, \ \ldots, \\ \ldots, & & & \end{array}$$

that is, the distinct symbols

$$x^a y^b \qquad \text{with } a \in \mathbb{N} \text{ and } b \in \mathbb{N},$$

and whose operation is defined by

$$\left(x^a y^b\right) \cdot \left(x^c y^d\right) = x^{a+c} y^{b+d} \qquad \text{for all } a, b, c, d \in \mathbb{N}.$$

[129] You might wonder whether such sums are well-defined in the first place. Yes, they are, if one correctly defines them. For a complete definition, see (e.g.) [21s, §3.2.2].

We write this monoid multiplicatively, but of course it is just the monoid $\mathbb{N}^2 = \left(\mathbb{N}^2, +, 0\right)$ in disguise (where the addition on $\mathbb{N}^2$ that we are calling "$+$" here is entrywise, and 0 means the pair $(0,0)$), with each element (a,b) renamed as $x^a y^b$ and with addition renamed as multiplication. The elements of $C^{(2)}$ are called **monomials** in x and y. We define two specific monomials x and y by

$$x = x^1 y^0 \qquad \text{and} \qquad y = x^0 y^1.$$

These two monomials x and y are called the **indeterminates** (or, somewhat imprecisely, the **variables**). It is easy to see that any monomial $x^a y^b \in C^{(2)}$ is indeed the product of the powers x^a and y^b of these indeterminates, just as the notation suggests.

Now, the **polynomial ring in two variables x and y over R** is defined to be the monoid algebra $R\left[C^{(2)}\right]$. It is commonly denoted by $R[x,y]$. Following Convention 4.1.8, we simply write m for e_m whenever $m \in C^{(2)}$; thus, $R[x,y]$ is a free R-module with basis

$$\left(x^a y^b\right)_{(a,b)\in\mathbb{N}^2}.$$

This means that any $p \in R[x,y]$ can be uniquely written as an R-linear combination

$$p = \sum_{(a,b)\in\mathbb{N}^2} r_{a,b} x^a y^b$$

with $r_{a,b} \in R$ (such that all but finitely many of these coefficients $r_{a,b}$ are 0).

Elements of $R[x,y]$ are called **polynomials** in x and y.

Thus, up to notation, the multivariate polynomial ring $R[x,y]$ is just the monoid algebra $R\left[\mathbb{N}^2\right]$ of the abelian monoid $\mathbb{N}^2 = \left(\mathbb{N}^2, +, 0\right)$. The unity of the R-algebra $R[x,y]$ is $x^0 y^0 = 1$.

Here are some examples of bivariate polynomials:

- If $R = \mathbb{Z}$, then

$$3x^2y^7 - 10x^1y^1 + 8x^0y^5 + 2x^0y^0 = 3x^2y^7 - 10xy + 8y^5 + 2$$

  is a polynomial in x and y, thus belongs to $\mathbb{Z}[x,y]$.

- If $R = \mathbb{Q}$, then $\dfrac{2}{3}x^7y^2 - \dfrac{1}{2}x^1y^1$ is a polynomial in x and y, thus belongs to $\mathbb{Q}[x,y]$. (Of course, we don't strictly need the coefficients to be non-integers; the integers are also included in $\mathbb{Q}$. Thus, for example, the polynomial $x^2y^3 - 2x$ also belongs to $\mathbb{Q}[x,y]$.)

- Note that $x^2 + 7x$ and $y^2 + 7y$ are two (distinct) polynomials in $\mathbb{Z}[x,y]$. They happen to involve only one of the two indeterminates each, but this

does not make them any less valid. (There are also constant polynomials in $\mathbb{Z}[x,y]$, such as $17x^0y^0 = 17$.)

4.2.3. Multivariate polynomials

We shall now define multivariate polynomial rings (in finitely many variables, which we name $x_1, x_2, \ldots, x_n$). Their definition is somewhat notationally dense (subscripts inside superscripts!), but it is just a straightforward generalization of Definition 4.2.3, except that the indeterminates will now be called $x_1, x_2, \ldots, x_n$ instead of x and y:

Definition 4.2.4. Let $n \in \mathbb{N}$. Let $C^{(n)}$ be the free abelian monoid with n generators $x_1, x_2, \ldots, x_n$. This is the monoid whose elements are the distinct symbols

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \qquad \text{with } (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n,$$

and whose operation is defined by

$$\left(x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}\right) \cdot \left(x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}\right) = x_1^{a_1+b_1} x_2^{a_2+b_2} \cdots x_n^{a_n+b_n}$$
$$\text{for all } (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n \text{ and } (b_1, b_2, \ldots, b_n) \in \mathbb{N}^n.$$

We write this monoid multiplicatively, but of course it is just the monoid $\mathbb{N}^n = (\mathbb{N}^n, +, 0)$ in disguise (where the addition on $\mathbb{N}^n$ that we are calling "$+$" here is entrywise, and 0 means the n-tuple $(0, 0, \ldots, 0)$), with each element $(a_1, a_2, \ldots, a_n)$ renamed as $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ and with addition renamed as multiplication. The elements of $C^{(n)}$ are called **monomials** in $x_1, x_2, \ldots, x_n$. For each $i \in \{1, 2, \ldots, n\}$, we define a monomial x_i by

$$x_i = x_1^0 x_2^0 \cdots x_{i-1}^0 x_i^1 x_{i+1}^0 x_{i+2}^0 \cdots x_n^0.$$

These specific elements $x_1, x_2, \ldots, x_n$ are called the **indeterminates**. It is easy to see that any monomial $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \in C^{(n)}$ is indeed the product of the powers $x_1^{a_1}, x_2^{a_2}, \ldots, x_n^{a_n}$, just as the notation suggests.

Now, the **polynomial ring in n variables $x_1, x_2, \ldots, x_n$ over R** is defined to be the monoid algebra $R\left[C^{(n)}\right]$. It is commonly denoted by $R[x_1, x_2, \ldots, x_n]$. Following Convention 4.1.8, we simply write m for e_m whenever $m \in C^{(n)}$; thus, $R[x_1, x_2, \ldots, x_n]$ is a free R-module with basis

$$\left(x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}\right)_{(a_1, a_2, \ldots, a_n) \in \mathbb{N}^n}.$$

This means that any $p \in R[x_1, x_2, \ldots, x_n]$ can be uniquely written as an R-linear combination

$$p = \sum_{(a_1, a_2, \ldots, a_n) \in \mathbb{N}^n} r_{a_1, a_2, \ldots, a_n} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

with $r_{a_1,a_2,\ldots,a_n} \in R$ (such that all but finitely many of these coefficients $r_{a_1,a_2,\ldots,a_n}$ are 0).

Elements of $R[x_1, x_2, \ldots, x_n]$ are called **polynomials** in $x_1, x_2, \ldots, x_n$.

Thus, up to notation, the multivariate polynomial ring $R[x_1, x_2, \ldots, x_n]$ is just the monoid algebra $R[\mathbb{N}^n]$ of the abelian monoid $\mathbb{N}^n = (\mathbb{N}^n, +, 0)$.

The multivariate polynomial ring $R[x_1, x_2, \ldots, x_n]$ is commutative (by Proposition 4.1.9, since the monoid $\mathbb{N}^n$ is abelian).

The univariate polynomial ring $R[x]$ can be viewed as a particular case of the multivariate polynomial ring $R[x_1, x_2, \ldots, x_n]$ (obtained by taking $n = 1$ and renaming x_1 as x) [130]. Likewise, the bivariate polynomial ring $R[x, y]$ is a particular case of the multivariate polynomial ring $R[x_1, x_2, \ldots, x_n]$ (obtained by taking $n = 2$ and renaming x_1 and x_2 as x and y).

4.2.4. Evaluation, aka substitution for univariate polynomials

Polynomials as formal linear combinations are already useful and nice. But they become a much stronger tool once you learn how to evaluate them, i.e., substitute things into them. Unlike a function, a univariate polynomial over R does not have a fixed domain; you can substitute an element of R into it, but also a square matrix over R or even another polynomial, and more generally, any element of an R-algebra:

Definition 4.2.5. Let $p \in R[x]$ be a univariate polynomial. Let A be any R-algebra. Let $a \in A$.

We define the element $p(a) \in A$ as follows: Write p as

$$p = \sum_{i \in \mathbb{N}} p_i x^i$$

with $p_i \in R$ (where $p_i = 0$ for all but finitely many $i \in \mathbb{N}$), and set

$$p(a) := \sum_{i \in \mathbb{N}} p_i a^i. \tag{74}$$

This element $p(a)$ is called the **evaluation** of p at a; we also say that it is obtained by **substituting** a for x in p.

Sometimes I will denote it by $p[a]$ instead of $p(a)$ (for reasons explained below).

Note that the $p_i \in R$ in Definition 4.2.5 are unique, since $\left(x^0, x^1, x^2, \ldots\right)$ is a basis of the R-module $R[x]$. Note also that the infinite sum on the right hand side of (74) is well-defined, since we have $p_i = 0$ for all but finitely many $i \in \mathbb{N}$.

[130] Strictly speaking, this requires a minor abuse of notation: We need to identify each nonnegative integer $n \in \mathbb{N}$ with the 1-tuple $(n) \in \mathbb{N}^1$, so that the free monoid C becomes identified with $C^{(1)}$, and therefore its monoid ring $R[C]$ becomes $R\left[C^{(1)}\right]$.

As I said, A can be any R-algebra in Definition 4.2.5: for example, R itself, or a matrix ring $R^{n\times n}$, or the polynomial ring $R[x]$. In particular, we can substitute x for x in p, obtaining $p(x) = p$.

Warning 4.2.6. The notation $p(a)$ in Definition 4.2.5 has potential for confusion: Is $p(p+1)$ the evaluation of p at $p+1$ or the product of p with $p+1$? This is why I prefer the notation $p[a]$ instead of $p(a)$. I also recommend using $\cdot$ for products whenever such confusion could arise (thus, write $p \cdot (p+1)$ if you mean the product of p with $p+1$). When reading algebra literature, be aware that you will sometimes have to look at the context and make sanity checks.

Example 4.2.7. Let $R = \mathbb{Z}/2$, and let p be the polynomial $x^2 + x = x \cdot \left(x + \overline{1}\right) \in R[x]$. Let us evaluate p at elements of R:

$$p\left(\overline{0}\right) = \overline{0}^2 + \overline{0} = \overline{0};$$
$$p\left(\overline{1}\right) = \overline{1}^2 + \overline{1} = \overline{1} + \overline{1} = \overline{2} = \overline{0}.$$

Thus, the polynomial p gives $\overline{0}$ when evaluated at any element of $\mathbb{Z}/2$, even though p is not zero as a polynomial. If you want a nonzero evaluation of p, one thing you can do is to evaluate it on a square matrix:

$$p\left(\begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}\right) = \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix}^2 + \begin{pmatrix} \overline{0} & \overline{1} \\ \overline{1} & \overline{0} \end{pmatrix} = \begin{pmatrix} \overline{1} & \overline{1} \\ \overline{1} & \overline{1} \end{pmatrix} \neq 0_{2\times 2}.$$

(Or you can evaluate it at x, getting $p(x) = p \neq 0$.)

Given an R-algebra A and an element $a \in A$, we can study the operation of substituting a for x into polynomials $p \in R[x]$. This operation is rather well-behaved:

Theorem 4.2.8. Let A be an R-algebra. Let $a \in A$. Then, the map

$$\begin{aligned} R[x] &\to A, \\ p &\mapsto p[a] \end{aligned}$$

is an R-algebra morphism. In particular, for any two polynomials $p, q \in R[x]$, we have

$$(pq)[a] = p[a] \cdot q[a]; \tag{75}$$
$$(p+q)[a] = p[a] + q[a]. \tag{76}$$

The proof of this theorem will be easiest to do after showing the following simple lemma (compare with Lemma 3.12.1):

Lemma 4.2.9. Let R be a commutative ring. Let A and B be two R-algebras. Let $f : A \to B$ be an R-linear map. Let $(m_i)_{i \in I}$ be a family of vectors in A that spans A. If we have

$$f\left(m_i m_j\right) = f\left(m_i\right) f\left(m_j\right) \qquad \text{for all } i, j \in I, \tag{77}$$

then we have

$$f(ab) = f(a) f(b) \qquad \text{for all } a, b \in A. \tag{78}$$

Proof of Lemma 4.2.9. Let $a, b \in A$. Since the family $(m_i)_{i \in I}$ spans A, we can write the two vectors a and b as

$$a = \sum_{i \in I} a_i m_i \qquad \text{and} \qquad b = \sum_{j \in I} b_j m_j \tag{79}$$

for some coefficients a_i and b_j in R. Consider these coefficients. Hence,

$$ab = \left(\sum_{i \in I} a_i m_i\right)\left(\sum_{j \in I} b_j m_j\right) = \sum_{i \in I} \sum_{j \in I} a_i b_j m_i m_j$$

(since the multiplication of A is R-bilinear) and thus

$$f(ab) = f\left(\sum_{i \in I} \sum_{j \in I} a_i b_j m_i m_j\right) = \sum_{i \in I} \sum_{j \in I} a_i b_j \underbrace{f\left(m_i m_j\right)}_{\substack{= f(m_i) f\left(m_j\right) \\ \text{(by (77))}}} \qquad \text{(since } f \text{ is } R\text{-linear)}$$

$$= \sum_{i \in I} \sum_{j \in I} a_i b_j f(m_i) f\left(m_j\right) = \left(\sum_{i \in I} a_i f(m_i)\right)\left(\sum_{j \in I} b_j f\left(m_j\right)\right)$$

(since the multiplication of B is R-bilinear). Comparing this with

$$f(a) f(b) = f\left(\sum_{i \in I} a_i m_i\right) f\left(\sum_{j \in I} b_j m_j\right) \qquad \text{(by (79))}$$

$$= \left(\sum_{i \in I} a_i f(m_i)\right)\left(\sum_{j \in I} b_j f\left(m_j\right)\right) \qquad \text{(since } f \text{ is } R\text{-linear)},$$

we obtain $f(ab) = f(a) f(b)$. This proves Lemma 4.2.9. □

Proof of Theorem 4.2.8. Let f be the map

$$\begin{aligned} R[x] &\to A, \\ p &\mapsto p[a]. \end{aligned}$$

We must show that f is an R-algebra morphism.

It is easy to see that f is R-linear. (For example, in order to show that it respects addition, you need to check that $(p+q)[a] = p[a] + q[a]$ for any $p, q \in R[x]$. But this is done exactly as you would think: Write p and q as $p = \sum_{i \in \mathbb{N}} p_i x^i$ (with $p_i \in R$) and $q = \sum_{i \in \mathbb{N}} q_i x^i$ (with $q_i \in R$), and conclude that

$$p + q = \sum_{i \in \mathbb{N}} p_i x^i + \sum_{i \in \mathbb{N}} q_i x^i = \sum_{i \in \mathbb{N}} \left(p_i x^i + q_i x^i \right) = \sum_{i \in \mathbb{N}} (p_i + q_i) x^i,$$

so that

$$\begin{aligned} (p+q)[a] &= \sum_{i \in \mathbb{N}} (p_i + q_i) a^i \qquad \text{(by the definition of } (p+q)[a]) \\ &= \sum_{i \in \mathbb{N}} p_i a^i + \sum_{i \in \mathbb{N}} q_i a^i; \end{aligned}$$

but it is just as easy to see that $p[a] + q[a]$ gives the same result.)

It is furthermore clear that the map f respects the unity; indeed, $f(1) = 1[a] = 1$ (since substituting a for x in the polynomial $1 = 1x^0 + 0x^1 + 0x^2 + \cdots$ results in $1a^0 + 0a^1 + 0a^2 + \cdots = 1$).

All that now remains is to show that f respects multiplication. In other words, it remains to show that $f(pq) = f(p) f(q)$ for all $p, q \in R[x]$. Lemma 4.2.9 gives us a shortcut to proving this: Since the family $\left(x^i\right)_{i \in \mathbb{N}}$ is a basis of the R-module $R[x]$ (and thus spans this R-module), and since we already know that f is R-linear, it suffices to show that

$$f\left(x^i x^j\right) = f\left(x^i\right) f\left(x^j\right) \qquad \text{for all } i, j \in \mathbb{N} \tag{80}$$

(because if we can show this, then Lemma 4.2.9 will yield that $f(pq) = f(p) f(q)$ for all $p, q \in R[x]$).

So let us prove (80). Fix $i, j \in \mathbb{N}$. Then, $x^i[a] = a^i$ (because substituting a for x in the polynomial $x^i = 0x^0 + 0x^1 + \cdots + 0x^{i-1} + 1x^i + 0x^{i+1} + 0x^{i+2} + \cdots$ results in $0a^0 + 0a^1 + \cdots + 0a^{i-1} + 1a^i + 0a^{i+1} + 0a^{i+2} + \cdots = a^i$) and similarly $x^j[a] = a^j$ and $x^{i+j}[a] = a^{i+j}$. But $x^i x^j = x^{i+j}$, so that

$$\begin{aligned} f\left(x^i x^j\right) = f\left(x^{i+j}\right) &= x^{i+j}[a] \qquad \text{(by the definition of } f) \\ &= a^{i+j} = \underbrace{a^i}_{\substack{=x^i[a] \\ =f\left(x^i\right)}} \underbrace{a^j}_{\substack{=x^j[a] \\ =f\left(x^j\right)}} = f\left(x^i\right) f\left(x^j\right). \end{aligned}$$

(by the definition of f) (by the definition of f)

This proves (80), and thus concludes the proof of Theorem 4.2.8. □

4.2.5. Evaluation, aka substitution for multivariate polynomials

Likewise, we can substitute multiple elements into a multivariate polynomial, as long as these elements commute:

Definition 4.2.10. Let $n \in \mathbb{N}$. Let $p \in R[x_1, x_2, \ldots, x_n]$ be a multivariate polynomial. Let A be any R-algebra. Let $a_1, a_2, \ldots, a_n \in A$ be n elements of A that mutually commute (i.e., that satisfy $a_i a_j = a_j a_i$ for each $i, j \in \{1, 2, \ldots, n\}$).

We define the element $p(a_1, a_2, \ldots, a_n) \in A$ as follows: Write the polynomial p as

$$p = \sum_{(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n} p_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

with $p_{i_1, i_2, \ldots, i_n} \in R$ (where $p_{i_1, i_2, \ldots, i_n} = 0$ for all but finitely many $(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$), and set

$$p(a_1, a_2, \ldots, a_n) := \sum_{(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n} p_{i_1, i_2, \ldots, i_n} a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n}.$$

This element $p(a_1, a_2, \ldots, a_n)$ is called the **evaluation** of p at $a_1, a_2, \ldots, a_n$; we also say that it is obtained by **substituting** $a_1, a_2, \ldots, a_n$ for $x_1, x_2, \ldots, x_n$ in p.

Sometimes, I will denote it by $p[a_1, a_2, \ldots, a_n]$ instead of $p(a_1, a_2, \ldots, a_n)$.

Needless to say, this definition generalizes Definition 4.2.5.

It is clear that $p(x_1, x_2, \ldots, x_n) = p$ for any polynomial $p \in R[x_1, x_2, \ldots, x_n]$.

The analogue to Theorem 4.2.8 now is the following:

Theorem 4.2.11. Let $n \in \mathbb{N}$. Let A be an R-algebra. Let $a_1, a_2, \ldots, a_n \in A$ be n elements of A that mutually commute. Then, the map

$$\begin{aligned} R[x_1, x_2, \ldots, x_n] &\to A, \\ p &\mapsto p(a_1, a_2, \ldots, a_n) \end{aligned}$$

is an R-algebra morphism.

Proof. This is similar to the proof of Theorem 4.2.8, but more sophisticated due to the presence of multiple variables. Let f denote the map defined in Theorem 4.2.11. Again, the only nontrivial task is to show that f respects multiplication. We note that the definition of f easily yields that

$$f\left(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}\right) = a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n} \tag{81}$$

for every $(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$. We also observe that every $(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$

and $(j_1, j_2, \ldots, j_n) \in \mathbb{N}^n$ satisfy

$$\begin{aligned} &\left(a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n}\right) \cdot \left(a_1^{j_1} a_2^{j_2} \cdots a_n^{j_n}\right) \\ &= a_1^{i_1+j_1} a_2^{i_2+j_2} \cdots a_n^{i_n+j_n}. \end{aligned} \tag{82}$$

(This follows with a bit of work from the assumption that $a_1, a_2, \ldots, a_n$ mutually commute[131].)

To prove that f respects multiplication, we again use Lemma 4.2.9. This time, instead of proving (80), we need to prove the equality

$$f\left(\left(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}\right) \cdot \left(x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}\right)\right) = f\left(x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}\right) \cdot f\left(x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}\right)$$

[131] *Proof sketch.* Fix $(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$ and $(j_1, j_2, \ldots, j_n) \in \mathbb{N}^n$.

First, show that if a given element $b \in A$ commutes with each of k given elements $c_1, c_2, \ldots, c_k \in A$, then it also commutes with their product $c_1 c_2 \cdots c_k$. Use this to show that if b and c are two elements of A that commute, then b^i and c^j commute for all $i, j \in \mathbb{N}$. Conclude that each power $a_k^{i_k}$ commutes with all the powers $a_1^{j_1}, a_2^{j_2}, \ldots, a_{k-1}^{j_{k-1}}$ and thus also with their product $a_1^{j_1} a_2^{j_2} \cdots a_{k-1}^{j_{k-1}}$. In other words,

$$a_k^{i_k} \cdot \left(a_1^{j_1} a_2^{j_2} \cdots a_{k-1}^{j_{k-1}}\right) = \left(a_1^{j_1} a_2^{j_2} \cdots a_{k-1}^{j_{k-1}}\right) \cdot a_k^{i_k} \tag{83}$$

for each $k \in \{1, 2, \ldots, n\}$.

Now, you can show that the equality

$$\left(a_1^{i_1} a_2^{i_2} \cdots a_k^{i_k}\right) \cdot \left(a_1^{j_1} a_2^{j_2} \cdots a_k^{j_k}\right) = a_1^{i_1+j_1} a_2^{i_2+j_2} \cdots a_k^{i_k+j_k} \tag{84}$$

holds for each $k \in \{0, 1, \ldots, n\}$. Indeed, this equality can be proved by induction on k, where the induction step (from $k-1$ to k) proceeds by the following computation:

$$\begin{aligned} &\underbrace{\left(a_1^{i_1} a_2^{i_2} \cdots a_k^{i_k}\right)}_{= \left(a_1^{i_1} a_2^{i_2} \cdots a_{k-1}^{i_{k-1}}\right) a_k^{i_k}} \cdot \underbrace{\left(a_1^{j_1} a_2^{j_2} \cdots a_k^{j_k}\right)}_{= \left(a_1^{j_1} a_2^{j_2} \cdots a_{k-1}^{j_{k-1}}\right) a_k^{j_k}} \\ &= \left(a_1^{i_1} a_2^{i_2} \cdots a_{k-1}^{i_{k-1}}\right) \underbrace{a_k^{i_k} \cdot \left(a_1^{j_1} a_2^{j_2} \cdots a_{k-1}^{j_{k-1}}\right)}_{= \left(a_1^{j_1} a_2^{j_2} \cdots a_{k-1}^{j_{k-1}}\right) \cdot a_k^{i_k} \text{ (by (83))}} a_k^{j_k} \\ &= \underbrace{\left(a_1^{i_1} a_2^{i_2} \cdots a_{k-1}^{i_{k-1}}\right) \left(a_1^{j_1} a_2^{j_2} \cdots a_{k-1}^{j_{k-1}}\right)}_{= a_1^{i_1+j_1} a_2^{i_2+j_2} \cdots a_{k-1}^{i_{k-1}+j_{k-1}} \text{ (by the induction hypothesis)}} \cdot \underbrace{a_k^{i_k} a_k^{j_k}}_{= a_k^{i_k+j_k}} \\ &= \left(a_1^{i_1+j_1} a_2^{i_2+j_2} \cdots a_{k-1}^{i_{k-1}+j_{k-1}}\right) \cdot a_k^{i_k+j_k} = a_1^{i_1+j_1} a_2^{i_2+j_2} \cdots a_k^{i_k+j_k}. \end{aligned}$$

Thus, (84) is proved.

Now, applying (84) to $k = n$, we obtain

$$\left(a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n}\right) \cdot \left(a_1^{j_1} a_2^{j_2} \cdots a_n^{j_n}\right) = a_1^{i_1+j_1} a_2^{i_2+j_2} \cdots a_n^{i_n+j_n},$$

qed.

for all $(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n$ and $(j_1, j_2, \ldots, j_n) \in \mathbb{N}^n$. This equality follows by comparing

$$f\left(\underbrace{\left(x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\right)\cdot\left(x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}\right)}_{=x_1^{i_1+j_1}x_2^{i_2+j_2}\cdots x_n^{i_n+j_n}}\right) = f\left(x_1^{i_1+j_1}x_2^{i_2+j_2}\cdots x_n^{i_n+j_n}\right)$$

$$= a_1^{i_1+j_1}a_2^{i_2+j_2}\cdots a_n^{i_n+j_n} \qquad \text{(by (81))}$$

with

$$\underbrace{f\left(x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}\right)}_{\substack{=a_1^{i_1}a_2^{i_2}\cdots a_n^{i_n}\\ \text{(by (81))}}}\cdot\underbrace{f\left(x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}\right)}_{\substack{=a_1^{j_1}a_2^{j_2}\cdots a_n^{j_n}\\ \text{(by (81))}}} = \left(a_1^{i_1}a_2^{i_2}\cdots a_n^{i_n}\right)\cdot\left(a_1^{j_1}a_2^{j_2}\cdots a_n^{j_n}\right)$$

$$= a_1^{i_1+j_1}a_2^{i_2+j_2}\cdots a_n^{i_n+j_n} \qquad \text{(by (82))}.$$

Thus, we conclude (using Lemma 4.2.9) that f respects multiplication, and so the proof of Theorem 4.2.11 is easily completed. □

Exercise 4.2.1. Let $f \in R[x, y]$ be a polynomial in two variables x and y. Let $g = f(y, x)$. (This is the evaluation of f at y, x. In other words, g is the result of replacing each monomial $x^i y^j$ by $y^i x^j$ in f. For example, if $f = x^2 + 7xy - y$, then $g = y^2 + 7yx - x$.)

Prove that the difference $f - g$ is divisible by $x - y$ in the ring $R[x, y]$.

[**Hint:** Use linearity to reduce the general case to the case when f is a single monomial.]

Exercise 4.2.2. Let $n \in \mathbb{N}$. Let P be the multivariate polynomial ring $R[x_1, x_2, \ldots, x_n]$.

A polynomial $f \in P$ will be called **symmetric** if every permutation σ of the set $\{1, 2, \ldots, n\}$ satisfies

$$f\left(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}\right) = f(x_1, x_2, \ldots, x_n).$$

(In other words, a polynomial $f \in P$ is symmetric if and only if f remains unchanged whenever the indeterminates are permuted. For example, the polynomials $x_1 + x_2 + \cdots + x_n$ and $(3 + x_1)(3 + x_2)\cdots(3 + x_n)$ are symmetric, but the polynomial $x_1x_2 + x_2x_3 + \cdots + x_{n-1}x_n$ is not[132].)

Prove that the set of all symmetric polynomials $f \in P$ is an R-subalgebra of P.

[132] unless R is trivial or $n \leq 2$

4.2.6. Constant polynomials

Finally, a few more pieces of notation. We recall the notion of a constant element of a monoid ring (Convention 4.1.11). Since a polynomial ring is a monoid ring, we can apply it to polynomial rings, and obtain the following:

Convention 4.2.12. Let $n \in \mathbb{N}$. Then, we identify each $r \in R$ with $r \cdot 1 \in R[x_1, x_2, \ldots, x_n]$ (where 1 means the monomial $x_1^0 x_2^0 \cdots x_n^0$, which is the unity of $R[x_1, x_2, \ldots, x_n]$). This identification is harmless, and turns R into an R-subalgebra of $R[x_1, x_2, \ldots, x_n]$.

A polynomial $p \in R[x_1, x_2, \ldots, x_n]$ is said to be **constant** if it lies in this subalgebra (i.e., if it satisfies $p = r \cdot 1$ for some $r \in R$).

Example 4.2.13. The polynomial $3 = 3x^0 \in R[x]$ is constant, but the polynomial $3x = 3x^1$ is not.

4.2.7. Coefficients

By their definition, polynomials are R-linear combinations of monomials. Let us introduce a notation for the coefficients in these R-linear combinations:

Definition 4.2.14. Let $p \in R[x_1, x_2, \ldots, x_n]$ be a polynomial. Let $\mathfrak{m} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ be a monomial. Then, the **coefficient** of $\mathfrak{m}$ in p is the element $[\mathfrak{m}]\, p$ of R defined as follows: If we write p as

$$p = \sum_{(i_1, i_2, \ldots, i_n) \in \mathbb{N}^n} p_{i_1, i_2, \ldots, i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$$

with $p_{i_1, i_2, \ldots, i_n} \in R$, then we set

$$[\mathfrak{m}]\, p := p_{a_1, a_2, \ldots, a_n}.$$

Example 4.2.15.

(a) For univariate polynomials, we have

$$\left[x^3\right]\left((1+x)^5\right) = 10 \qquad \text{and} \qquad \left[x^7\right]\left((1+x)^5\right) = 0$$

(since $(1+x)^5 = 1 + 5x + 10x^2 + 10x^3 + 5x^4 + x^5$).

(b) For multivariate polynomials, we have

$$\left[x_1^2 x_2^3\right]\left((x_1+x_2)^5\right) = 10 \qquad \text{and} \qquad [x_1]\left((x_1+x_2)^5\right) = 0$$

(since $(x_1+x_2)^5 = x_1^5 + 5x_1^4 x_2 + 10x_1^3 x_2^2 + 10x_1^2 x_2^3 + 5x_1 x_2^4 + x_2^5$).

4.2.8. Renaming indeterminates

Often we will want to use symbols other than $x_1, x_2, \ldots, x_n$ for indeterminates. Thus, we allow ourselves to rename these indeterminates when it pleases us. For example, we can rename the indeterminates x_1 and x_2 of the polynomial ring $R[x_1, x_2]$ as x and y, so that the equations in Example 4.2.15 **(b)** become

$$\left[x^2y^3\right]\left((x+y)^5\right) = 10 \qquad \text{and} \qquad [x]\left((x+y)^5\right) = 0.$$

When we do this, we shall also rename the ring $R[x_1, x_2]$ as $R[x, y]$. More generally, we can have polynomial rings in any (finite) set of indeterminates; these rings are written by putting the names of these indeterminates into the square brackets. For example, $R[a, b, x, y]$ means a polynomial ring in four indeterminates named a, b, x, y.

Remark 4.2.16. This convention will serve us well in this course, but it eventually reveals itself to be inconvenient as you move into more advanced territory. In fact, it is better to think of polynomial rings with differently named indeterminates as being genuinely distinct rather than merely renamed versions of one another. For example, the two polynomial rings $R[x]$ and $R[y]$ are best regarded as distinct (even though they are isomorphic). This allows us to view them both as two **different** subrings of $R[x, y]$ (where the first one consists of all polynomials that don't contain y, such as $x^3 + 2x + 1$, whereas the second consists of all polynomials that don't contain x, such as $y^2 - 2y$). This viewpoint is rather natural, but cannot be rigorously justified as long as we view y as being the same indetermiate as x in all but name. Our definition of a multivariate polynomial ring $R[x_1, x_2, \ldots, x_n]$ (Definition 4.2.4) depends only on a ring R and a number n, so that it does not support distinguishing between different polynomial rings with the same R and the same n.

Thus, it is advisable to have a more flexible definition, which allows us to arbitrarily specify the names of the indeterminates. For example, we should be able to define the polynomial rings $R[x, y]$ and $R[y, z]$, which are each isomorphic to $R[x_1, x_2]$, but should not be treated as being the same ring (since the former has indeterminates x and y whereas the latter has indeterminates y and z).

Such a definition can be obtained by making some minor changes to our Definition 4.2.4. Namely, let S be any finite set of symbols, which we want to use as indeterminates (for example, we can have $S = \{x, y\}$ or $S = \{y, z\}$ or $S = \{\alpha, \mathbf{w}, \clubsuit\}$ if we are being ridiculous). Now, instead of using the monoid

$$C^{(n)} = \left\{x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \;\mid\; (a_1, a_2, \ldots, a_n) \in \mathbb{N}^n\right\}$$

as the set of monomials, we use the monoid

$$C^{(S)} := \left\{\prod_{s\in S} s^{a_s} \;\mid\; a_s \in \mathbb{N} \text{ for each } s \in S\right\},$$

where the "product" $\prod_{s \in S} s^{a_s}$ is just a formal symbol that encodes a family $(a_s)_{s \in S} \in \mathbb{N}^S$ of nonnegative integers (one for each element s of S). A monomial in $C^{(S)}$ is thus a "formal" product of the form $\prod_{s \in S} s^{a_s}$ (with each factor being a formal power of one of our indeterminates), and two such monomials are multiplied by the rule

$$\left(\prod_{s \in S} s^{a_s}\right) \cdot \left(\prod_{s \in S} s^{b_s}\right) = \prod_{s \in S} s^{a_s + b_s}.$$

The polynomial ring in the set S of indeterminates is then defined as the monoid ring $R\left[C^{(S)}\right]$ of this monoid $C^{(S)}$. We shall refer to such a ring as a **multivariate polynomial ring with named variables**, and just call it $R[S]$.

Thus, for a three-element set $S = \{x, y, z\}$, we obtain the ring $R[S] = R\left[C^{(S)}\right] = R[x, y, z]$, which is the polynomial ring over R in three variables that are named x, y, z. For instance, $x^2 + 7y^3z - xyz$ is a polynomial in this ring $R[x, y, z]$.

Now, of course, this polynomial ring $R[x, y, z]$ is isomorphic to $R[x_1, x_2, x_3]$ as an R-algebra (via the isomorphism that sends each monomial $x^a y^b z^c$ to $x_1^a x_2^b x_3^c$). More generally, we have $R[S] \cong R[x_1, x_2, \ldots, x_n]$ whenever S is an n-element set. Thus, the rings $R[x, y]$, $R[y, z]$ and $R[x_1, x_2]$ are all isomorphic, even though they are distinct. Hence, named variables do not introduce anything genuinely new to our theory as long as we are studying a single polynomial ring at a time. But their flexibility is helpful when working with several polynomial rings, e.g., by allowing us to treat $R[x]$ and $R[y]$ as two different subrings of $R[x, y]$.

This definition of the polynomial ring $R[S]$ with named variables can be easily adapted to infinite sets S as well, with a slight change: The monoid $C^{(S)}$ then needs to be defined as

$$\left\{ \prod_{s \in S} s^{a_s} \;\mid\; a_s \in \mathbb{N} \text{ for each } s \in S, \text{ and all but finitely many } s \in S \text{ satisfy } a_s = 0 \right\}.$$

(Thus, each monomial contains only finitely many indeterminates in nonzero powers.)

4.2.9. A remark on noncommutative R

Remark 4.2.17. We have been requiring that the ring R be commutative. However, it absolutely is possible to define polynomials over a noncommutative ring, if you are sufficiently careful. (In particular, this includes polynomials over matrix rings; these are rather useful in linear algebra. The inde-

terminates in such polynomials commute with all elements of R.) We have defined the notion of an R-algebra only for commutative rings R, but there are ways to adapt it to the general setup; alternatively, it is possible to redo the construction of the polynomial ring by hand without using R-algebras. See [ChaLoi21, §1.3] for the latter approach.

4.3. Univariate polynomials

4.3.1. Degrees and coefficients

Let us now take a closer look at univariate polynomials (which are the best-behaved among the polynomials).

As we recall, if $p \in R[x]$ is a polynomial, and if $i \in \mathbb{N}$, then $\left[x^i\right] p$ is the coefficient of x^i in p. That is, if p is written as $p = \sum_{j \in \mathbb{N}} p_j x^j$ with $p_j \in R$, then $\left[x^i\right] p = p_i$.

Definition 4.3.1. Let $p \in R[x]$ be a univariate polynomial.

(a) For any $i \in \mathbb{N}$, the coefficient $\left[x^i\right] p$ is also called the **x^i-coefficient** of p.

(b) If $p \neq 0$, then the **degree** of p is defined to be the largest $i \in \mathbb{N}$ such that $\left[x^i\right] p \neq 0$. The degree of the zero polynomial $0 \in R[x]$ is defined to be $-\infty$ (a symbol subject to the rules $-\infty < m$ and $-\infty + m = -\infty$ for any $m \in \mathbb{Z}$).

The degree of p is denoted by $\deg p$.

(c) If $p \neq 0$, then the **leading coefficient** of p is defined to be the coefficient $\left[x^{\deg p}\right] p \in R$.

(d) The polynomial p is said to be **monic** (or, as some say, **normalized**) if its leading coefficient is 1.

For example, the polynomial

$$5x^3 + 2x + 1 \in \mathbb{Q}[x]$$

has degree 3 and leading coefficient 5, and hence is not monic (since $5 \neq 1$). The polynomial

$$\overline{5}x^3 + \overline{2}x + \overline{1} \in (\mathbb{Z}/n)[x] \qquad \text{(for a given integer } n > 0\text{)}$$

has

- degree 3 if $n > 5$;

- degree 1 if $n = 5$ (because if $n = 5$, then the $\overline{5}x^3 = \overline{0}x^3$ term disappears);
- degree 3 if $n = 2, 3, 4$; and
- degree $-\infty$ if $n = 1$ (since all terms disappear if $n = 1$).

(Degrees are somewhat degenerate for trivial rings: If R is a trivial ring, then any polynomial in $R[x]$ is 0 and has degree $-\infty$.)

The polynomial $(1+x)^3 = 1 + 3x + 3x^2 + x^3$ is monic (i.e., has leading coefficient 1) and has degree 3.

Let me stress again that the zero polynomial $0 = 0x^0 + 0x^1 + 0x^2 + \cdots$ has degree $-\infty$ by definition. This $-\infty$ is not a number, but we agree that $-\infty$ is smaller than any integer and does not change if you add an integer to it (i.e., we have $(-\infty) + m = -\infty$ for any $m \in \mathbb{Z}$).

Here are some properties of degrees:

Remark 4.3.2. Let $n \in \mathbb{N}$. Then,

$$\begin{aligned}
&\{f \in R[x] \mid \deg f \leq n\} \\
&= \left\{f \in R[x] \mid f = a_0x^0 + a_1x^1 + \cdots + a_nx^n \text{ for some } a_0, a_1, \ldots, a_n \in R\right\} \\
&= \operatorname{span}\left(x^0, x^1, \ldots, x^n\right).
\end{aligned}$$

This is clearly an R-submodule of $R[x]$.

Corollary 4.3.3. Let $p, q \in R[x]$. Then,

$$\deg(p+q) \leq \max\{\deg p, \deg q\} \qquad \text{and} \tag{85}$$
$$\deg(p-q) \leq \max\{\deg p, \deg q\}. \tag{86}$$

Proof. Let $n = \max\{\deg p, \deg q\}$. Let N denote the subset $\{f \in R[x] \mid \deg f \leq n\}$ of $R[x]$. Then, we know from Remark 4.3.2 that N is an R-submodule of $R[x]$. Moreover, the definition of n shows that $\deg p \leq n$, so that $p \in N$. Similarly, $q \in N$. Hence, $p + q \in N$ (since N is an R-submodule of $R[x]$); in other words, $\deg(p+q) \leq n$. In other words, $\deg(p+q) \leq \max\{\deg p, \deg q\}$ (since $n = \max\{\deg p, \deg q\}$). Similarly, we can find $\deg(p-q) \leq \max\{\deg p, \deg q\}$. This proves Corollary 4.3.3. □

Remark 4.3.4. The polynomials of degree ≤ 0 are precisely the constant polynomials – i.e., the elements of R (embedded into $R[x]$ as explained in Convention 4.2.12).

The following proposition collects some properties of products of univariate polynomials:

Proposition 4.3.5. Let $p, q \in R[x]$. Then:

(a) We have $\deg(pq) \leq \deg p + \deg q$.

(b) We have $\deg(pq) = \deg p + \deg q$ if $p \neq 0$ and the leading coefficient of p is a unit.

(c) We have $\deg(pq) = \deg p + \deg q$ if R is an integral domain.

(d) If $n, m \in \mathbb{N}$ satisfy $n \geq \deg p$ and $m \geq \deg q$, then

$$\left[x^{n+m}\right](pq) = \left[x^n\right](p) \cdot \left[x^m\right](q).$$

(e) If $pq = 0$ and $p \neq 0$ and if the leading coefficient of p is a unit, then $q = 0$.

Corollary 4.3.6. If R is an integral domain, then the polynomial ring $R[x]$ is an integral domain.

Proof of Proposition 4.3.5. We will give an informal "proof by example". Rigorous arguments can be found in various places[133].

Let p and q be two polynomials of degrees $\deg p = 2$ and $\deg q = 3$. Write p and q as $p = ax^2 + bx + c$ and $q = dx^3 + ex^2 + fx + g$ (with $a, b, c, \ldots, g \in R$). Then,

$$\begin{aligned} pq &= \left(ax^2 + bx + c\right)\left(dx^3 + ex^2 + fx + g\right) \\ &= adx^5 + (\text{lower powers of } x). \end{aligned} \tag{87}$$

Thus, $\deg(pq) \leq 5 = 2 + 3 = \deg p + \deg q$. This proves Proposition 4.3.5 **(a)**.

Moreover, $a \neq 0$ (since $\deg p = 2$) and $d \neq 0$ (since $\deg q = 3$). If R is an integral domain, then this entails $ad \neq 0$ and therefore $\deg(pq) = 5$ (by (87)). This proves Proposition 4.3.5 **(c)**. On the other hand, if a is a unit, then we also have $ad \neq 0$ (because otherwise, we would have $ad = 0$ and thus $a^{-1}\underbrace{ad}_{=0} = 0$, which would contradict $a^{-1}ad = d \neq 0$) and therefore $\deg(pq) = 5$ (by (87)). This proves Proposition 4.3.5 **(b)** (since a is the leading coefficient of p).

The equality (87) shows that the coefficient of x^5 in pq is ad, and no higher powers of x than x^5 appear in pq. That is, we have $\left[x^5\right](pq) = \underbrace{a}_{=[x^2](p)}\underbrace{d}_{=[x^3](q)} =$

[133] Can they? I'm not so sure any more; apparently everyone just handwaves them away or leaves them to the reader (e.g., Bourbaki writes about part **(a)** that "the proof is immediate"). A while ago I have written up proofs for parts **(a)** and **(d)** in [Grinbe20] (where they appear as parts **(a)** and **(b)** of Lemma 3.12), albeit only in the particular case when p is monic (but the proofs can easily be generalized). A generalization of parts **(b)** and **(c)** also appears in [ChaLoi21, Proposition (1.3.12)].

$\left[x^2\right](p) \cdot \left[x^3\right](q)$, and we have $\left[x^i\right](pq) = 0$ for all $i > 5$. This quickly yields Proposition 4.3.5 **(d)**.

To prove Proposition 4.3.5 **(e)**, we assume the contrary. Thus, $pq = 0$ and $p \neq 0$ and the leading coefficient of p is a unit, but $q \neq 0$. Then, Proposition 4.3.5 **(b)** yields $\deg(pq) = \underbrace{\deg p}_{\geq 0} + \underbrace{\deg q}_{\geq 0} \geq 0$. However, $pq = 0$, so $\deg(pq) = \deg 0 = -\infty < 0$. These two inequalities clearly contradict each other, and our proof of Proposition 4.3.5 **(e)** is complete. □

Proof of Corollary 4.3.6. Assume that R is an integral domain. Let $p, q \in R[x]$ be nonzero. Then, Proposition 4.3.5 **(c)** yields $\deg(pq) = \underbrace{\deg p}_{\geq 0} + \underbrace{\deg q}_{\geq 0} \geq 0$, and thus $pq \neq 0$ (since $pq = 0$ would yield $\deg(pq) = \deg 0 = -\infty < 0$). Thus, we have shown that $pq \neq 0$ for any nonzero $p, q \in R[x]$. In other words, $R[x]$ is an integral domain. □

If R is not an integral domain, then polynomials over R can behave rather strangely. For example, over $\mathbb{Z}/4$, we have

$$\left(\overline{1} + \overline{2}x\right)^2 = \overline{1} + \overline{4}x + \overline{4}x^2 = \overline{1} \qquad \left(\text{since } \overline{4} = \overline{0}\right).$$

So the degree of a polynomial can decrease when it is squared!

Exercise 4.3.1. Let $n \in \mathbb{N}$. Prove that we have $x^2 + x + 1 \mid x^{2n} + x^n + 1$ in the polynomial ring $\mathbb{Z}[x]$ if and only if $3 \nmid n$ in $\mathbb{Z}$.

[**Hint:** First show that $x^3 \equiv 1 \bmod x^2 + x + 1$ in the ring $\mathbb{Z}[x]$. Here, we are using the notation $a \equiv b \bmod c$ (spoken "a is congruent to b modulo c") for $c \mid a - b$ whenever a, b, c are three elements of a commutative ring R. Congruences in R are a straightforward generalization of congruences of integers (which are known from elementary number theory), and behave just as nicely; in particular, they can be added, subtracted and multiplied.]

The equality $\left(\overline{1} + \overline{2}x\right)^2 = \overline{1}$ in $\mathbb{Z}/4$ that we observed above is surprising not only because of the strange "loss of degree" that happens when $\overline{1} + \overline{2}x$ is squared, but also for another reason: It shows that the non-constant polynomial $\overline{1} + \overline{2}x$ in $(\mathbb{Z}/4)[x]$ is actually a unit of $(\mathbb{Z}/4)[x]$! As Proposition 4.3.5 **(c)** explains, this cannot happen for polynomials over an integral domain. The following exercise characterizes precisely when this happens:

Exercise 4.3.2. Let R be a commutative ring. Let $f \in R[x]$ be a polynomial. Recall that the notation $\left[x^i\right] f$ stands for the coefficient of the monomial x^i in f.

Prove that f is a unit of the ring $R[x]$ if and only if

- the coefficient $\left[x^0\right] f$ is a unit of R, and
- all the remaining coefficients $\left[x^1\right] f$, $\left[x^2\right] f$, $\left[x^3\right] f$, ... of f are nilpotent.

[**Hint:** Exercise 2.8.6 **(c)** shows that the nilpotent elements of $R[x]$ form an ideal, whereas Exercise 2.5.9 **(b)** shows that the difference of a unit and a nilpotent element is always a unit (in $R[x]$). This should help with the "if" direction. For the "only if" direction, let $f = f_0x^0 + f_1x^1 + \cdots + f_nx^n \in R[x]$ be a unit and $g = g_0x^0 + g_1x^1 + \cdots + g_mx^m \in R[x]$ be its inverse. Use induction on r to show that $f_n^{r+1}g_{m-r} = 0$ for each $r \in \{0, 1, \ldots, m\}$. Use this to conclude that f_n is nilpotent.]

4.3.2. Division with remainder

The most important feature of univariate polynomials is division with remainder:

Theorem 4.3.7 (Division-with-remainder theorem for polynomials)**.** Let $b \in R[x]$ be a nonzero polynomial whose leading coefficient is a unit. Let $a \in R[x]$ be any polynomial.

(a) Then, there is a **unique** pair (q, r) of polynomials in $R[x]$ such that

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b.$$

(b) Moreover, this pair satisfies $\deg q \leq \deg a - \deg b$.

The polynomials q and r in Theorem 4.3.7 are called the **quotient** and the **remainder** obtained when dividing a by b. Note that if $\deg a < \deg b$, then the quotient q is 0 whereas the remainder r is a. The quotient and the remainder become interesting when $\deg a \geq \deg b$.

Example 4.3.8. Let $R = \mathbb{Z}$ and $a = 3x^4 + x^2 + 6x - 2$ and $b = x^2 - 3x + 1$. Then, Theorem 4.3.7 **(a)** shows that there is a **unique** pair (q, r) of polynomials in $R[x]$ such that

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b.$$

This pair (q, r) is $\left(3x^2 + 9x + 25,\ 72x - 27\right)$. Indeed, if you set $q = 3x^2 + 9x + 25$ and $r = 72x - 27$, then the equality $a = qb + r$ can be verified by a straightforward computation, whereas the inequality $\deg r < \deg b$ is obvious. Thus, the quotient obtained when dividing a by b is $q = 3x^2 + 9x + 25$, and the remainder is $r = 72x - 27$.

Example 4.3.9. Let us give a **non-example:** Let $R = \mathbb{Z}$ and $b = 2$ (a constant polynomial) and $a = x$. The leading coefficient of b is not a unit (since 2 is not a unit in $\mathbb{Z}$), so we don't expect Theorem 4.3.7 to hold. And indeed: we cannot write $a = qb + r$ with $\deg r < \deg b$. Indeed, this would mean $x = q \cdot 2 + r$ with $\deg r < 0$ (since the constant polynomial 2 has degree

$\deg 2 = 0$); but this is impossible, since this would entail $x = q \cdot 2$, which would contradict the fact that x is not divisible by 2.

Instead of proving Theorem 4.3.7 directly, we will first show the particular case in which b is required to be monic, and then use it to derive the general case. The particular case is the following lemma:

Lemma 4.3.10. Let $b \in R[x]$ be a monic polynomial. Let $a \in R[x]$ be any polynomial.

(a) Then, there is a **unique** pair (q, r) of polynomials in $R[x]$ such that

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b.$$

(b) Moreover, this pair satisfies $\deg q \leq \deg a - \deg b$.

Proof. **(a)** Again, we shall give a proof by example. (For a rigorous proof, see [Grinbe20, Theorem 3.16 and Lemma 3.19] or [Ford22, Theorem 3.6.4] or [ChaLoi21, Theorem (1.3.15)] or [Knapp16, Proposition 1.12] or [DumFoo04, §9.2, Theorem 3]. Note that some of these sources assume that R is a field; however, the proofs easily adapt to our general case.)

We are doing a proof by example, so let us assume that $\deg a = 3$ and $\deg b = 2$. Thus, we can write a and b as $a = cx^3 + dx^2 + ex + f$ and $b = x^2 + gx + h$ for some $c, d, e, f, g, h \in R$ (since b is monic).

Now, we repeatedly subtract appropriate multiples of b from a in order to decrease its degree:

$$\begin{aligned}
& a = cx^3 + dx^2 + ex + f \\
\Longrightarrow\ & a - (cx)\, b = (d - cg)\, x^2 + (e - ch)\, x + f \\
& \qquad \Big(\text{here, we have subtracted } (cx)\, b \text{ to kill off the } cx^3 \text{ term}\Big) \\
\Longrightarrow\ & a - (cx)\, b - (d - cg)\, b = (e - ch - (d - cg)\, g)\, x + (f - (d - cg)\, h) \\
& \qquad \left(\begin{array}{c} \text{here, we have subtracted } (d - cg)\, b \text{ to kill off} \\ \text{the } (d - cg)\, x^2 \text{ term} \end{array}\right).
\end{aligned}$$

Thus,

$$\begin{aligned}
a &= (cx)\, b + (d - cg)\, b + (e - ch - (d - cg)\, g)\, x + (f - (d - cg)\, h) \\
&= (cx + (d - cg))\, b + (e - ch - (d - cg)\, g)\, x + (f - (d - cg)\, h).
\end{aligned}$$

Setting $q := cx + (d - cg)$ and $r := (e - ch - (d - cg)\, g)\, x + (f - (d - cg)\, h)$, we can rewrite this as

$$a = qb + r.$$

Note that $\deg r < \deg b$ (since any polynomial of degree $\geq \deg b$ could still be reduced further by subtracting a multiple of b from it).

Thus we have found a pair (q, r) of polynomials satisfying

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b.$$

It remains to prove its uniqueness. In other words, we have to prove that if (q_1, r_1) and (q_2, r_2) are two pairs of polynomials satisfying

$$\begin{array}{llll} a = q_1 b + r_1 & \text{and} & \deg r_1 < \deg b & \text{and} \\ a = q_2 b + r_2 & \text{and} & \deg r_2 < \deg b, & \end{array}$$

then $(q_1, r_1) = (q_2, r_2)$. To prove this, we fix two such pairs (q_1, r_1) and (q_2, r_2). Then, we have

$$q_1 b + r_1 = a = q_2 b + r_2,$$

so that $r_1 - r_2 = q_2 b - q_1 b = b\left(q_2 - q_1\right)$. Hence, $b\left(q_2 - q_1\right) = r_1 - r_2$, so that

$$\begin{aligned} \deg\left(b\left(q_2 - q_1\right)\right) &= \deg\left(r_1 - r_2\right) \leq \max\left\{\deg r_1, \deg r_2\right\} \qquad \text{(by (86))} \\ &< \deg b \qquad \left(\text{since } \deg r_1 < \deg b \text{ and } \deg r_2 < \deg b\right). \end{aligned}$$

However, the leading coefficient of b is a unit[134]. Hence, if the polynomial $q_2 - q_1$ was nonzero, then Proposition 4.3.5 **(b)** would entail

$$\deg\left(b\left(q_2 - q_1\right)\right) = \deg b + \underbrace{\deg\left(q_2 - q_1\right)}_{\geq 0} \geq \deg b,$$

which would contradict $\deg\left(b\left(q_2 - q_1\right)\right) < \deg b$. So $q_2 - q_1$ must be zero. In other words, $q_2 - q_1 = 0$, so that $q_1 = q_2$. Moreover, $r_1 - r_2 = b\underbrace{\left(q_2 - q_1\right)}_{=0} = 0$, so that $r_1 = r_2$. Hence, $(q_1, r_1) = (q_2, r_2)$. This completes the proof of the uniqueness of (q, r). Thus, Lemma 4.3.10 **(a)** is proved.

(b) You can obtain Lemma 4.3.10 **(b)** by a careful analysis of the construction of the pair (q, r) in our proof of part **(a)**. Indeed, each of the terms of q was originally a factor that we multiplied with b in order to reduce a; however, the highest power of x in a was $x^{\deg a}$, so the factors we used did not contain any powers of x higher than $x^{\deg a - \deg b}$.

Alternatively, you can prove Lemma 4.3.10 **(b)** independently of part **(a)**: Let (q, r) be a pair of polynomials in $R[x]$ such that

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b.$$

We must prove that $\deg q \leq \deg a - \deg b$. Assume the contrary. Thus, $\deg q > \deg a - \deg b$. Therefore, in particular, $q \neq 0$ (since $q = 0$ would entail $\deg q =$

[134] Indeed, this coefficient is 1, since b is monic.

$\deg 0 = -\infty \leq \deg a - \deg b$), so that $\deg q \geq 0$. However, the leading coefficient of b is a unit[135]; thus, Proposition 4.3.5 **(b)** yields that

$$\deg(bq) = \deg b + \deg q > \deg a \qquad (\text{since } \deg q > \deg a - \deg b).$$

Also,

$$\deg(bq) = \deg b + \underbrace{\deg q}_{\geq 0} \geq \deg b > \deg r \qquad (\text{since } \deg r < \deg b).$$

Combining these two inequalities, we obtain

$$\deg(bq) > \max\{\deg a, \deg r\}.$$

But from $a = qb + r$, we obtain $a - r = qb = bq$, so that $bq = a - r$. Hence,

$$\deg(bq) = \deg(a - r) \leq \max\{\deg a, \deg r\} \qquad (\text{by (86)}),$$

which contradicts $\deg(bq) > \max\{\deg a, \deg r\}$. This contradiction shows that our assumption was wrong; thus, Lemma 4.3.10 **(b)** is proven. □

We can now prove the general case:

Proof of Theorem 4.3.7. **(a)** As in our above proof of Lemma 4.3.10 **(a)**, we can show that the pair (q, r) is unique. It remains to show that this pair exists.

Let u be the leading coefficient of b. Then, u is a unit (by assumption), and thus has an inverse u^{-1}. Scaling the polynomial b by u^{-1} results in a new polynomial $u^{-1}b$, which has leading coefficient $u^{-1}u$ (since the leading coefficient u of b gets multiplied by u^{-1}) and thus is monic (since $u^{-1}u = 1$). Hence, we can apply Lemma 4.3.10 **(a)** to $u^{-1}b$ instead of b. As a result, we conclude that there is a **unique** pair (q, r) of polynomials in $R[x]$ such that

$$a = q\left(u^{-1}b\right) + r \qquad \text{and} \qquad \deg r < \deg\left(u^{-1}b\right).$$

Let us denote this pair (q, r) by $(\widetilde{q}, \widetilde{r})$. Thus, $(\widetilde{q}, \widetilde{r})$ is a pair of polynomials in $R[x]$ and satisfies

$$a = \widetilde{q}\left(u^{-1}b\right) + \widetilde{r} \qquad \text{and} \qquad \deg \widetilde{r} < \deg\left(u^{-1}b\right).$$

Now,

$$a = \widetilde{q}\left(u^{-1}b\right) + \widetilde{r} = \left(u^{-1}\widetilde{q}\right)b + \widetilde{r}$$

and $\deg \widetilde{r} < \deg\left(u^{-1}b\right) \leq \deg b$ (because scaling a polynomial cannot increase its degree). Hence, pair (q, r) of polynomials in $R[x]$ such that

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b$$

[135] Indeed, this coefficient is 1, since b is monic.

(namely, the pair $(q,r) = \left(u^{-1}\widetilde{q}, \widetilde{r}\right)$). Since we have already shown that such a pair is unique, we thus have finished proving Theorem 4.3.7 **(a)**.

(b) Our above proof of Lemma 4.3.10 **(b)** (specifically, the "alternative" proof that is independent of part **(a)**) applies to Theorem 4.3.7 **(b)** as well. □

We record an automatic corollary of Theorem 4.3.7:

Corollary 4.3.11. Let F be a field. Let $b \in F[x]$ be any nonzero polynomial. Let $a \in F[x]$ be any polynomial.

(a) Then, there is a **unique** pair (q,r) of polynomials in $F[x]$ such that

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b.$$

(b) Moreover, this pair satisfies $\deg q \leq \deg a - \deg b$.

Proof. The polynomial b is nonzero; thus, its leading coefficient is a unit (since any nonzero element of the field F is a unit). Hence, Theorem 4.3.7 applies (to $R = F$). □

The following simple proposition is the polynomial analogue of the classical fact that a positive integer b divides an integer a if and only if the remainder that a leaves when divided by b is 0:

Proposition 4.3.12. Let $b \in R[x]$ be a nonzero polynomial whose leading coefficient is a unit. Let $a \in R[x]$ be any polynomial. Let q and r be the quotient and the remainder obtained when dividing a by b. Then, we have the logical equivalence $(r = 0) \iff (b \mid a \text{ in } R[x])$.

Proof. The definition of quotient and remainder yields $a = qb + r$. Hence, if $r = 0$, then $a = qb + \underbrace{r}_{=0} = qb$ and thus $b \mid a$ in $R[x]$. This proves the "$\Longrightarrow$" direction of the required equivalence. It thus remains to prove the "$\Longleftarrow$" direction.

So we assume that $b \mid a$ in $R[x]$. We need to show that $r = 0$.

We have assumed $b \mid a$ in $R[x]$. In other words, there exists a $c \in R[x]$ such that $a = cb$. Consider this c. We have $a = cb = bc = bc + 0$ and $\deg 0 = -\infty < \deg b$. Thus, $(c, 0)$ is a pair $(\widetilde{q}, \widetilde{r})$ of polynomials in $F[x]$ such that $a = \widetilde{q}b + \widetilde{r}$ and $\deg \widetilde{r} < \deg b$. But (q,r) is also such a pair (by the definition of quotient and remainder). However, Lemma 4.3.10 **(a)** shows that there is a **unique** such pair. In particular, any two such pairs must be identical. Thus, the two pairs (q,r) and $(c,0)$ must be identical. That is, we have $q = c$ and $r = 0$. In particular, $r = 0$; this completes the proof of the "$\Longleftarrow$" direction. Proposition 4.3.12 is thus proven. □

Exercise 4.3.3. Let R be any commutative ring. Let $n \in \mathbb{N}$.

(a) Find the quotient and the remainder obtained when dividing $(x+1)^n$ by x (in the polynomial ring $R[x]$).

(b) Find the quotient and the remainder obtained when dividing x^n by $x-1$.

(c) Find the remainder obtained when dividing $(x+1)^n$ by $x-1$.

[**Hint:** "Finding" a polynomial here means computing its coefficients. For instance, in part **(a)**, the coefficients of the quotient will be certain binomial coefficients. I am deliberately not asking for the quotient in part **(c)**, since I don't know a closed form for its coefficients that doesn't use summation signs.]

Exercise 4.3.4. Let R be any commutative ring. Let $n \in \mathbb{N}$.

Prove that the remainder obtained when dividing x^n by $(x-1)^2$ in the polynomial ring $R[x]$ is $nx - n + 1$.

Exercise 4.3.5. Let R be any commutative ring. Let n be a positive integer.

(a) Prove that $(x-1)^3 \mid x^{2n} - nx^{n+1} + nx^{n-1} - 1$ in $R[x]$.

(b) Prove that $x+1 \mid x^{2n} - nx^{n+1} + nx^{n-1} - 1$ in $R[x]$.

(c) Prove that $(x+1)^3 \mid x^{2n} - nx^{n+1} + nx^{n-1} - 1$ in $R[x]$ if n is odd.

Exercise 4.3.6. Let R be any commutative ring. Let $n \in \mathbb{N}$.

In terms of the Fibonacci numbers (Definition 2.3.4), find the quotient and the remainder obtained when dividing x^n by $x^2 - x - 1$.

[**Hint:** Compute them (e.g.) for $n = 10$, and prove the pattern you discover.]

Exercise 4.3.7. Let $a \in \mathbb{Z}[x]$ and $b \in \mathbb{Z}[x]$ be two polynomials, with b being nonzero. Without requiring anything about the leading coefficient of b, we cannot apply Theorem 4.3.7, so we don't know whether there exists a pair (q, r) of polynomials in $\mathbb{Z}[x]$ such that

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b.$$

Nevertheless, such a pair might exist.

(a) Does such a pair exist when $a = 3x^2 + 1$ and $b = 3x - 1$?

(b) Does such a pair exist when $a = 3x^3 + 1$ and $b = 3x - 1$?

(c) Does such a pair exist when $a = 3x^2 + 2x$ and $b = 3x - 1$?

(Make sure to prove your claims!)

The following exercise partially generalizes Theorem 4.3.7 to the case when the leading coefficient of b is not (necessarily) a unit:

Exercise 4.3.8. Let R be any commutative ring. Let $b \in R[x]$ be a nonzero polynomial, and let $\lambda \in R$ be its leading coefficient. Let $a \in R[x]$ be any polynomial such that $\deg a \geq \deg b$. Prove that there is a pair (q, r) of polynomials in $R[x]$ such that

$$\lambda^{\deg a - \deg b + 1} a = qb + r \qquad \text{and}$$
$$\deg r < \deg b \qquad \text{and} \qquad \deg q \leq \deg a - \deg b.$$

(Note that we can no longer claim that this pair (q, r) is unique.)

4.3.3. Roots

We shall now discuss roots of polynomials.

Definition 4.3.13. Let A be an R-algebra. Let $f \in R[x]$. An element $a \in A$ is said to be a **root** of f if $f(a) = 0$ (that is, $f[a] = 0$).

This is a rather wide notion of roots. For example, the matrix $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in \mathbb{Q}^{2\times 2}$ is a root of the polynomial $x^2 \in \mathbb{Q}[x]$, since the square of this matrix is 0. For another example, the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \mathbb{Q}^{2\times 2}$ is a root of the polynomial $x^2 - 1 \in \mathbb{Q}[x]$, since

$$\left(x^2 - 1\right)\left[\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 - 1_{\mathbb{Q}^{2\times 2}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} = 0_{\mathbb{Q}^{2\times 2}}.$$

The simplest kind of roots, however, are those that lie in the original ring R. Here are some of their properties:

Proposition 4.3.14. Let f be a polynomial in $R[x]$. Let $a \in R$. Then, we have the following logical equivalence:

$$(a \text{ is a root of } f) \iff (x - a \mid f \text{ in } R[x]).$$

Proof of Proposition 4.3.14. The polynomial $x - a$ is monic. Hence, Lemma 4.3.10 **(a)** (applied to f and $x - a$ instead of a and b) shows that there is a **unique** pair (q, r) of polynomials in $R[x]$ such that

$$f = q \cdot (x - a) + r \qquad \text{and} \qquad \deg r < \deg(x - a).$$

Consider this pair (q, r). From $\deg r < \deg(x-a) = 1$, we see that $\deg r \leq 0$, which means that r is a constant. In other words, $r \in R$.

Now, let us substitute a for x on both sides of the equality $f = q \cdot (x-a) + r$. Thus we get

$$f[a] = q[a] \cdot (a-a) + r[a]. \tag{88}$$

It is worth going through the proof of this equality in some more detail. Namely, we have $f = q \cdot (x-a) + r$, so that

$$\begin{aligned} f[a] &= (q \cdot (x-a) + r)[a] \\ &= (q \cdot (x-a))[a] + r[a] \qquad \left(\begin{array}{c} \text{by (76), applied to } R, q \cdot (x-a) \text{ and } r \\ \text{instead of } A, p \text{ and } q \end{array} \right) \\ &= q[a] \cdot \underbrace{(x-a)[a]}_{\substack{=a-a \\ \text{(by the definition} \\ \text{of an evaluation)}}} + r[a] \qquad \left(\begin{array}{c} \text{by (75), applied to } R, q \text{ and } x-a \\ \text{instead of } A, p \text{ and } q \end{array} \right) \\ &= q[a] \cdot (a-a) + r[a]. \end{aligned}$$

Thus, (88) has been proven in detail.

Now, (88) becomes

$$f[a] = q[a] \cdot \underbrace{(a-a)}_{=0} + r[a] = r[a] = r \qquad (\text{since } r \text{ is a constant}).$$

Now, we have the following chain of equivalences:

$$\begin{aligned} (a \text{ is a root of } f) &\iff (f[a] = 0) \qquad (\text{by the definition of a root}) \\ &\iff (r = 0) \qquad (\text{since } f[a] = r) \\ &\iff (x-a \mid f \text{ in } R[x]) \end{aligned}$$

(by Proposition 4.3.12, applied to $x-a$ and f instead of b and a). This proves Proposition 4.3.14. □

The following theorem is often known as the **easy half of the FTA (Fundamental Theorem of Algebra)**:

Theorem 4.3.15. Let R be an integral domain. Let $n \in \mathbb{N}$. Then, any nonzero polynomial $f \in R[x]$ of degree $\leq n$ has at most n roots in R. (We are not counting the roots with multiplicity here.)

Proof. We induct on n. The *base case* ($n = 0$) is obvious (indeed, a nonzero polynomial of degree ≤ 0 must be constant, and thus cannot have any roots to begin with).

Induction step: Let m be a positive integer. Assume (as the induction hypothesis) that Theorem 4.3.15 holds for $n = m-1$. We must prove that Theorem 4.3.15 holds for $n = m$.

So let $f \in R[x]$ be a nonzero polynomial of degree $\leq m$. We must prove that f has at most m roots in R.

Indeed, assume the contrary. Thus, f has $m+1$ distinct roots $a_1, a_2, \ldots, a_{m+1}$ in R (and possibly more, but we will only need these $m+1$).

In particular, a_{m+1} is a root of f, so that we have $x - a_{m+1} \mid f$ in $R[x]$ (by Proposition 4.3.14, applied to $a = a_{m+1}$). That is, there exists a polynomial $q \in R[x]$ such that $f = (x - a_{m+1}) \cdot q$. Consider this q. Now, it is easy to see that $a_1, a_2, \ldots, a_m$ are roots of q (indeed, this uses the fact that $a_1, a_2, \ldots, a_{m+1}$ are **distinct** roots of f and that R is an integral domain[136]). Hence, the polynomial q has at least m roots in R (since these m roots $a_1, a_2, \ldots, a_m$ are distinct). Also, the polynomial q is nonzero (since otherwise, we would have $q = 0$ and thus $f = (x - a_{m+1}) \cdot \underbrace{q}_{=0} = 0$, contradicting the fact that f is nonzero).

However, Proposition 4.3.5 **(c)** (or Proposition 4.3.5 **(b)**, if you wish) yields

$$\deg\left((x - a_{m+1}) \cdot q\right) = \underbrace{\deg\left(x - a_{m+1}\right)}_{=1} + \deg q = 1 + \deg q,$$

so that

$$\deg q = \deg\left(\underbrace{(x - a_{m+1}) \cdot q}_{=f}\right) - 1 = \underbrace{\deg f}_{\substack{\leq m \\ \text{(since } f \text{ has degree } \leq m\text{)}}} - 1 \leq m - 1.$$

In other words, the polynomial q has degree $\leq m - 1$. Hence, by the induction hypothesis, we can apply Theorem 4.3.15 to q and $m-1$ instead of f and n. We thus conclude that q has at most $m - 1$ roots in R. This contradicts the fact that q has at least m roots in R (which we have shown above). This contradiction completes the induction step, and so we are done proving Theorem 4.3.15. □

Remark 4.3.16. Theorem 4.3.15 can fail if R is not an integral domain. For instance, the polynomial $x^2 - \overline{1} \in (\mathbb{Z}/8)[x]$ has degree 2 but has 4 roots in $\mathbb{Z}/8$ (namely, $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$).

[136] Here is the proof in detail: Let $i \in \{1, 2, \ldots, m\}$. We must show that a_i is a root of q. Note that $i \neq m+1$ (since $i \in \{1, 2, \ldots, m\}$) and thus $a_i \neq a_{m+1}$ (since $a_1, a_2, \ldots, a_{m+1}$ are distinct). Substituting a_i for x in the equality $f = (x - a_{m+1}) \cdot q$, we find

$$f[a_i] = (a_i - a_{m+1}) \cdot q[a_i]$$

(formally speaking, this relies on a similar argument as we used to prove (88)). Hence,

$$(a_i - a_{m+1}) \cdot q[a_i] = f[a_i] = 0 \qquad \text{(since } a_i \text{ is a root of } f\text{)}.$$

Since R is an integral domain, this entails that we have $a_i - a_{m+1} = 0$ or $q[a_i] = 0$. Since $a_i - a_{m+1} = 0$ is impossible (because $a_i \neq a_{m+1}$), we thus conclude that $q[a_i] = 0$. In other words, a_i is a root of q. Qed.

Remark 4.3.17. Proposition 4.3.14 and Theorem 4.3.15 are only concerned with roots in the original ring R. As stated, they don't apply to roots that belong to other R-algebras A. And indeed, Theorem 4.3.15 fails quite dramatically if we try to apply it to other R-algebras A. For instance, the polynomial $x^2 + 1 \in \mathbb{R}[x]$ has infinitely many roots in the ring of quaternions $\mathbb{H}$ (see Exercise 2.2.6 **(b)**). Proposition 4.3.14 can be extended to commutative R-algebras A (thus allowing $a \in A$ instead of $a \in R$, and "converting" the polynomial f into a polynomial in $A[x]$), although this would not make it significantly more general, since we can **already** apply it to A instead of R in such case (see Exercise 4.3.10).

Remark 4.3.18. Let us say a few words about the weird name of Theorem 4.3.15. The famous **fundamental theorem of algebra** (short: **FTA**) says that any polynomial of degree n in $\mathbb{C}[x]$ has exactly n roots in $\mathbb{C}$, if we count the roots with multiplicity. Despite its name, this theorem is not actually algebraic in nature, since it relies on the analytic structure of the complex numbers (and the underlying real numbers), and does not hold (e.g.) for the Gaussian rationals $\mathbb{Q}[i]$. Accordingly, each proof of the FTA requires at least a little bit of real analysis (and sometimes far more than a little bit). Various proofs can be found in [LaNaSc16, Chapter 3], [Aluffi16, Theorem 7.1], [Knapp16, Chapter IX, §10], [Warner90, Theorem 44.8], [Steinb06, Theorem 11.6.7] and many other places (some of which prove weaker-sounding but equivalent versions of the result); more exotic proofs are listed in `https://mathoverflow.net/questions/10535` .

However, one "half" of the FTA – namely, the claim that a polynomial of degree n in $\mathbb{C}[x]$ always has **at most** n roots in $\mathbb{C}$ – actually can be proved algebraically, and holds not just for $\mathbb{C}$ but also for any integral domain R in its stead. If we drop the notion of multiplicities, then this "half" is precisely Theorem 4.3.15. Thus, Theorem 4.3.15 is called the "easy half of the FTA". Despite being the easy half, it is surprisingly useful, and we will see some of its applications in the following subsections. In comparison, the "hard half of the FTA" (the part that really requires $\mathbb{C}$) is rarely used in abstract algebra (since algebraists prefer to work in settings more general than $\mathbb{C}$), but it is important (e.g.) in complex linear algebra, where it is responsible (e.g.) for the fact that each $n \times n$-matrix over $\mathbb{C}$ has n eigenvalues (counted with multiplicities). Thus, the name "FTA" should be regarded as somewhat of a historical artefact.

Exercise 4.3.9. Let R and S be two commutative rings. Let $f : R \to S$ be a ring morphism. Let $f[x]$ denote the map

$$\begin{aligned} & R[x] \to S[x], \\ & \sum_{i \in \mathbb{N}} r_i x^i \mapsto \sum_{i \in \mathbb{N}} f(r_i) x^i \qquad \text{(for all } r_i \in R\text{)}. \end{aligned}$$

(This map transforms a polynomial by applying f to each of its coefficients.)

Prove that $f[x]$ is a ring morphism.

Exercise 4.3.10. Let R be a commutative ring, and let A be a commutative R-algebra. For each polynomial $f = \sum_{i \in \mathbb{N}} f_i x^i \in R[x]$ (with $f_i \in R$), we let f_A denote the polynomial $\sum_{i \in \mathbb{N}} (f_i \cdot 1_A) x^i \in A[x]$ (which is simply the polynomial f, with each coefficient "converted" into an element of A using the standard map $R \to A$, $r \mapsto r \cdot 1_A$).

(a) Prove that the map

$$R[x] \to A[x], \quad f \mapsto f_A$$

is an R-algebra morphism.

(b) Prove that $f_A[a] = f[a]$ for any $f \in R[x]$ and any $a \in A$.

The following exercise provides an analogue of Theorem 4.3.15 for polynomials in two variables. (Analogues for n variables can be obtained similarly, but require some more cumbersome notation.)

Exercise 4.3.11. Let R be an integral domain.

The **x-degree** of a nonzero polynomial $p \in R[x,y]$ is defined to be the largest $i \in \mathbb{N}$ such that there exists some $j \in \mathbb{N}$ satisfying $\left[x^i y^j\right] p \neq 0$. This x-degree is denoted by $\deg_x p$. Similarly, the **y-degree** of a nonzero polynomial $p \in R[x,y]$ is defined to be the largest $j \in \mathbb{N}$ such that there exists some $i \in \mathbb{N}$ satisfying $\left[x^i y^j\right] p \neq 0$. This y-degree is denoted by $\deg_y p$. (For example, the polynomial $p = 2x^6y + 3xy^2 - x^3 + xy \in \mathbb{Z}[x,y]$ has x-degree $\deg_x p = 6$ and y-degree $\deg_y p = 2$.) If p is the zero polynomial, then we set $\deg_x p = -\infty$ and $\deg_y p = -\infty$.

Let $n, m \in \mathbb{N}$. Let $p \in R[x,y]$ be any polynomial satisfying $\deg_x p \leq n$ and $\deg_y q \leq m$.

Let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of R. Let $b_0, b_1, \ldots, b_m$ be $m+1$ distinct elements of R. Prove the following: If

$$p\left[a_i, b_j\right] = 0 \qquad \text{for all } (i,j) \in \{0,1,\ldots,n\} \times \{0,1,\ldots,m\},$$

then $p = 0$ in $R[x,y]$.

[**Hint:** Use Theorem 4.3.15 many times. Specifically, for each $j \in \{0,1,\ldots,m\}$, argue that the univariate polynomial $p\left[x, b_j\right] \in R[x]$ has too many roots to be nonzero. Then, decompose p into $p = \sum_{k=0}^{n} p_k[y] x^k$, where $p_0, p_1, \ldots, p_n$ are univariate polynomials of degree $\leq m$. Apply Theorem 4.3.15 again to each of these polynomials $p_0, p_1, \ldots, p_n$.]

4.3.4. Application to $\mathbb{Z}/p$: Wilson revisited

The easy half of the FTA has a surprising plenitude of applications. Let me show an application to finite fields.

We fix a prime number p for the rest of this subsection.

First, let us reword Fermat's Little Theorem (Proposition 2.6.4) in the language of polynomials. First, we consider the polynomial

$$x^p - x \in (\mathbb{Z}/p)[x].$$

Proposition 2.6.4 yields that all evaluations of this polynomial at elements of $\mathbb{Z}/p$ are 0 (in fact, for each $u \in \mathbb{Z}/p$, we have $(x^p - x)[u] = u^p - u = 0$, since Proposition 2.6.4 yields $u^p = u$). The polynomial itself is not zero, and this is no surprise: It is a degree-p polynomial, so it can afford to have p roots in $\mathbb{Z}/p$ without being forced by Theorem 4.3.15 to be the zero polynomial. However, it is "dangerously close"; if its degree was even a little bit smaller than p, then we would obtain a contradiction. We can exploit this to extract a nice corollary.

To this end, we define the more sophisticated polynomial

$$f := (x^p - x) - \underbrace{\prod_{u \in \mathbb{Z}/p} (x-u)}_{= (x-\overline{0})(x-\overline{1})\cdots(x-\overline{(p-1)})} \in (\mathbb{Z}/p)[x].$$

This polynomial f has degree $\leq p-1$ (check this![137]). But it still has (at least) p roots in $\mathbb{Z}/p$; indeed, all the p elements of $\mathbb{Z}/p$ are roots of f, since each $w \in \mathbb{Z}/p$ satisfies

$$f[w] = \underbrace{(w^p - w)}_{\substack{=0 \\ \text{(since Proposition 2.6.4} \\ \text{yields } w^p = w\text{)}}} - \underbrace{\prod_{u \in \mathbb{Z}/p} (w-u)}_{\substack{=0 \\ \text{(since one of the factors} \\ \text{in this product is } w-w=0\text{)}}} = 0 - 0 = 0.$$

If the polynomial f was nonzero, then this would contradict Theorem 4.3.15 (since $\mathbb{Z}/p$ is a field and thus an integral domain). Hence, f must be zero. Since we defined f to be the difference $(x^p - x) - \prod_{u \in \mathbb{Z}/p} (x-u)$, we thus conclude that $x^p - x = \prod_{u \in \mathbb{Z}/p} (x-u)$. Let us state this as a proposition:

[137] *Proof.* Both polynomials $x^p - x$ and $\prod_{u \in \mathbb{Z}/p} (x-u)$ have degree p and leading coefficient 1. Thus, when you subtract the polynomial $\prod_{u \in \mathbb{Z}/p} (x-u)$ from $x^p - x$, the x^p terms of both polynomials cancel, and what remains is a linear combination of $x^0, x^1, \ldots, x^{p-1}$ – that is, a polynomial of degree $\leq p-1$.

Proposition 4.3.19. Let p be a prime number. Then,

$$x^p - x = \prod_{u \in \mathbb{Z}/p} (x - u) \qquad \text{in the polynomial ring } (\mathbb{Z}/p)[x].$$

Now, let us milk this for consequences. We have

$$\begin{aligned}
\prod_{u \in \mathbb{Z}/p} (x-u) &= \left(x - \overline{0}\right)\left(x - \overline{1}\right) \cdots \left(x - \overline{(p-1)}\right) \\
&\qquad \left(\text{since } \mathbb{Z}/p = \left\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\right\}\right) \\
&= x \quad \underbrace{\left(x - \overline{1}\right)\left(x - \overline{2}\right) \cdots \left(x - \overline{(p-1)}\right)}_{= \left(-\overline{1}\right)\left(-\overline{2}\right)\cdots\left(-\overline{(p-1)}\right) \cdot x^0 + (\text{higher powers of } x)} \\
&\qquad \begin{array}{c}\text{(here, ``higher powers of } x\text{'' means} \\ \text{``any powers of } x \text{ higher than } x^0\text{''})\end{array} \\
&= x\left(\left(-\overline{1}\right)\left(-\overline{2}\right) \cdots \left(-\overline{(p-1)}\right) \cdot x^0 + (\text{higher powers of } x)\right) \\
&= \left(-\overline{1}\right)\left(-\overline{2}\right) \cdots \left(-\overline{(p-1)}\right) \cdot x^1 + (\text{higher powers of } x).
\end{aligned}$$

Thus, the coefficient of x^1 in the polynomial $\prod_{u \in \mathbb{Z}/p} (x-u)$ is

$$\begin{aligned}
\left(-\overline{1}\right)\left(-\overline{2}\right) \cdots \left(-\overline{(p-1)}\right) &= \overline{(-1)^{p-1} \cdot (1 \cdot 2 \cdot \cdots \cdot (p-1))} \\
&= \overline{(-1)^{p-1} \cdot (p-1)!}.
\end{aligned}$$

On the other hand, the coefficient of x^1 in the polynomial $x^p - x$ is $\overline{-1}$ (since $p > 1$). But these two coefficients must be equal (since Proposition 4.3.19 says that the polynomials $\prod_{u \in \mathbb{Z}/p} (x-u)$ and $x^p - x$ are equal). Hence, $\overline{(-1)^{p-1} \cdot (p-1)!} = \overline{-1}$. In other words,

$$(-1)^{p-1} \cdot (p-1)! \equiv -1 \bmod p.$$

If we multiply this congruence by $(-1)^{p-1}$, then the left hand side becomes $(p-1)!$ (since $(-1)^{p-1} \cdot (-1)^{p-1} = 1$), and thus we get

$$(p-1)! \equiv (-1)^{p-1} \cdot (-1) = (-1)^p \equiv -1 \bmod p$$

(by Theorem 2.6.3, applied to $a = -1$). Thus, we have proved Wilson's theorem (Theorem 2.16.2) again!

We note that Proposition 4.3.19 can be generalized to arbitrary finite fields:

Exercise 4.3.12. Let F be a finite field.

(a) Prove that

$$x^{|F|} - x = \prod_{u \in F} (x - u) \qquad \text{in the polynomial ring } F[x].$$

(b) Prove that the product of all nonzero elements of F equals -1_F.

The method by which we obtained Proposition 4.3.19, too, can be generalized:

Exercise 4.3.13. Let R be an integral domain. Let $n \in \mathbb{N}$. Let $f \in R[x]$ be a nonzero polynomial that has degree $\leq n$. Prove the following:

(a) If $a_1, a_2, \ldots, a_k$ are k distinct roots of f in R for some $k \in \mathbb{N}$, then

$$f = q \cdot (x - a_1)(x - a_2) \cdots (x - a_k)$$

for some polynomial $q \in R[x]$ with $\deg q \leq n - k$.

(b) If $a_1, a_2, \ldots, a_n$ are n distinct roots of f in R, then

$$f = c(x - a_1)(x - a_2) \cdots (x - a_n),$$

where $c = [x^n] f$ is the coefficient of x^n in f.

(c) More generally, let us replace the assumption "Let R be an integral domain" by "Let R be a commutative ring". Instead of requiring that $a_1, a_2, \ldots, a_k$ (resp., $a_1, a_2, \ldots, a_n$) be distinct, we now require that the pairwise differences $a_i - a_j$ for $1 \leq i < j \leq k$ (resp., $1 \leq i < j \leq n$) are units of R. Prove that parts **(a)** and **(b)** of this exercise remain valid.

Another application of Theorem 4.3.15 is the following converse to Proposition 2.6.6:

Exercise 4.3.14. Let F be a finite field (i.e., a field with finitely many elements). Let $i > 1$ be an integer such that each $u \in F$ satisfies $u^i = u$. Prove that $i \geq |F|$.

4.3.5. Application to $\mathbb{Z}/p$: Sum of k-th powers

Here is another surprisingly simple application of Theorem 4.3.15:

Proposition 4.3.20. Let p be a prime. Let $k \in \{0, 1, \ldots, p-2\}$. Then, the integer $0^k + 1^k + \cdots + (p-1)^k = \sum_{j=0}^{p-1} j^k$ is divisible by p.

For example, for $k = 3$ and $p = 5$, this says that $0^3 + 1^3 + 2^3 + 3^3 + 4^3 = 100$ is divisible by 5.

Proof of Proposition 4.3.20. This is obvious when $k = 0$ (because when $k = 0$, we have $\sum_{j=0}^{p-1} \underbrace{j^k}_{=j^0=1} = \sum_{j=0}^{p-1} 1 = p$, which is clearly divisible by p). Thus, we WLOG assume that $k \neq 0$.

In $\mathbb{Z}/p$, we have

$$\overline{\sum_{j=0}^{p-1} j^k} = \sum_{j=0}^{p-1} \overline{j}^k = \sum_{u \in \mathbb{Z}/p} u^k \tag{89}$$

(since $\mathbb{Z}/p = \left\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\right\}$). Let us denote the sum $\sum_{u \in \mathbb{Z}/p} u^k$ by S. Thus, (89) becomes

$$\overline{\sum_{j=0}^{p-1} j^k} = S. \tag{90}$$

If we can show that $S = 0$, then (90) will simplify to $\overline{\sum_{j=0}^{p-1} j^k} = 0$, which will mean that $\sum_{j=0}^{p-1} j^k$ is divisible by p; thus, Proposition 4.3.20 will be proved. Hence, it remains to prove that $S = 0$.

Define a polynomial $f \in (\mathbb{Z}/p)[x]$ by $f = x^{k+1} - x$. This polynomial is nonzero (since $k \neq 0$) and has degree $k + 1 \leq p - 1$ (since $k \leq p - 2$). Thus, Theorem 4.3.15 (applied to $R = \mathbb{Z}/p$ and $n = p - 1$) yields that it has at most $p - 1$ roots in $\mathbb{Z}/p$. Hence, there exists at least one $a \in \mathbb{Z}/p$ such that $f[a] \neq 0$ (because otherwise, all the p elements $a \in \mathbb{Z}/p$ would be roots of f, but this would give f more than $p - 1$ roots). Consider this a.

From $f = x^{k+1} - x$, we obtain $f[a] = a^{k+1} - a = a\left(a^k - 1\right)$, so that $a\left(a^k - 1\right) = f[a] \neq 0$. Hence, $a \neq 0$ and $a^k - 1 \neq 0$. The element a of $\mathbb{Z}/p$ is nonzero (since $a \neq 0$) and thus a unit (since $\mathbb{Z}/p$ is a field). It therefore has an inverse a^{-1}. Hence, the map

$$\begin{aligned} \mathbb{Z}/p &\to \mathbb{Z}/p, \\ u &\mapsto au \end{aligned}$$

is invertible[138], i.e., a bijection. We can thus substitute au for u in the sum

[138] Its inverse is the map

$$\begin{aligned} \mathbb{Z}/p &\to \mathbb{Z}/p, \\ u &\mapsto a^{-1}u. \end{aligned}$$

$\sum\limits_{u \in \mathbb{Z}/p} u^k$. We obtain

$$\sum_{u \in \mathbb{Z}/p} u^k = \sum_{u \in \mathbb{Z}/p} \underbrace{(au)^k}_{=a^k u^k} = \sum_{u \in \mathbb{Z}/p} a^k u^k = a^k \sum_{u \in \mathbb{Z}/p} u^k.$$

In view of $\sum\limits_{u \in \mathbb{Z}/p} u^k = S$, we can rewrite this equality as $S = a^k S$. Hence, $a^k S - S = 0$. In other words, $\left(a^k - 1\right) S = 0$. Since $\mathbb{Z}/p$ is an integral domain, and since $a^k - 1 \neq 0$, this entails $S = 0$ (because otherwise, from $a^k - 1 \neq 0$ and $S \neq 0$, we would obtain $\left(a^k - 1\right) S \neq 0$). As explained above, this completes the proof of Proposition 4.3.20. □

Corollary 4.3.21. Let p be a prime. Let $f \in \mathbb{Z}[x]$ be a polynomial (with integer coefficients!) of degree $\leq p-2$. Then, $\sum\limits_{j=0}^{p-1} f(j) \equiv 0 \bmod p$.

Proof. Write the polynomial f in the form

$$f = \sum_{k=0}^{p-2} a_k x^k \tag{91}$$

with $a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z}$. (This can be done, since $f \in \mathbb{Z}[x]$ has degree $\leq p-2$.) Thus,

$$\sum_{j=0}^{p-1} \underbrace{f(j)}_{\substack{=\sum\limits_{k=0}^{p-2} a_k j^k \\ \text{(by (91))}}} = \sum_{j=0}^{p-1} \sum_{k=0}^{p-2} a_k j^k = \sum_{k=0}^{p-2} a_k \underbrace{\sum_{j=0}^{p-1} j^k}_{\substack{\equiv 0 \bmod p \\ \text{(since Proposition 4.3.20} \\ \text{yields that } \sum\limits_{j=0}^{p-1} j^k \text{ is} \\ \text{divisible by } p\text{)}}} \equiv \sum_{k=0}^{p-2} a_k 0 = 0 \bmod p.$$

This proves Corollary 4.3.21. □

We can generalize Proposition 4.3.20 a little bit:

Exercise 4.3.15. Let p be a prime. Let $k \in \mathbb{N}$. Prove that the integer $0^k + 1^k + \cdots + (p-1)^k = \sum\limits_{j=0}^{p-1} j^k$ is divisible by p if and only if k is not a positive multiple of $p-1$.

Exercise 4.3.16. Let p be a prime. Let $k \in \mathbb{N}$ be not a multiple of $p-1$. Assume that the rational number $\dfrac{1}{1^k} + \dfrac{1}{2^k} + \cdots + \dfrac{1}{(p-1)^k} = \sum\limits_{j=1}^{p-1} \dfrac{1}{j^k}$ has been written as a ratio $\dfrac{u}{v}$ of two integers u and v.

(a) Prove that $p \mid u$.

(b) Assume that $p > 3$ and $k = 1$. Prove that $p^2 \mid u$.

[**Hint:** For part **(a)**, multiply $\sum_{j=1}^{p-1} \frac{1}{j^k}$ by $(p-1)!^k$ to obtain an integer; then, work in $\mathbb{Z}/p$. For part **(b)**, observe that $\frac{1}{j} + \frac{1}{p-j} = \frac{p}{j(p-j)}$.]

4.3.6. $F[x]$ is a Euclidean domain

Let us go back to the case of polynomials over a general field. We next record an abstract consequence of Corollary 4.3.11 **(a)**:

Theorem 4.3.22. Let F be a field. Then:

(a) The polynomial ring $F[x]$ is a Euclidean domain. The map

$$N : F[x] \to \mathbb{N},$$
$$p \mapsto \max\{\deg p, 0\} = \begin{cases} \deg p, & \text{if } p \neq 0; \\ 0, & \text{if } p = 0 \end{cases}$$

is a Euclidean norm on $F[x]$.

(b) Thus, the polynomial ring $F[x]$ is a PID, hence also a UFD.

Proof. **(a)** Define a map $N : F[x] \to \mathbb{N}$ by

$$N(p) = \max\{\deg p, 0\} \qquad \text{for any } p \in F[x].$$

Then, Corollary 4.3.11 **(a)** shows that N is a Euclidean norm on the ring $F[x]$. Hence, $F[x]$ is a Euclidean domain (since Corollary 4.3.6 shows that $F[x]$ is an integral domain). This proves Theorem 4.3.22 **(a)**.

(b) We know from Proposition 2.14.2 that every Euclidean domain is a PID. Hence, $F[x]$ is a PID (since $F[x]$ is a Euclidean domain), and therefore a UFD (since we know from Theorem 2.15.11 that every PID is a UFD). □

Note that the "UFD" part of Theorem 4.3.22 **(b)** is not a very constructive result; there is no general algorithm for actually finding a prime factorization of a polynomial (i.e., for factoring a polynomial into irreducible polynomials) that works over any field. There are reasonably good algorithms for prime factorization in $\mathbb{Q}[x]$, however (see Section 6.5 below for one such algorithm, although a very inefficient one).

Theorem 4.3.22 entails, in particular, that univariate polynomials over a field have gcds and lcms (by Theorem 2.14.12). Moreover, the analogue of Bezout's theorem holds:

Theorem 4.3.23 (Bezout's theorem for polynomials)**.** Let F be a field. Let $a, b \in F[x]$ be two polynomials. Then, for any choice of $\gcd(a,b)$, there exist two polynomials $u, v \in F[x]$ such that $ua + vb = \gcd(a,b)$.

Proof. This is a general fact that holds in every PID (but not in every UFD). To wit, let us set $R = F[x]$, and recall that R is a PID (by Theorem 4.3.22 **(b)**). Recall how we proved the existence of a gcd (the proof of Theorem 2.14.12): Namely, we argued that there exists a $c \in R$ satisfying $aR + bR = cR$ (since R is a PID, so that the ideal $aR + bR$ of R must be principal), and then we proved that this c is a gcd of a and b. Now, assume that we have chosen some gcd of a and b, and denoted it by $\gcd(a,b)$. This $\gcd(a,b)$ is not necessarily identical to c, but it is clearly associate to c, since Proposition 2.14.11 **(a)** says that any two gcds of a and b are associate. Thus, $\gcd(a,b) = cu$ for some unit u of R. Consider this u. Now,

$$\gcd(a,b) = c\underbrace{u}_{\in R} \in cR = aR + bR.$$

In other words, there exist some $u, v \in R$ such that $\gcd(a,b) = au + bv$. In other words, there exist some $u, v \in R$ such that $\gcd(a,b) = ua + vb$. This proves Theorem 4.3.23. □

A few words about computability are in order. If F is a field, and if $a, b \in F[x]$ are two polynomials, then we can compute a $\gcd(a,b)$ by the extended Euclidean algorithm (more precisely, the algorithm explained in the proof of Theorem 2.13.8 **(b)** computes a Bezout 5-tuple for (a,b), and then Corollary 2.14.14 reveals that the third entry of this 5-tuple is a gcd of a and b). This is one of the most useful features of univariate polynomials. The following exercises should give you some practice with this algorithm:

Exercise 4.3.17. Work in the polynomial ring $\mathbb{Q}[x]$.

(a) Compute a $\gcd\left(x^3 - x,\ x^5 - 3x + 2\right)$. (The indefinite article "a" refers to the fact that a gcd is unique only up to multiplying by a unit.)

(b) Compute a $\gcd\left(x^4 + x^2 + 1,\ x^4 + x^3 + x^2 + 2\right)$.

Exercise 4.3.18. Let F be a field. We will work in the polynomial ring $F[x]$.

(a) Compute a $\gcd\left(x^2 - 1,\ x^3 - 1\right)$.

(b) Compute a $\gcd\left(x^2 - 1,\ x^5 - 1\right)$.

(c) Compute a $\gcd\left(x^4 - 1,\ x^6 - 1\right)$.

(d) Let $m, n \in \mathbb{N}$. Prove that $\gcd\left(x^m - 1,\ x^n - 1\right) = x^{\gcd(m,n)} - 1$. (To be more precise, show that $x^{\gcd(m,n)} - 1$ is a gcd of $x^m - 1$ and $x^n - 1$. Of course, multiplying this gcd by a nonzero scalar in F will yield another gcd.)

Exercise 4.3.19. Let F be a field. We will work in the polynomial ring $F[x]$.

(a) Compute a gcd $\left(x^2+1,\ x^3+1\right)$ under the assumption that $2 \cdot 1_F \neq 0_F$.

(b) Compute a gcd $\left(x^2+1,\ x^3+1\right)$ under the assumption that $2 \cdot 1_F = 0_F$.

(c) Compute a gcd $\left(x^3+1,\ x^5+1\right)$.

(d) Let $m, n \in \mathbb{N}$ be odd. Prove that $\gcd\left(x^m+1,\ x^n+1\right) = x^{\gcd(m,n)}+1$.

(e) Let m be an even positive integer, and n an odd positive integer. Prove that $\gcd\left(x^m+1,\ x^n+1\right) = 1$ if $2 \cdot 1_F \neq 0_F$.

(f) More generally, prove the following: If m and n are positive integers, and if $a, b \in F$ are two elements satisfying $a^n \neq b^m$, then $\gcd\left(x^m-a,\ x^n-b\right) = 1$.

[**Hint:** For part **(d)**, a substitution can be helpful. Part **(e)** is easiest to derive from part **(f)**.]

Warning 4.3.24. Multivariate polynomial rings (like $\mathbb{Q}[x,y]$) are not PIDs (and thus not Euclidean domains either). For example, if $R = \mathbb{Q}[x,y]$, then the ideal $xR + yR$ is not principal. (Check this! This ideal is easily seen to consist of all polynomials whose constant term (= coefficient of x^0y^0) is 0, but these polynomials are not the multiples of a single polynomial.) However, multivariate polynomial rings over fields (and, more generally, over UFDs) are still UFDs. This is a deeper result than the ones we have proved above (see, e.g., [DumFoo04, §9.3, Corollary 8] or [Ford22, Theorem 3.7.4] or [ChaLoi21, Corollary (2.6.7)] or [Knapp16, Corollary 8.21 and Remark after it] or [Swanso17, Theorem 36.11] for proofs). As a consequence, polynomials over a field (or a UFD) have gcds; however, they don't generally satisfy Bezout's theorem unless the polynomials are univariate polynomials over a field.

Univariate polynomial rings over non-fields (like $\mathbb{Z}[x]$) behave similarly: They are not PIDs, but they are UFDs when the base ring is a UFD. (That is, if R is a UFD, then so is $R[x]$.)

4.3.7. Lagrange interpolation

Theorem 4.3.15 has the following simple corollary:

Corollary 4.3.25 (uniqueness of interpolating polynomial)**.** Let R be an integral domain. Let $n \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of R. Let $f, g \in R[x]$ be two polynomials of degree $\leq n$. Assume that

$$f[a_i] = g[a_i] \qquad \text{for all } i \in \{0,1,\ldots,n\}. \tag{92}$$

Then, $f = g$.

Corollary 4.3.25 is saying that if two univariate polynomials of degree $\leq n$ over an integral domain R agree in at least $n+1$ distinct positions $a_0, a_1, \ldots, a_n$, then they must be equal. In particular, if two univariate polynomials (of any degree) over an integral domain R agree at infinitely many distinct positions, then they must be equal. This is an extremely useful result with applications all over mathematics.[139]

Proof of Corollary 4.3.25. Assume the contrary. Thus, $f \neq g$, so that $f - g \neq 0$. The nonzero polynomial $f - g$ has degree $\leq n$ (since each of f and g has degree $\leq n$). Thus, Theorem 4.3.15 (applied to $f - g$ instead of f) shows that $f - g$ has at most n roots in R.

However, for each $i \in \{0, 1, \ldots, n\}$, the element a_i is a root of $f - g$, since

$$(f - g)[a_i] = f[a_i] - g[a_i] = 0 \qquad \text{(by (92))}.$$

In other words, the $n+1$ elements $a_0, a_1, \ldots, a_n$ of R are roots of $f - g$. Since these elements $a_0, a_1, \ldots, a_n$ are distinct, this shows that the polynomial $f - g$ has at least $n+1$ roots in R. But this contradicts the fact that $f - g$ has at most n roots in R. This contradiction shows that our assumption was false. Thus, Corollary 4.3.25 is proven. □

Corollary 4.3.25 can be restated as follows: A univariate polynomial $f \in R[x]$ of degree $\leq n$ over an integral domain R is uniquely determined by any $n+1$ values $f[a_0]$, $f[a_1]$, $\ldots$, $f[a_n]$ (provided, of course, that the inputs $a_0, a_1, \ldots, a_n \in R$ are distinct and known). This is a nice uniqueness statement. Can we find a matching existence statement for it? In other words, if we are given $n+1$ distinct elements $a_0, a_1, \ldots, a_n$ of an integral domain R and $n+1$ arbitrary elements $b_0, b_1, \ldots, b_n$ of R, then is there necessarily some polynomial $f \in R[x]$ of degree $\leq n$ that satisfies

$$f[a_i] = b_i \qquad \text{for all } i \in \{0, 1, \ldots, n\} \ ?$$

A bit of thought reveals that the answer is negative. Indeed, there is no polynomial $f \in \mathbb{Z}[x]$ that satisfies $f[0] = 0$ and $f[2] = 1$. The reason is a lack of divisibility: Any polynomial $f \in \mathbb{Z}[x]$ satisfies $a - b \mid f[a] - f[b]$ for all $a, b \in \mathbb{Z}$ (check this!), but our conditions $f[0] = 0$ and $f[2] = 1$ would make this divisibility false for $a = 2$ and $b = 0$. Thus, our alleged existence statement cannot hold for arbitrary integral domains R.

However, it turns out to be true when R is a field. Moreover, the required polynomial f can be expressed directly:

[139] For example, its particular case for $R = \mathbb{C}$ is [Grinbe21, Corollary 7.5.7], and is subsequently used in [Grinbe21, §7.5.3] is used to prove identities for binomial coefficients. Many more applications exist in a similar vein (see, e.g., [21s, Combinatorial proof of Proposition 6.1.1]); this technique is known as the "polynomial identity trick".

Theorem 4.3.26 (Lagrange interpolation)**.** Let F be a field. Consider the univariate polynomial ring $F[x]$. Let $n \in \mathbb{N}$.

Let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of F. Let $b_0, b_1, \ldots, b_n$ be $n+1$ arbitrary elements of F. Then:

(a) There is a **unique** polynomial $p \in F[x]$ satisfying $\deg p \leq n$ and

$$p[a_i] = b_i \qquad \text{for all } i \in \{0, 1, \ldots, n\}.$$

(b) This polynomial p is given by

$$p = \sum_{j=0}^{n} b_j \frac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)}$$

(where the "$\prod\limits_{k \neq j}$" sign means a product over all $k \in \{0, 1, \ldots, n\}$ satisfying $k \neq j$).

For example, if $n = 2$, then

- Theorem 4.3.26 **(a)** is saying that there is a unique polynomial $p \in F[x]$ satisfying $\deg p \leq 2$ and

$$p[a_0] = b_0 \qquad \text{and} \qquad p[a_1] = b_1 \qquad \text{and} \qquad p[a_2] = b_2,$$

- and Theorem 4.3.26 **(b)** is saying that this polynomial p is given by

$$p = b_0 \frac{(x - a_1)(x - a_2)}{(a_0 - a_1)(a_0 - a_2)} + b_1 \frac{(x - a_0)(x - a_2)}{(a_1 - a_0)(a_1 - a_2)} + b_2 \frac{(x - a_0)(x - a_1)}{(a_2 - a_0)(a_2 - a_1)}.$$

Proof of Theorem 4.3.26. Define a polynomial $g \in F[x]$ by

$$g = \sum_{j=0}^{n} b_j \frac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)} \tag{93}$$

(where the "$\prod\limits_{k \neq j}$" signs means a product over all $k \in \{0, 1, \ldots, n\}$ satisfying $k \neq j$). Note that g is well-defined; indeed, all the differences $a_j - a_k$ appearing in the denominators are nonzero (because $a_0, a_1, \ldots, a_n$ are distinct) and thus are units (since F is a field).

Each of the $n+1$ addends $b_j \dfrac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)}$ on the right hand side of (93) is a polynomial of degree $\leq n$ (since the numerator $\prod\limits_{k \neq j} (x - a_k)$ is a product of n degree-1 polynomials $x - a_k$, whereas the remaining pieces b_j and $\prod\limits_{k \neq j} (a_j - a_k)$ of the expression are elements of F). Hence, their sum must be a polynomial of degree $\leq n$ as well (since any sum of polynomials of degree $\leq n$ is again a polynomial of degree $\leq n$). In other words, g is a polynomial of degree $\leq n$ (since (93) shows that g is their sum). That is, we have $\deg g \leq n$.

If $i \in \{0, 1, \ldots, n\}$ and $j \in \{0, 1, \ldots, n\}$ satisfy $j \neq i$, then we have

$$\prod_{k \neq j} (a_i - a_k) = 0 \tag{94}$$

(because in this case, the product $\prod\limits_{k \neq j} (a_i - a_k)$ contains the factor $a_i - a_i$ (since $i \neq j$), but this factor is 0, and therefore the whole product is 0).

For each $i \in \{0, 1, \ldots, n\}$, we have

$$\begin{aligned}
g[a_i] &= \left(\sum_{j=0}^{n} b_j \frac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)} \right) [a_i] \qquad \text{(by the definition of } g\text{)} \\
&= \sum_{j=0}^{n} b_j \frac{\prod\limits_{k \neq j} (a_i - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)} \\
&= b_i \underbrace{\frac{\prod\limits_{k \neq i} (a_i - a_k)}{\prod\limits_{k \neq i} (a_i - a_k)}}_{=1} + \sum_{\substack{j \in \{0,1,\ldots,n\}; \\ j \neq i}} b_j \underbrace{\frac{\prod\limits_{k \neq j} (a_i - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)}}_{\substack{=0 \\ \text{(by (94))}}} \\
&\qquad \text{(here, we have split off the addend for } j = i \text{ from the sum)} \\
&= b_i + \underbrace{\sum_{\substack{j \in \{0,1,\ldots,n\}; \\ j \neq i}} b_j \cdot 0}_{=0} = b_i.
\end{aligned}$$

Hence, g is a polynomial $p \in F[x]$ satisfying $\deg p \leq n$ and

$$p[a_i] = b_i \qquad \text{for all } i \in \{0, 1, \ldots, n\} \tag{95}$$

(since we already know that $\deg g \leq n$).

(a) We need to prove that there is a unique polynomial $p \in F[x]$ satisfying $\deg p \leq n$ and (95). We already know that such a p exists (because we have just shown that g is such a p); thus, it remains to prove its uniqueness. In other words, we need to prove the following claim:

> *Claim 1:* Let p_1 and p_2 be two polynomials $p \in F[x]$ satisfying $\deg p \leq n$ and (95). Then, $p_1 = p_2$.

Proof of Claim 1. We have assumed that p_1 is a polynomial $p \in F[x]$ satisfying $\deg p \leq n$ and (95). In other words, $p_1 \in F[x]$ is a polynomial and satisfies $\deg p_1 \leq n$ and

$$p_1[a_i] = b_i \qquad \text{for all } i \in \{0, 1, \ldots, n\}. \tag{96}$$

Similarly, $p_2 \in F[x]$ is a polynomial and satisfies $\deg p_2 \leq n$ and

$$p_2[a_i] = b_i \qquad \text{for all } i \in \{0, 1, \ldots, n\}. \tag{97}$$

For each $i \in \{0, 1, \ldots, n\}$, we have

$$\begin{aligned} p_1[a_i] &= b_i && \text{(by (96))} \\ &= p_2[a_i] && \text{(by (97))}. \end{aligned}$$

Hence, Corollary 4.3.25 (applied to $R = F$, $f = p_1$ and $g = p_2$) yields that $p_1 = p_2$ (since p_1 and p_2 both have degree $\leq n$). This proves Claim 1. □

Now, our proof of Theorem 4.3.26 **(a)** is complete.

(b) In our above proof of Theorem 4.3.26 **(a)**, we have shown not just that there is a unique polynomial $p \in F[x]$ satisfying $\deg p \leq n$ and (95); we have also shown that g is such a polynomial. But since this p is unique, this means that g is the **only** such polynomial. Thus, the only such polynomial is $g = \sum_{j=0}^{n} b_j \dfrac{\prod_{k \neq j} (x - a_k)}{\prod_{k \neq j} (a_j - a_k)}$. This proves Theorem 4.3.26 **(b)**. □

One of many applications of Theorem 4.3.26 **(b)** is an explicit formula for recovering a univariate polynomial f of degree $\leq n$ (over a field) from any $n+1$ values $f[a_0]$, $f[a_1]$, $\ldots$, $f[a_n]$ of f (provided that the inputs $a_0, a_1, \ldots, a_n$ are distinct and known). Let us make this explicit:

Corollary 4.3.27. Let F be a field. Consider the univariate polynomial ring $F[x]$. Let $n \in \mathbb{N}$.

Let $f \in F[x]$ be a polynomial of degree $\leq n$.

Let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of F. Then,

$$f = \sum_{j=0}^{n} f[a_j] \cdot \frac{\prod_{k \neq j} (x - a_k)}{\prod_{k \neq j} (a_j - a_k)}$$

(where the "$\prod\limits_{k\neq j}$" sign means a product over all $k \in \{0,1,\ldots,n\}$ satisfying $k \neq j$).

Proof. Theorem 4.3.26 **(a)** (applied to $b_i = f[a_i]$) yields that there is a **unique** polynomial $p \in F[x]$ satisfying $\deg p \leq n$ and

$$p[a_i] = f[a_i] \qquad \text{for all } i \in \{0,1,\ldots,n\}.$$

Furthermore, Theorem 4.3.26 **(b)** (applied to $b_i = f[a_i]$) yields that this polynomial p is given by

$$p = \sum_{j=0}^{n} f[a_j] \cdot \frac{\prod\limits_{k\neq j}(x-a_k)}{\prod\limits_{k\neq j}(a_j-a_k)}.$$

Combining this, we conclude that if $p \in F[x]$ is a polynomial satisfying $\deg p \leq n$ and

$$p[a_i] = f[a_i] \qquad \text{for all } i \in \{0,1,\ldots,n\},$$

then

$$p = \sum_{j=0}^{n} f[a_j] \cdot \frac{\prod\limits_{k\neq j}(x-a_k)}{\prod\limits_{k\neq j}(a_j-a_k)}.$$

Applying this to $p = f$, we obtain

$$f = \sum_{j=0}^{n} f[a_j] \cdot \frac{\prod\limits_{k\neq j}(x-a_k)}{\prod\limits_{k\neq j}(a_j-a_k)}$$

(since $f \in F[x]$ is a polynomial satisfying $\deg f \leq n$ and $f[a_i] = f[a_i]$ for all $i \in \{0,1,\ldots,n\}$). This proves Corollary 4.3.27. □

Exercise 4.3.20. Let F be a field. Let $n \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of F. Prove that for each $\ell \in \{0,1,\ldots,n\}$, we have

$$\sum_{j=0}^{n} \frac{a_j^{\ell}}{\prod\limits_{k\neq j}(a_j-a_k)} = \begin{cases} 1, & \text{if } \ell = n; \\ 0, & \text{if } \ell < n \end{cases}$$

(where the "$\prod\limits_{k\neq j}$" sign means a product over all $k \in \{0,1,\ldots,n\}$ satisfying $k \neq j$).

[**Hint:** Apply Corollary 4.3.27 to $f = x^{\ell}$ and compare the x^n-coefficients on both sides of the equality.]

Exercise 4.3.21. Let $n \in \mathbb{N}$ and $\ell \in \mathbb{N}$. Prove that

$$\sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} j^{\ell} = \begin{cases} n!, & \text{if } \ell = n; \\ 0, & \text{if } \ell < n. \end{cases}$$

[**Hint:** Apply Exercise 4.3.20 to $F = \mathbb{Q}$ and $a_i = i$.]

Exercise 4.3.22. Let $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$ and $\ell \in \{0, 1, \ldots, n\}$. Prove that

$$\sum_{j=0}^{n} (-1)^{n-j} \binom{n}{j} \binom{aj+b}{\ell} = \begin{cases} a^n, & \text{if } \ell = n; \\ 0, & \text{if } \ell < n. \end{cases}$$

(Recall that the binomial coefficient $\binom{u}{\ell}$ is defined to be $\dfrac{u(u-1)(u-2)\cdots(u-\ell+1)}{\ell!}$ for each $u \in \mathbb{R}$.)

Exercise 4.3.23. Let F be a field. Let $n \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of F. Let $f \in F[x]$ be a polynomial of degree $\leq n$. Prove that

$$\sum_{j=0}^{n} \frac{f[a_j]}{\prod\limits_{k \neq j} (a_j - a_k)} = [x^n] f$$

(where the "$\prod\limits_{k \neq j}$" sign means a product over all $k \in \{0, 1, \ldots, n\}$ satisfying $k \neq j$).

[**Hint:** Apply Corollary 4.3.27. Then, take the x^n-coefficient.]

Exercise 4.3.24. Let F be a field. Let $n \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of F. Prove that

$$\sum_{j=0}^{n} \frac{a_j^{n+1}}{\prod\limits_{k \neq j} (a_j - a_k)} = a_0 + a_1 + \cdots + a_n$$

(where the "$\prod\limits_{k \neq j}$" sign means a product over all $k \in \{0, 1, \ldots, n\}$ satisfying $k \neq j$).

[**Hint:** Apply Exercise 4.3.23 to $f = x^{n+1} - \prod\limits_{k=0}^{n} (x - a_k)$.]

Exercise 4.3.25. Let F be a field. Let $n \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of F. Prove that

$$\sum_{j=0}^{n} a_j \frac{\prod\limits_{k \neq j} (a_j + a_k)}{\prod\limits_{k \neq j} (a_j - a_k)} = a_0 + a_1 + \cdots + a_n$$

(where the "$\prod\limits_{k \neq j}$" sign means a product over all $k \in \{0, 1, \ldots, n\}$ satisfying $k \neq j$).

[**Hint:** Let $2_F := 2 \cdot 1_F \in F$. Distinguish between the cases when $2_F = 0_F$ and when $2_F \neq 0_F$. In the former case, $a + b = a - b$ for all $a, b \in F$ (why?), and the claim becomes very easy. Now, consider the latter case. In this case, 2_F is a unit of F, thus can be cancelled. Now, apply Exercise 4.3.23 to $f = \prod_{k=0}^{n} (x + a_k) - \prod_{k=0}^{n} (x - a_k)$. Then, simplify and cancel 2_F.]

(This exercise is Crux Mathematicorum problem #4762, proposed by Didier Pinchon and George Stoica in issue 49/2.)

Exercise 4.3.26. Let F be a field. Let $n \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of F. Prove that

$$\sum_{j=0}^{n} \frac{\prod\limits_{k \neq j} (a_j + a_k)}{\prod\limits_{k \neq j} (a_j - a_k)} = \begin{cases} 1, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}$$

(where the "$\prod\limits_{k \neq j}$" sign means a product over all $k \in \{0, 1, \ldots, n\}$ satisfying $k \neq j$).

[**Hint:** Let $2_F := 2 \cdot 1_F \in F$. Deal with the case $2_F = 0_F$ as in Exercise 4.3.25. In the remaining case, show that the polynomial $\prod_{k=0}^{n} (a_k + x) - \prod_{k=0}^{n} (a_k - x) \in F[x]$ is divisible by $2x$, and let f be the quotient of this division. Now, apply Exercise 4.3.23 to this f.]

For more identities in the vein of Exercises 4.3.20, 4.3.24, 4.3.26 and 4.3.25, see [Nica22].

Exercise 4.3.27. Let $n \in \mathbb{N}$. Let $p \in \mathbb{Q}[x]$ be a polynomial of degree $\leq n$ such that

$$p[i] = 2^i \qquad \text{for all } i \in \{0, 1, \ldots, n\}.$$

Find $p[n+1]$.

Exercise 4.3.28. Let $n \in \mathbb{N}$. Let $p \in \mathbb{Q}[x]$ be a polynomial of degree $\leq n$ such that

$$p[i] = \frac{1}{\binom{n+1}{i}} \qquad \text{for all } i \in \{0, 1, \ldots, n\}.$$

Find $p[n+1]$.

The next exercise gives a two-variable version of Lagrange interpolation (to be more specific, of Theorem 4.3.26):

Exercise 4.3.29. Let F be a field. Consider the polynomial ring $F[x, y]$ in two variables x and y.

For any polynomial $p \in F[x, y]$, define the x-degree $\deg_x p$ and the y-degree $\deg_y p$ as in Exercise 4.3.11.

Let $n, m \in \mathbb{N}$.

Let $a_0, a_1, \ldots, a_n$ be $n+1$ distinct elements of F. Let $b_0, b_1, \ldots, b_m$ be $m+1$ distinct elements of F. Let $c_{i,j}$ be an element of F for each pair $(i,j) \in \{0,1,\ldots,n\} \times \{0,1,\ldots,m\}$. Prove the following:

(a) There is a **unique** polynomial $p \in F[x,y]$ satisfying $\deg_x p \leq n$ and $\deg_y p \leq m$ and

$$p\left[a_i, b_j\right] = c_{i,j} \qquad \text{for all } (i,j) \in \{0,1,\ldots,n\} \times \{0,1,\ldots,m\}.$$

(b) This polynomial p is given by

$$p = \sum_{k=0}^{n} \sum_{\ell=0}^{m} c_{k,\ell} \frac{\prod\limits_{u \neq k} (x - a_u)}{\prod\limits_{u \neq k} (a_k - a_u)} \cdot \frac{\prod\limits_{v \neq \ell} (y - b_v)}{\prod\limits_{v \neq \ell} (b_\ell - b_v)}$$

(where the "$\prod\limits_{u \neq k}$" sign means a product over all $u \in \{0,1,\ldots,n\}$ satisfying $u \neq k$, and where the "$\prod\limits_{v \neq \ell}$" sign means a product over all $v \in \{0,1,\ldots,m\}$ satisfying $v \neq \ell$).

4.4. Intermezzo: quotients of R-algebras

In preparation for the next section, let me quickly introduce quotients of R-algebras. I have previously defined quotients of rings modulo ideals, and quotients of R-modules modulo submodules. These two concepts can be combined to obtain quotients of R-algebras modulo ideals:

Theorem 4.4.1. Let A be an R-algebra. Let I be an ideal of A. Then:

(a) The ideal I is also an R-submodule of A.

(b) The quotient ring A/I and the quotient R-module A/I fit together to form an R-algebra.

(c) The canonical projection $\pi : A \to A/I$ (which sends each $a \in A$ to its residue class $\overline{a} = a + I$) is an R-algebra morphism (from the original R-algebra A to the R-algebra A/I that we just constructed in part **(b)**).

Proof. **(a)** We already know that I is closed under addition and contains zero (since I is an ideal). So we must only show that I is closed under scaling. In other words, we must show that $ri \in I$ for each $r \in R$ and $i \in I$. But this is

easy: If $r \in R$ and $i \in I$, then

$$r \underbrace{i}_{=1_A \cdot i} = r \cdot 1_A \cdot i = \underbrace{(r \cdot 1_A)}_{\in A} \cdot \underbrace{i}_{\in I} \in I \qquad \left(\text{since } I \text{ is an ideal of } A\right).$$

(b) LTTR. (You just need to verify the "scale-invariance of multiplication" axiom, but this is straightforward.)

(c) We already know that this canonical projection is a ring morphism and an R-module morphism; thus, it is an R-algebra morphism. □

Definition 4.4.2. Let A and I be as in Theorem 4.4.1. Then, the R-algebra A/I constructed in Theorem 4.4.1 **(b)** is called the **quotient algebra** (or **quotient R-algebra**) of A by the ideal I.

Let us next recall the universal property of quotient rings (in its two forms: Theorem 2.9.5 and Theorem 2.9.6). This property is the tool of choice from constructing ring morphisms out of a quotient ring. We can adapt this theorem to R-algebras with just trivial modifications (alas, we have to rename R and S as A and B, since R already means something different):

Theorem 4.4.3 (Universal property of quotient algebras, elementwise form)**.** Let A be an R-algebra. Let I be an ideal of A.

Let B be an R-algebra. Let $f : A \to B$ be an R-algebra morphism. Assume that $f(I) = 0$ (this is shorthand for saying that $f(a) = 0$ for all $a \in I$). Then, the map

$$\begin{aligned} f' : A/I &\to B, \\ \overline{a} &\mapsto f(a) \qquad \left(\text{for all } a \in A\right) \end{aligned}$$

is well-defined (i.e., the value $f(a)$ depends only on the residue class $\overline{a}$, not on a itself) and is an R-algebra morphism.

Proof. Adapt the argument that we used to prove Theorem 2.9.5. The only new thing we need to check is that the map f' constructed in the proof is R-linear; but this is just as straightforward as showing that this map is a ring morphism. □

Theorem 4.4.4 (Universal property of quotient algebras, abstract form)**.** Let A be an R-algebra. Let I be an ideal of A. Consider the canonical projection $\pi : A \to A/I$.

Let B be an R-algebra. Let $f : A \to B$ be an R-algebra morphism. Assume that $f(I) = 0$ (this is shorthand for saying that $f(a) = 0$ for all $a \in I$). Then, there is a unique R-algebra morphism $f' : A/I \to B$ satisfying $f = f' \circ \pi$.

Proof. Adapt the argument that we used to prove Theorem 2.9.6. □

The First Isomorphism Theorem for rings (Theorem 2.9.9) also has an analogue for R-algebras. We leave it to the reader to state it.

4.5. Adjoining roots

4.5.1. Examples

What is a complex number? Nowadays, the complex numbers are commonly defined as pairs of real numbers; this is a fairly straightforward process (first you define addition and multiplication and zero and unity; then you show that the ring axioms hold) and can be found in many textbooks (e.g., [Grinbe19, §4.1]). But this is the modern definition. When Girolamo Cardano originally invented complex numbers back in the 16th century, he had a different vision: Cardano essentially proposed to **imagine** that there is a new number called i that satisfies $i^2 = -1$ but otherwise behaves like the numbers we know. Thus, you're allowed to form arbitrary polynomials in i, but you have to equate i^2 to -1, so you never end up getting anything more complicated than numbers of the form $a + bi$ with $a, b \in \mathbb{R}$ (since any higher power of i can be reduced to ± 1 or $\pm i$ using the $i^2 = -1$ rule). Thus, it makes sense to encode complex numbers as pairs of real numbers, but this is merely one way of encoding them.[140]

Of course, Cardano's original vision is not a rigorous definition; just as easily you could introduce a number j satisfying $0j = 1$, and thus collapse the entire number system (since this new number would let you argue that $1 = 0j = (0+0)\,j = 0j + 0j = 1 + 1 = 2$). So, if we want to make Cardano's definition rigorous, we have to rewrite it algebraically. One way to do this is to define $\mathbb{C}$ as the quotient ring

$$\mathbb{R}[x] \,/\, \left(x^2 + 1\right) \mathbb{R}[x].$$

In fact, we start with $\mathbb{R}[x]$ because our complex numbers should be polynomials in a single symbol i (which will be represented by the indeterminate x in $\mathbb{R}[x]$); but then we quotient out the ideal $\left(x^2 + 1\right) \mathbb{R}[x]$ since we want $i^2 + 1$ (and thus also each multiple of $i^2 + 1$) to be 0 in our complex numbers.

To be on the safe side, let us show that this quotient ring $\mathbb{R}[x] \,/\, \left(x^2 + 1\right) \mathbb{R}[x]$ is isomorphic to the complex numbers $\mathbb{C}$ as we know them (i.e., defined in the modern way, as pairs of real numbers).

[140] I am being sloppy with the history here. The relevant source is Girolamo Cardano's 1545 book *Ars magna*, specifically its Chapter XXXVII, in which he asks the reader to "imagine $\sqrt{-15}$". Of course, this is not much different from imagining $i = \sqrt{-1}$, since a square root of -15 could be obtained from a square root of -1 by multiplying with the real number $\sqrt{15}$.

Cardano was writing at a time when even the notion of a negative number was far from widely accepted in the West (though known in India and Persia). Cardano himself called negative numbers "fictitious" (arguably an improvement from previous European authors, who called them "absurd"), and did not quite treat them as first-class numbers. His *Ars magna* is often considered to be the first serious treatment of negative numbers written in Europe. That the very same book introduces complex numbers is thus an example of the "when it rains, it pours" phenomenon in the history of ideas.

Cardano did not introduce the name i for the imaginary unit $\sqrt{-1}$. This was done by Euler much later.

First of all, we introduce a shorthand:

Convention 4.5.1. If R is a commutative ring, and if $a \in R$, then the quotient ring R/aR will be abbreviated as R/a. We are already using a particular case of this notation, as we are writing $\mathbb{Z}/n$ for $\mathbb{Z}/n\mathbb{Z}$ when n is an integer.

We note that the quotient ring $R/a = R/aR$ is not just a ring, but an R-algebra as well (by Theorem 4.4.1 **(b)**). Furthermore, the R-algebra R/a is commutative (since it is a quotient of R). This all will be tacitly used in what follows.

So we want to prove that $\mathbb{R}[x] / \left(x^2+1\right) \cong \mathbb{C}$ as rings – and even better, as $\mathbb{R}$-algebras. Let's be a little bit more precise:

Proposition 4.5.2. We have $\mathbb{R}[x] / \left(x^2+1\right) \cong \mathbb{C}$ as $\mathbb{R}$-algebras. More concretely: There is an $\mathbb{R}$-algebra isomorphism

$$\begin{aligned} \mathbb{R}[x] / \left(x^2+1\right) &\to \mathbb{C}, \\ \overline{p} &\mapsto p[i]. \end{aligned}$$

Proof. We already know that $\mathbb{C}$ is an $\mathbb{R}$-algebra. Thus, Theorem 4.2.8 (applied to $R = \mathbb{R}$ and $A = \mathbb{C}$ and $a = i$) yields that the map

$$\begin{aligned} f : \mathbb{R}[x] &\to \mathbb{C}, \\ p &\mapsto p[i] \end{aligned}$$

is an $\mathbb{R}$-algebra morphism. This map f sends the principal ideal $\left(x^2+1\right)\mathbb{R}[x]$ to 0, because for each $q \in \mathbb{R}[x]$, we have

$$f\left(\left(x^2+1\right) \cdot q\right) = \left(\left(x^2+1\right) \cdot q\right)[i] = \underbrace{\left(i^2+1\right)}_{=0} \cdot q[i] = 0.$$

Hence, Theorem 4.4.3 (applied to $R = \mathbb{R}$, $A = \mathbb{R}[x]$, $I = \left(x^2+1\right)\mathbb{R}[x]$ and $B = \mathbb{C}$) shows that the map

$$\begin{aligned} f' : \mathbb{R}[x] / \left(x^2+1\right) &\to \mathbb{C}, \\ \overline{a} &\mapsto f(a) \end{aligned}$$

is well-defined and is an $\mathbb{R}$-algebra morphism. Consider this map f'. Each $p \in \mathbb{R}[x]$ satisfies

$$\begin{aligned} f'(\overline{p}) &= f(p) && \left(\text{by the definition of } f'\right) \\ &= p[i] && \left(\text{by the definition of } f\right). \end{aligned} \tag{98}$$

Now, why is f' an isomorphism?

It's not hard to see that f' is surjective: Indeed, any $z \in \mathbb{C}$ can be written as $z = a + bi$ for some $a, b \in \mathbb{R}$, and then we have $z = a + bi = f'\left(\overline{a + bx}\right)$ (since (98) yields $f'\left(\overline{a + bx}\right) = (a + bx)[i] = a + bi$).

Now, how can we prove that f' is injective? Since f' is $\mathbb{R}$-linear, it suffices to show that $\operatorname{Ker}(f') = \{0\}$ (by Lemma 3.5.10).

Let $u \in \operatorname{Ker}(f')$. Thus, $u \in \mathbb{R}[x] / \left(x^2 + 1\right)$, so that $u = \overline{p}$ for some $p \in \mathbb{R}[x]$. Consider this p.

However, Theorem 4.3.7 **(a)** (applied to $R = \mathbb{R}$, $b = x^2 + 1$ and $a = p$) yields that there is a unique pair (q, r) of polynomials in $\mathbb{R}[x]$ such that

$$p = q \cdot \left(x^2 + 1\right) + r \qquad \text{and} \qquad \deg r < \deg\left(x^2 + 1\right).$$

Consider this pair (q, r). From $\deg r < \deg\left(x^2 + 1\right) = 2$, we see that the polynomial r can be written as $a + bx$ for some $a, b \in \mathbb{R}$. Consider these a, b. From $p = q \cdot \left(x^2 + 1\right) + r$, we obtain $p - r = q \cdot \left(x^2 + 1\right) \in \left(x^2 + 1\right)\mathbb{R}[x]$; thus, $\overline{p} = \overline{r}$ in the quotient ring $\mathbb{R}[x] / \left(x^2 + 1\right)$. Now,

$$\begin{aligned} u = \overline{p} = \overline{r} &= \overline{a + bx} \qquad (\text{since } r = a + bx), \qquad \text{so that} \\ f'(u) &= f'\left(\overline{a + bx}\right) = (a + bx)[i] \qquad (\text{by (98)}) \\ &= a + bi. \end{aligned}$$

Hence, $a + bi = f'(u) = 0$ (since $u \in \operatorname{Ker}(f')$). Since $a, b \in \mathbb{R}$, this entails $a = b = 0$ (since the complex numbers 1 and i are $\mathbb{R}$-linearly independent). Thus, $u = \overline{a + bx}$ rewrites as $u = \overline{0 + 0x} = 0 \in \{0\}$.

Forget that we fixed u. We thus have shown that $u \in \{0\}$ for each $u \in \operatorname{Ker}(f')$. In other words, $\operatorname{Ker}(f') \subseteq \{0\}$. Since the reverse inclusion $\{0\} \subseteq \operatorname{Ker}(f')$ is obvious, we thus conclude that $\operatorname{Ker}(f') = \{0\}$. As we have said, this entails that f' is injective.

Now we know that the map f' is injective and surjective. Hence, f' is bijective, i.e., invertible. Since every invertible $\mathbb{R}$-algebra morphism is an $\mathbb{R}$-algebra isomorphism (by Proposition 3.11.8), we thus conclude that f' is an $\mathbb{R}$-algebra isomorphism. This proves Proposition 4.5.2 (since the map f' satisfies $f'(\overline{p}) = p[i]$ for each $p \in \mathbb{R}[x]$, and thus is precisely the alleged isomorphism claimed in Proposition 4.5.2). □

Note the use of polynomial division (with remainder) in our above proof of Proposition 4.5.2. It has a natural usefulness in the study of quotient rings of $\mathbb{R}[x]$, just as integer division (with remainder) is crucial to the study of quotient rings of $\mathbb{Z}$.

Similarly to Proposition 4.5.2, we can reveal further quotient rings of polynomial rings as certain rings we know:

Proposition 4.5.3.

(a) Recall the ring $\mathbb{Z}[i]$ of Gaussian integers. We have $\mathbb{Z}[x] / \left(x^2+1\right) \cong \mathbb{Z}[i]$ as $\mathbb{Z}$-algebras. More concretely: There is a $\mathbb{Z}$-algebra isomorphism

$$\begin{aligned} \mathbb{Z}[x] / \left(x^2+1\right) &\to \mathbb{Z}[i], \\ \overline{p} &\mapsto p[i]. \end{aligned}$$

(b) Recall the ring $\mathbb{S} = \mathbb{Q}\left[\sqrt{5}\right] = \left\{a+b\sqrt{5} \mid a, b \in \mathbb{Q}\right\}$ (a subring of $\mathbb{R}$). We have $\mathbb{Q}[x] / \left(x^2-5\right) \cong \mathbb{S}$ as $\mathbb{Q}$-algebras. More concretely: There is a $\mathbb{Q}$-algebra isomorphism

$$\begin{aligned} \mathbb{Q}[x] / \left(x^2-5\right) &\to \mathbb{S}, \\ \overline{p} &\mapsto p\left[\sqrt{5}\right]. \end{aligned}$$

Proof. **(a)** Analogous to the proof of Proposition 4.5.2.
(b) Analogous to the proof of Proposition 4.5.2. □

Proposition 4.5.2 and Proposition 4.5.3 suggest that when we start with a ring R and a polynomial $b \in R[x]$, then the quotient ring $R[x]/b$ is (in some way) an "extension" of R by a root of b, in the sense that it contains R as a subring (at least up to isomorphism) but also contains a root of b (namely, $\overline{x}$). Thus, we can hope that by taking the quotient ring $R[x]/b$, we can "adjoin" a root of b to the ring R even if b has no root in R (just as Cardano defined the complex numbers by "adjoining" a root of x^2+1 to $\mathbb{R}$). The word "adjoin" here means something like "insert", "attach" or "throw in".

This is a good intuition, but there are nuances: In the process of "adjoining" our root to our ring R, we may end up making R "smaller", in the sense that different elements of R become equal when the root is "adjoined" (and thus the resulting ring is not really an "extension" of R). The following example (in which we take a quotient of $\mathbb{Z}[x]$ by a constant polynomial) demonstrates this:

Proposition 4.5.4.

(a) We have $(\mathbb{Z}[x])/m \cong (\mathbb{Z}/m)[x]$ as $\mathbb{Z}$-algebras (i.e., as rings) for any integer m.

(b) The ring $(\mathbb{Z}[x])/1$ is trivial.

Proof sketch. **(a)** Let m be an integer. Then, the principal ideal $m\mathbb{Z}[x]$ of $\mathbb{Z}[x]$ consists of all polynomials whose all coefficients are multiples of m. Thus, it is

easy to see that the map

$$f : (\mathbb{Z}[x])/m \to (\mathbb{Z}/m)[x],$$
$$\overline{a_0x^0 + a_1x^1 + a_2x^2 + \cdots} \mapsto \overline{a_0}x^0 + \overline{a_1}x^1 + \overline{a_2}x^2 + \cdots$$

is well-defined and is a $\mathbb{Z}$-algebra isomorphism. This proves Proposition 4.5.4 **(a)**.

(b) More generally: If R is any commutative ring, then the ring $R/1$ is trivial. This is because the principal ideal $1R$ of R is the whole ring R, so there is only one coset modulo this ideal. □

Proposition 4.5.4 **(a)** (applied to $m = 2$) shows that if we take the quotient ring of $\mathbb{Z}[x]$ modulo (the principal ideal generated by) the constant polynomial 2, then we don't get an "extension" of $\mathbb{Z}$; what we instead get is the polynomial ring $(\mathbb{Z}/2)[x]$, in which (unlike in $\mathbb{Z}$) we have $1 + 1 = 0$ (so it certainly cannot contain a copy of $\mathbb{Z}$ as a subring). But if you think about this carefully, you will realize that this perfectly agrees with the idea of "adjoining a root". Indeed, to "adjoin" a root of the constant polynomial 2 to $\mathbb{Z}$ means to introduce a new "number" x satisfying $2 = 0$. The equation $2 = 0$ tells us nothing about the "number" x (so it remains completely unconstrained), but collapses all even integers to 0, thus leaving us with the ring $(\mathbb{Z}/2)[x]$. This is precisely what Proposition 4.5.4 **(a)** told us. Likewise, "adjoining" a root of 1 to $\mathbb{Z}$ causes $1 = 0$, which renders the ring trivial (since any element of a ring is a multiple of 1); this agrees with Proposition 4.5.4 **(b)**.

The examples so far have taught us that – yes – we can "adjoin" a root of any polynomial to a commutative ring R, but we don't always get an extension of R (although we do always get an R-algebra). In Theorem 4.5.9 **(c)**, we will see a (sufficient) criterion for when we do.

Here is another natural question: What happens if we "adjoin" a root of a polynomial b that already has a root in R ? For example, let us take the polynomial $x^2 - 1$ over $\mathbb{Q}$ (which has 1 and -1 as roots). It turns out that the resulting quotient ring $\mathbb{Q}[x] / \left(x^2 - 1\right)$ is a good friend of ours by now:

Proposition 4.5.5. Recall the group algebra $\mathbb{Q}[C_2]$ of the cyclic group C_2 from Example 4.1.4. Then,

$$\mathbb{Q}[x] / \left(x^2 - 1\right) \cong \mathbb{Q}[C_2] \cong \mathbb{Q} \times \mathbb{Q} \qquad \text{as } \mathbb{Q}\text{-algebras.}$$

Proof. In Example 4.1.4, we have seen that the group algebra $\mathbb{Q}[C_2]$ has a basis (e_1, e_u) (as a $\mathbb{Q}$-module). By Convention 4.1.8, we can write 1 and u for e_1 and e_u, so that this basis becomes $(1, u)$. We also know (from Example 4.1.4) that $\mathbb{Q}[C_2] \cong \mathbb{Q} \times \mathbb{Q}$ as $\mathbb{Q}$-algebras. It thus remains to prove that $\mathbb{Q}[x] / \left(x^2 - 1\right) \cong \mathbb{Q}[C_2]$.

Note the similarity between $\mathbb{Q}[C_2]$ and $\mathbb{C}$:

- The $\mathbb{Q}$-module $\mathbb{Q}[C_2]$ has basis $(1, u)$, with $u^2 = 1$.
- The $\mathbb{R}$-module $\mathbb{C}$ has basis $(1, i)$, with $i^2 = -1$.

This suggests that we just copypaste our above proof of Proposition 4.5.2, replacing $\mathbb{R}$, $\mathbb{C}$ and i by $\mathbb{Q}$, $\mathbb{Q}[C_2]$ and u and occasionally flipping signs. This is precisely what we are now going to do (but in a smaller font, to avoid wasting paper).

Theorem 4.2.8 (applied to $R = \mathbb{Q}$ and $A = \mathbb{Q}[C_2]$ and $a = u$) yields that the map

$$\begin{aligned} f : \mathbb{Q}[x] &\to \mathbb{Q}[C_2], \\ p &\mapsto p[u] \end{aligned}$$

is a $\mathbb{Q}$-algebra morphism. This map f sends the principal ideal $\left(x^2-1\right)\mathbb{Q}[x]$ to 0, because for each $q \in \mathbb{Q}[x]$, we have

$$f\left(\left(x^2-1\right)\cdot q\right) = \left(\left(x^2-1\right)\cdot q\right)[u] = \underbrace{\left(u^2-1\right)}_{\substack{=0 \\ (\text{since } u^2=1)}} \cdot q[u] = 0.$$

Hence, Theorem 4.4.3 (applied to $R = \mathbb{Q}$, $A = \mathbb{Q}[x]$, $I = \left(x^2-1\right)\mathbb{Q}[x]$ and $B = \mathbb{Q}[C_2]$) shows that the map

$$\begin{aligned} f' : \mathbb{Q}[x] / \left(x^2-1\right) &\to \mathbb{Q}[C_2], \\ \overline{a} &\mapsto f(a) \end{aligned}$$

is well-defined and is a $\mathbb{Q}$-algebra morphism. Consider this f'. Each $p \in \mathbb{Q}[x]$ satisfies

$$\begin{aligned} f'(\overline{p}) &= f(p) && \left(\text{by the definition of } f'\right) \\ &= p[u] && (\text{by the definition of } f). \end{aligned} \tag{99}$$

Now, why is f' an isomorphism?

It's not hard to see that f' is surjective: Indeed, any $z \in \mathbb{Q}[C_2]$ can be written as $z = a + bu$ for some $a, b \in \mathbb{Q}$, and then we have $z = a + bu = f'\left(\overline{a+bx}\right)$ (since (99) yields $f'\left(\overline{a+bx}\right) = (a+bx)[u] = a + bu$).

Now, how can we prove that f' is injective? Since f' is $\mathbb{Q}$-linear, it suffices to show that $\operatorname{Ker}(f') = \{0\}$ (by Lemma 3.5.10).

Let $u \in \operatorname{Ker}(f')$. Thus, $u \in \mathbb{Q}[x] / \left(x^2-1\right)$, so that $u = \overline{p}$ for some $p \in \mathbb{Q}[x]$. Consider this p.

However, Theorem 4.3.7 **(a)** (applied to $R = \mathbb{Q}$, $b = x^2-1$ and $a = p$) yields that there is a unique pair (q, r) of polynomials in $\mathbb{Q}[x]$ such that

$$p = q \cdot \left(x^2-1\right) + r \qquad \text{and} \qquad \deg r < \deg\left(x^2-1\right).$$

Consider this pair (q, r). From $\deg r < \deg\left(x^2-1\right) = 2$, we see that the polynomial r can be written as $a + bx$ for some $a, b \in \mathbb{Q}$. Consider these a, b. From $p = q \cdot \left(x^2-1\right) +$

r, we obtain $p - r = q \cdot \left(x^2 - 1\right) \in \left(x^2 - 1\right) \mathbb{Q}[x]$; thus, $\overline{p} = \overline{r}$ in the quotient ring $\mathbb{Q}[x] / \left(x^2 - 1\right)$. Now,

$$\begin{aligned} u = \overline{p} = \overline{r} &= \overline{a + bx} \qquad (\text{since } r = a + bx), \qquad \text{so that} \\ f'(u) &= f'\left(\overline{a + bx}\right) = (a + bx)[u] \qquad (\text{by (99)}) \\ &= a + bu. \end{aligned}$$

Hence, $a + bu = f'(u) = 0$ (since $u \in \operatorname{Ker}(f')$). Since $a, b \in \mathbb{Q}$, this entails $a = b = 0$ (since the vectors 1 and u in $\mathbb{Q}[C_2]$ are $\mathbb{Q}$-linearly independent). Thus, $u = \overline{a + bx}$ rewrites as $u = \overline{0 + 0x} = 0 \in \{0\}$.

Forget that we fixed u. We thus have shown that $u \in \{0\}$ for each $u \in \operatorname{Ker}(f')$. In other words, $\operatorname{Ker}(f') \subseteq \{0\}$. Since the reverse inclusion $\{0\} \subseteq \operatorname{Ker}(f')$ is obvious, we thus conclude that $\operatorname{Ker}(f') = \{0\}$. As we have said, this entails that f' is injective.

Now we know that the map f' is injective and surjective. Hence, f' is bijective, i.e., invertible. Since every invertible $\mathbb{Q}$-algebra morphism is a $\mathbb{Q}$-algebra isomorphism (by Proposition 3.11.8), we thus conclude that f' is an $\mathbb{Q}$-algebra isomorphism. Hence, $\mathbb{Q}[x] / \left(x^2 - 1\right) \cong \mathbb{Q}[C_2]$. As we said, this proves Proposition 4.5.5. □

Exercise 4.5.1. Let R be a commutative ring. Recall the R-algebra $\mathbb{D}_R$ defined in Exercise 3.11.2, along with the element $\varepsilon = (0, 1) \in \mathbb{D}_R$ defined ibidem. Prove that there is an R-algebra isomorphism

$$\begin{aligned} R[x] / \left(x^2\right) &\to \mathbb{D}_R, \\ \overline{p} &\mapsto p[\varepsilon]. \end{aligned}$$

Exercise 4.5.2. Let φ be the **golden ratio** – i.e., the real number $\dfrac{1 + \sqrt{5}}{2} \approx 1.618\ldots$. Let $\mathbb{Z}[\varphi]$ be the set of all reals of the form $a + b\varphi$ with $a, b \in \mathbb{Z}$.

(a) Prove that $\mathbb{Z}[\varphi]$ is a subring of $\mathbb{R}$.

(b) Prove that

$$\mathbb{Z}[\varphi] \cong \mathcal{F} \cong \mathbb{Z}[x] / \left(x^2 - x - 1\right) \qquad \text{as rings,}$$

where $\mathcal{F}$ is the ring defined in Exercise 2.3.6.

Exercise 4.5.3. Let R be the commutative group algebra $\mathbb{Q}[C_3]$ discussed in Example 4.1.6. Consider its idempotent element $z = \dfrac{1 + e_u + e_v}{3} = \dfrac{1 + u + v}{3}$. Let S be the principal ideal $(1 - z) R$ of R. As we know from Exercise 2.10.4 **(b)** (applied to $e = z$), this principal ideal S is itself a ring, with addition and multiplication inherited from R and with zero 0_R and with unity $1 - z$.

(a) Prove that this ring S is isomorphic to $\mathbb{Q}[x] / \left(x^2 + x + 1\right)$ as rings.

(b) Prove that S is furthermore isomorphic to the subring

$$\mathbb{Q}\left[\sqrt{-3}\right] = \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Q}\right\} \qquad \text{of } \mathbb{C}.$$

[**Hint:** For part **(a)**, first show that

$$S = \{a + bu + cv \mid a, b, c \in \mathbb{Q} \text{ with } a + b + c = 0\}.$$

Then, show that the $\mathbb{Q}$-algebra morphism

$$f : \mathbb{Q}[x] / \left(x^2 + x + 1\right) \to S, \\ \overline{p} \mapsto p\left[u\left(1 - z\right)\right]$$

is well-defined and invertible. The quickest way to verify invertibility is using linear algebra over $\mathbb{Q}$, as f is a $\mathbb{Q}$-linear map between two 2-dimensional $\mathbb{Q}$-vector spaces.

For part **(b)**, find a root of the polynomial $x^2 + x + 1$ in $\mathbb{Q}\left[\sqrt{-3}\right]$.]

In our proofs of Propositions 4.5.2, 4.5.5 and 4.5.3 (even though I left the latter to the reader), we used that the leading coefficients of the polynomials we were quotienting out were units. Indeed, this is what allowed us to apply Theorem 4.3.7 **(a)**, which was a crucial step in proving that f' is injective. Describing quotient rings becomes much more complicated when the leading coefficient of the polynomial is not a unit. Sometimes it is nevertheless possible. Here is a particularly well-behaved example:

Proposition 4.5.6. Fix a nonzero integer m. Define the ring R_m as in Exercise 2.3.2; that is, R_m is the subring

$$\left\{r \in \mathbb{Z} \mid \text{there exists an } m \in \mathbb{N} \text{ satisfying } m^k r \in \mathbb{Z}\right\}$$

of $\mathbb{Q}$. Then,

$$\mathbb{Z}[x] / (mx - 1) \cong R_m \qquad \text{as } \mathbb{Z}\text{-algebras (i.e., as rings).}$$

More concretely: There is a $\mathbb{Z}$-algebra isomorphism

$$\mathbb{Z}[x] / (mx - 1) \to R_m, \\ \overline{p} \mapsto p\left[\frac{1}{m}\right].$$

Proof sketch. Intuitively, this should be exactly what you expect: According to our "adjoining roots" philosophy, the ring $\mathbb{Z}[x] / (mx - 1)$ is what you get if you "adjoin" a root of the polynomial $mx - 1$ to $\mathbb{Z}$. But such a root would behave like the rational number $\dfrac{1}{m}$; so it is no surprise that the resulting ring

would be isomorphic to R_m (since R_m is really just "the numbers you can get if you start with the integers and also allow multiplying by $\frac{1}{m}$"). This, of course, is not a proof.

An actual proof can be done along the following lines:

1. Show that a $\mathbb{Z}$-algebra morphism
$$\begin{aligned} \alpha : \mathbb{Z}[x] / (mx-1) &\to R_m, \\ \overline{p} &\mapsto p\left[\frac{1}{m}\right] \end{aligned}$$
exists. This is similar to the corresponding part of the proof of Proposition 4.5.2 (where we called the corresponding morphism f' rather than α); the main roles are played by Theorem 4.2.8 and Theorem 4.4.3.

2. (Optional:) Show that this morphism α is surjective. (In fact, each element of R_m has the form $\frac{a}{m^k}$ for some $a \in \mathbb{Z}$ and some $k \in \mathbb{N}$, and thus equals $\alpha\left(\overline{ax^k}\right)$.)

3. Don't waste your time trying to show that α is injective; there is no quick way to prove this directly.

4. Show that there is a map
$$\begin{aligned} \beta : R_m &\to \mathbb{Z}[x] / (mx-1), \\ \frac{a}{m^k} &\mapsto \overline{ax^k} \qquad (\text{where } a \in \mathbb{Z} \text{ and } k \in \mathbb{N}). \end{aligned}$$
(You need to show that this is well-defined – i.e., that if an element of R_m has been written in the form $\frac{a}{m^k}$ in two different ways, then the resulting residue classes $\overline{ax^k}$ will be equal.)

5. Show that β is a $\mathbb{Z}$-algebra morphism. (This is an exercise in bringing fractions to a common denominator.)

6. Show that $\beta \circ \alpha = \mathrm{id}$. (Indeed, $\beta \circ \alpha$ is a $\mathbb{Z}$-algebra morphism, since β and α are $\mathbb{Z}$-algebra morphisms. Moreover, it is easy to show that $(\beta \circ \alpha)(\overline{x}) = \overline{x}$. Hence, $(\beta \circ \alpha)\left(\sum_{i=0}^{n} c_i \overline{x}^i\right) = \sum_{i=0}^{n} c_i \overline{x}^i$ for each $n \in \mathbb{N}$ and any coefficients $c_0, c_1, \ldots, c_n \in \mathbb{Z}$ (since $\beta \circ \alpha$ is a $\mathbb{Z}$-algebra morphism). But this is saying that $\beta \circ \alpha = \mathrm{id}$, since every element of $\mathbb{Z}[x] / (mx-1)$ can be written as $\sum_{i=0}^{n} c_i \overline{x}^i$ for some $n \in \mathbb{N}$ and some coefficients $c_0, c_1, \ldots, c_n \in \mathbb{Z}$.)

7. Show that $\alpha \circ \beta = \mathrm{id}$. (Indeed, if you have done Step 2, then this follows from $\beta \circ \alpha = \mathrm{id}$. Otherwise, show it directly.)

8. Conclude from Steps 6 and 7 that the maps α and β are mutually inverse, and thus α is invertible. Since α is a $\mathbb{Z}$-algebra morphism, this entails that α is a $\mathbb{Z}$-algebra isomorphism, and you are done. □

4.5.2. The general construction

In the previous subsection, we have seen a few examples of the construction in which we start with a commutative ring R and a polynomial $b \in R[x]$, and construct the quotient ring $R[x]/b$. To recall, the bottom line of this construction is "throw a new root of b into the ring R and see what happens". Often, this produces a ring extension of R – i.e., a larger ring that contains R as a subring. (For example, this happens if $R = \mathbb{R}$ and $b = x^2 + 1$; this is how Cardano defined the complex numbers.) However, this doesn't always go well. Sometimes, what happens instead is that the ring R collapses to a trivial ring (e.g., if $b = 1$) or at least becomes smaller (e.g., we have $(\mathbb{Z}/6)[x]/(2x-1) \cong \mathbb{Z}/3$). Sometimes, the ring loses some of its properties: e.g., if we throw a new root of $x^2 - 1$ into the field $\mathbb{Q}$, then the resulting ring $\mathbb{Q}[x]/\left(x^2-1\right)$ not only fails to be a field, but even fails to be an integral domain (indeed, we have seen that this ring is isomorphic to $\mathbb{Q} \times \mathbb{Q}$).

Let us put these things in order. First, let us show that the residue class $\overline{x}$ in $R[x]/b$ is a root of b, so that our construction really creates a root of b:

Proposition 4.5.7. Let $b \in R[x]$ be a polynomial. (Recall that R is still a fixed commutative ring.)

(a) The projection map

$$\begin{aligned} \pi_b : R[x] &\to R[x]/b, \\ p &\mapsto \overline{p} \end{aligned}$$

is an $R[x]$-algebra morphism, and thus an R-algebra morphism.

(b) The map[141]

$$\begin{aligned} R &\to R[x]/b, \\ r &\mapsto \overline{r} \end{aligned}$$

is an R-algebra morphism.

(c) For any $p \in R[x]$, we have $p[\overline{x}] = \overline{p}$ in $R[x]/b$.

(d) The element $\overline{x} \in R[x]/b$ is a root of b.

None of this is difficult to prove, but the following proposition will make the proof (even) more comfortable:

Proposition 4.5.8 ("Polynomials commute with algebra morphisms")**.** Let A and B be two R-algebras. Let $f : A \to B$ be an R-algebra morphism. Let $a \in A$. Let $p \in R[x]$ be a polynomial. Then,

$$f(p[a]) = p[f(a)].$$

Proof of Proposition 4.5.8. Let us give a proof by example: Set $p = 5x^4 + x^3 + 7x^1$. Then, $p[a] = 5a^4 + a^3 + 7a^1$ and $p[f(a)] = 5f(a)^4 + f(a)^3 + 7f(a)^1$. Thus, the claim we have to prove rewrites as

$$f\left(5a^4 + a^3 + 7a^1\right) = 5f(a)^4 + f(a)^3 + 7f(a)^1.$$

But this follows easily from the fact that f is an R-algebra morphism: Indeed,

$$\begin{aligned} f\left(5a^4 + a^3 + 7a^1\right) &= f\left(5a^4\right) + f\left(a^3\right) + f\left(7a^1\right) && \text{(since } f \text{ respects addition)} \\ &= 5f\left(a^4\right) + f\left(a^3\right) + 7f\left(a^1\right) && \text{(since } f \text{ respects scaling)} \\ &= 5f(a)^4 + f(a)^3 + 7f(a)^1 && \text{(since } f \text{ respects powers)}. \end{aligned}$$

The rigorous proof in the general case is LTTR. □

Proof of Proposition 4.5.7. **(a)** This follows from the general fact (Theorem 4.4.1 **(c)**) that the canonical projection from an R-algebra to its quotient is an R-algebra morphism. Note that we need to apply this fact to $R[x]$ instead of R here, in order to conclude that the map in question is an $R[x]$-algebra morphism.

(b) The map

$$\begin{aligned} R &\to R[x]/b, \\ r &\mapsto \overline{r} \end{aligned}$$

is the composition of the projection map π_b from part **(a)** with the inclusion map

$$\begin{aligned} R &\to R[x], \\ r &\mapsto r = rx^0. \end{aligned}$$

[141] Note the difference between the maps in part **(a)** and in part **(b)**: The map in part **(a)** takes as input a polynomial $p \in R[x]$, whereas the map in part **(b)** takes as input a scalar $r \in R$ (and treats it as a constant polynomial, i.e., as $rx^0 \in R[x]$). If you regard R as a subring of $R[x]$, you can thus view the map in part **(b)** as a restriction of the map in part **(a)**.

Thus, it is a composition of two R-algebra morphisms (since both π_b and the inclusion map are R-algebra morphisms). Hence, it is an R-algebra morphism itself[142]. This proves Proposition 4.5.7 **(b)**.

(c) Here is an abstract argument: Let $p \in R[x]$. The projection map π_b from Proposition 4.5.7 **(a)** is an R-algebra morphism (by Proposition 4.5.7 **(a)**). Hence, Proposition 4.5.8 (applied to $A = R[x]$ and $B = R[x]/b$ and $a = x$ and $f = \pi_b$) yields

$$\pi_b(p[x]) = p[\pi_b(x)]. \tag{100}$$

However, the definition of π_b yields $\pi_b(p[x]) = \overline{p[x]} = \overline{p}$ (since $p[x] = p$) and $\pi_b(x) = \overline{x}$. Hence, (100) rewrites as $\overline{p} = p[\overline{x}]$. This proves Proposition 4.5.7 **(c)**.

Alternatively, you can prove it directly by writing p as $p = \sum_{i=0}^{n} p_i x^i$ with $p_i \in R$. (Indeed, if you do this, then the claim rewrites as $\sum_{i=0}^{n} p_i \overline{x}^i = \overline{\sum_{i=0}^{n} p_i x^i}$; but this is an easy consequence of how the quotient $R[x]/b$ was defined.)

(d) Proposition 4.5.7 **(c)** (applied to $p = b$) yields $b[\overline{x}] = \overline{b} = \overline{0}$ (since $b \in bR[x]$). In other words, $\overline{x}$ is a root of b. This proves Proposition 4.5.7 **(d)**. □

Next, for a large class of polynomials $b \in R[x]$ (including the monic ones, and all the nonzero polynomials over a field), we are going to show what $R[x]/b$ looks like as an R-module:

Theorem 4.5.9. Let $m \in \mathbb{N}$. Let $b \in R[x]$ be a polynomial of degree m such that its leading coefficient $[x^m]\, b$ is a unit of R. Then:

(a) Each element of $R[x]/b$ can be uniquely written in the form

$$a_0\overline{x^0} + a_1\overline{x^1} + \cdots + a_{m-1}\overline{x^{m-1}} \qquad \text{with } a_0, a_1, \ldots, a_{m-1} \in R.$$

(b) The m vectors $\overline{x^0}, \overline{x^1}, \ldots, \overline{x^{m-1}}$ form a basis of the R-module $R[x]/b$. Thus, this R-module $R[x]/b$ is free of rank $m = \deg b$.

(c) Assume that $m > 0$. Then, the R-algebra morphism[143]

$$R \to R[x]/b,$$
$$r \mapsto \overline{r}$$

is injective. Therefore, R can be viewed as an R-subalgebra (thus a subring) of $R[x]/b$ if we identify each $r \in R$ with its image $\overline{r} \in R[x]/b$.

(d) In particular, under the assumption that $m > 0$, there exists a commutative ring that contains R as a subring and that contains a root of b.

[142] Indeed, there is an easy fact (which we never stated, but which is completely straightforward to prove after what we have seen) that any composition of two R-algebra morphisms is itself an R-algebra morphism.

Proof. **(a)** Let $\alpha \in R[x]/b$. Then, $\alpha = \overline{a}$ for some polynomial $a \in R[x]$. Consider this a. The division-with-remainder theorem for polynomials (Theorem 4.3.7 **(a)**) tells us that there is a unique pair (q, r) of polynomials in $R[x]$ such that

$$a = qb + r \qquad \text{and} \qquad \deg r < \deg b.$$

Consider this pair (q, r). Then, in $R[x]/b$, we have $\overline{a} = \overline{r}$ (since $a = qb + r$ entails $a - r = qb = bq \in bR[x]$).

We have $\deg r < \deg b = m$; thus, we can write r in the form $r = r_0 x^0 + r_1 x^1 + \cdots + r_{m-1} x^{m-1}$ for some $r_0, r_1, \ldots, r_{m-1} \in R$. Consider these $r_0, r_1, \ldots, r_{m-1}$. We have

$$\begin{aligned}\alpha = \overline{a} = \overline{r} &= \overline{r_0 x^0 + r_1 x^1 + \cdots + r_{m-1} x^{m-1}} \\ &\qquad \left(\text{since } r = r_0 x^0 + r_1 x^1 + \cdots + r_{m-1} x^{m-1}\right) \\ &= r_0 \overline{x^0} + r_1 \overline{x^1} + \cdots + r_{m-1} \overline{x^{m-1}}\end{aligned}$$

(since the scaling and the addition of the quotient algebra $R[x]/b$ were inherited from $R[x]$).

Thus, we have represented our $\alpha \in R[x]/b$ in the form

$$a_0 \overline{x^0} + a_1 \overline{x^1} + \cdots + a_{m-1} \overline{x^{m-1}} \qquad \text{with } a_0, a_1, \ldots, a_{m-1} \in R$$

(namely, for $a_i = r_i$). It remains to show that this representation is unique.

This can be shown by walking the above proof backwards and using the uniqueness part of the division-with-remainder theorem. Here are the details: Assume that

$$\alpha = b_0 \overline{x^0} + b_1 \overline{x^1} + \cdots + b_{m-1} \overline{x^{m-1}} \qquad \text{with } b_0, b_1, \ldots, b_{m-1} \in R$$

is some representation of α in the above form. We must then show that this representation is actually the representation that we constructed above – i.e., that we have $b_i = r_i$ for each $i \in \{0, 1, \ldots, m-1\}$.

Indeed, define a polynomial $s \in R[x]$ by $s = b_0 x^0 + b_1 x^1 + \cdots + b_{m-1} x^{m-1}$. Then, $\deg s \leq m - 1 < m = \deg b$. Also,

$$\overline{a} = \alpha = b_0 \overline{x^0} + b_1 \overline{x^1} + \cdots + b_{m-1} \overline{x^{m-1}} = \overline{b_0 x^0 + b_1 x^1 + \cdots + b_{m-1} x^{m-1}} = \overline{s}$$

(since $b_0 x^0 + b_1 x^1 + \cdots + b_{m-1} x^{m-1} = s$). In other words, $a - s \in bR[x]$. In other words,

$$a - s = bd \qquad \text{for some } d \in R[x].$$

Consider this d. Thus, $a = bd + s = db + s$. Now, the pair (d, s) is a pair of polynomials in $R[x]$ satisfying $a = db + s$ and $\deg s < \deg b$. This means that it satisfies the exact conditions that the pair (q, r) was asked to satisfy. However,

[143] This is the map from Proposition 4.5.7 **(b)**.

the division-with-remainder theorem for polynomials said that the pair (q, r) satisfying those conditions was unique. Hence, we must have $(d, s) = (q, r)$ (since (d, s) satisfies the same conditions as (q, r)). Thus, $d = q$ and $s = r$.

Now,

$$b_0 x^0 + b_1 x^1 + \cdots + b_{m-1} x^{m-1} = s = r = r_0 x^0 + r_1 x^1 + \cdots + r_{m-1} x^{m-1}.$$

Comparing coefficients in these polynomials, we conclude that $b_i = r_i$ for each $i \in \{0, 1, \ldots, m-1\}$ (since $\left(x^0, x^1, x^2, \ldots\right)$ is a basis of the R-module $R[x]$). This is what we needed to show. Theorem 4.5.9 **(a)** is thus proved.

(b) This is just Theorem 4.5.9 **(a)**, rewritten in terms of modules and bases. In some more detail:

- Each element of $R[x]/b$ can be written in the form

$$a_0 \overline{x^0} + a_1 \overline{x^1} + \cdots + a_{m-1} \overline{x^{m-1}} \qquad \text{with } a_0, a_1, \ldots, a_{m-1} \in R$$

  (according to Theorem 4.5.9 **(a)**). In other words, each element of $R[x]/b$ is an R-linear combination of $\overline{x^0}, \overline{x^1}, \ldots, \overline{x^{m-1}}$. Thus, the list $\left(\overline{x^0}, \overline{x^1}, \ldots, \overline{x^{m-1}}\right)$ spans the R-module $R[x]/b$.

- Each element of $R[x]/b$ can be **uniquely** represented in the form

$$a_0 \overline{x^0} + a_1 \overline{x^1} + \cdots + a_{m-1} \overline{x^{m-1}} \qquad \text{with } a_0, a_1, \ldots, a_{m-1} \in R$$

  (according to Theorem 4.5.9 **(a)**). Hence, in particular, the zero vector $\overline{0} \in R[x]/b$ can be **uniquely** represented in this form. But it is clear how to represent $\overline{0}$ in this form: We just write

$$\overline{0} = 0\overline{x^0} + 0\overline{x^1} + \cdots + 0\overline{x^{m-1}}.$$

  Since we have just said that $\overline{0}$ can be **uniquely** represented in this form, we thus conclude that this is the **only** way to represent $\overline{0}$ in this form. In other words, if $\overline{0}$ has been represented in the form $a_0 \overline{x^0} + a_1 \overline{x^1} + \cdots + a_{m-1} \overline{x^{m-1}}$ with $a_0, a_1, \ldots, a_{m-1} \in R$, then we must have $a_0 = a_1 = \cdots = a_{m-1} = 0$. In other words, if $a_0, a_1, \ldots, a_{m-1} \in R$ satisfy $a_0 \overline{x^0} + a_1 \overline{x^1} + \cdots + a_{m-1} \overline{x^{m-1}} = \overline{0}$, then $a_0 = a_1 = \cdots = a_{m-1} = 0$. But this is saying precisely that the list $\left(\overline{x^0}, \overline{x^1}, \ldots, \overline{x^{m-1}}\right)$ is R-linearly independent.

Thus, we have shown that the list $\left(\overline{x^0}, \overline{x^1}, \ldots, \overline{x^{m-1}}\right)$ is R-linearly independent and spans $R[x]/b$. In other words, this list is a basis of $R[x]/b$. This proves Theorem 4.5.9 **(b)**.

(c) We know (from Proposition 4.5.7 **(b)**) that the map

$$\begin{aligned} R &\to R\left[x\right]/b, \\ r &\mapsto \overline{r} \end{aligned}$$

is an R-algebra morphism. We only need to show that it is injective. It clearly suffices to show that its kernel is $\{0\}$ (because we know that an R-module morphism is injective if and only if its kernel is $\{0\}$).

So let r be in the kernel of this morphism. We must prove that $r = 0$.

Since r is in the kernel of the above morphism, we have $\overline{r} = 0$ in $R\left[x\right]/b$. In other words, r is a multiple of b. In other words, $r = bc$ for some polynomial $c \in R\left[x\right]$. Consider this c. From $r = bc$, we obtain $\deg r = \deg\left(bc\right) = \deg b + \deg c$ (by Proposition 4.3.5 **(b)**, since the leading coefficient of b is a unit). Thus, $\deg b + \deg c = \deg r \leq 0$ (since r is constant). However, $\deg b = m > 0$ by assumption. Hence, $\deg b > 0 \geq \deg b + \deg c$. This entails $\deg c < 0$. This means that $c = 0$, whence $r = b\underbrace{c}_{=0} = 0$.

Forget that we fixed r. We thus have proved that if r is in the kernel of our morphism, then $r = 0$. Hence, the kernel of our morphism is $\{0\}$ (since 0 is clearly in its kernel). Thus, the morphism is injective, and Theorem 4.5.9 **(c)** is proven.

(d) Assume that $m > 0$. The ring $R\left[x\right]/b$ contains a root of b (namely, $\overline{x}$, according to Proposition 4.5.7 **(d)**), and also contains "a copy of R", in the sense that there is an injective ring morphism from R to $R\left[x\right]/b$ (namely, the one we constructed in Theorem 4.5.9 **(c)**). If we replace this copy of R by the original R (by replacing each $\overline{r} \in R\left[x\right]/b$ with the corresponding $r \in R$), then we obtain a ring that contains R as a subring but also contains a root of b. This proves Theorem 4.5.9 **(d)**. □

Let us summarize: We have generalized the construction of $\mathbb{C}$. Namely, we have found a way to "adjoin" a root of a polynomial $b \in R\left[x\right]$ to a commutative ring R by forming the quotient ring $R\left[x\right]/b$. This latter ring is always a commutative ring and an R-algebra. Moreover, if b is "nice" (that is, we have $\deg b > 0$, and the leading coefficient of b is a unit), then this latter ring $R\left[x\right]/b$ will contain R as a subring (by Theorem 4.5.9 **(c)**) and also will be a free R-module of rank $\deg b$ (by Theorem 4.5.9 **(b)**). If b is not as "nice", then the ring $R\left[x\right]/b$ may fail to contain R as a subring (even though it still is an R-algebra), and may be smaller than R or even trivial.

4.6. Field extensions from adjoining roots

Let F be a field. Then, any non-constant univariate polynomial $b \in F\left[x\right]$ is "nice" in the sense of the preceding paragraph, so that $F\left[x\right]/b$ is a commutative ring that contains F as a subring and that contains a root of b. When will this ring $F\left[x\right]/b$ be a field?

We first state a simple fact about the units of $F[x]$:

Proposition 4.6.1. Let F be a field. The units of the polynomial ring $F[x]$ are precisely the nonzero constant polynomials.

Proof. Any nonzero constant polynomial is a unit of $F[x]$ (since it is a unit of F). Conversely, any unit of $F[x]$ must be a nonzero constant polynomial[144]. □

Recall (from Theorem 4.3.22) that $F[x]$ is a Euclidean domain, hence a PID (by Proposition 2.14.2), hence a UFD (by Theorem 2.15.11). Furthermore, an element $p \in F[x]$ is prime[145] if and only if it is irreducible (by Proposition 2.15.4, since $F[x]$ is a PID). The notion of "irreducible" in $F[x]$ is precisely the classical concept of an irreducible polynomial:

Proposition 4.6.2. Let F be a field. Let $p \in F[x]$. Then, p is irreducible if and only if p is non-constant and cannot be written as a product of two non-constant polynomials.

Proof. The definition of "irreducible" says that p is irreducible if and only if p is nonzero and not a unit and has the property that whenever $a, b \in F[x]$ satisfy $ab = p$, at least one of a and b must be a unit.

In view of Proposition 4.6.1, this can be rewritten as follows: p is irreducible if and only if p is nonzero and not a nonzero constant polynomial and has the property that whenever $a, b \in F[x]$ satisfy $ab = p$, at least one of a and b must be a nonzero constant polynomial.

We can declutter this statement (e.g., "nonzero and not a nonzero constant polynomial" can be shortened to "non-constant"), and thus obtain the following: p is irreducible if and only if p is non-constant and has the property that whenever $a, b \in F[x]$ satisfy $ab = p$, at least one of a and b must be constant. In other words, p is irreducible if and only if p is non-constant and cannot be written as a product of two non-constant polynomials. □

Now, we can characterize when a quotient ring of the form $F[x]/p$ is a field:

Theorem 4.6.3. Let F be a field. Let $p \in F[x]$ be nonzero. Then, the ring $F[x]/p$ is a field if and only if p is irreducible.

[144] *Proof.* Let u be a unit of $F[x]$. We must show that u is a nonzero constant polynomial.

We know that u is a unit of $F[x]$; hence, there exists some $v \in F[x]$ satisfying $uv = 1$. Consider this v. From $uv = 1 \neq 0$, we obtain $u \neq 0$, so that u is nonzero. Hence, $\deg(uv) = \deg u + \deg v$ (by Proposition 4.3.5 **(c)**, since F is an integral domain). Moreover, from $uv = 1$, we obtain $\deg(uv) = \deg 1 = 0$, so that $0 = \deg(uv) = \deg u + \underbrace{\deg v}_{\geq 0} \geq \deg u$, which entails that u is constant. Thus, u is a nonzero constant polynomial, qed.

[145] See Definition 2.15.1 for the definitions of prime and irreducible elements of an integral domain.

For example, the irreducible polynomial x^2+1 over the field $\mathbb{R}$ yields the field $\mathbb{R}[x] / \left(x^2+1\right)$ (which is $\cong \mathbb{C}$), but the non-irreducible polynomial x^2-1 over the field $\mathbb{R}$ yields the non-field $\mathbb{R}[x] / \left(x^2-1\right) \cong \mathbb{R} \times \mathbb{R}$.

Theorem 4.6.3 is analogous to the fact that $\mathbb{Z}/n$ is a field (for a positive integer n) if and only if n is prime. Just like the latter fact, it is a particular case of the following general property of PIDs:

Theorem 4.6.4. Let R be a PID. Let $p \in R$ be nonzero. Then, the ring R/p is a field if and only if p is irreducible.

Proof. $\Longrightarrow$: LTTR.

$\Longleftarrow$: Assume that p is irreducible. We must show that R/p is a field.

First of all, p is not a unit (since p is irreducible), so that 1 is not a multiple of p. Hence, $\overline{1} \neq \overline{0}$ in R/p. In other words, the ring R/p is not trivial. This ring is furthermore commutative (since R is commutative).

Now, let $\alpha \in R/p$ be a nonzero element. We shall prove that α is a unit.

Write α as $\overline{a}$ for some $a \in R$. Then, $\overline{a} = \alpha \neq 0$ in R/p (since α is nonzero), so that $p \nmid a$.

Now, recall that R is a PID, so that any ideal of R is principal. In particular, this entails that the ideal $aR + pR$ is principal. In other words, there exists some $g \in R$ such that $aR + pR = gR$. Consider this g. According to Proposition 2.14.13 **(a)**, we can conclude from $aR + pR = gR$ that g is a gcd of a and p. Thus, $g \mid a$ and $g \mid p$.

However, p is irreducible; hence, every divisor of p is either a unit or associate to p (indeed, this is easily seen to be a consequence of the definition of "irreducible"[146]). Thus, g is either a unit or associate to p (since $g \mid p$). However, g cannot be associate to p (because if g was associate to p, then we would have $p \mid g \mid a$, which would contradict $p \nmid a$). Hence, g must be a unit. Thus, it has an inverse g^{-1}.

But $g = g \cdot 1 \in gR = aR + pR$. In other words, there exist two elements $u, v \in R$ such that $g = au + pv$. Consider these u, v. Then, $g = au + pv = ua + pv$, so that

$$\overline{g} = \overline{ua + pv} = \overline{ua} \qquad (\text{since } pv \in pR)$$

in R/p. Therefore,

$$\overline{g^{-1}u} \cdot \overline{a} = \overline{g^{-1}} \cdot \overline{u} \cdot \overline{a} = \overline{g^{-1}} \cdot \underbrace{\overline{ua}}_{=\overline{g}} = \overline{g^{-1}} \cdot \overline{g} = \overline{g^{-1}g} = \overline{1}.$$

But this equality shows that $\overline{g^{-1}u}$ is an inverse of $\overline{a}$ in the ring R/p (because we know that R/p is commutative, so that we don't need to check $\overline{a} \cdot \overline{g^{-1}u} = \overline{1}$ as well). Thus, $\overline{a}$ is a unit. In other words, α is a unit (since $\alpha = \overline{a}$).

[146] Indeed: If d is a divisor of p, then there exists an $e \in R$ such that $p = de$. Consider this e. From $p = de$, we conclude that d or e is a unit (since p is irreducible). In the first case, d is a unit; in the second case, d is associate to p.

Forget that we fixed α. We thus have shown that any nonzero $\alpha \in R/p$ is a unit. In other words, R/p is a field (since R/p is a nontrivial commutative ring). $\square$

Theorem 4.6.3 is a particular case of Theorem 4.6.4 (since $F[x]$ is a PID when F is a field).

As a consequence of Theorem 4.6.3, we can now "adjoin" a root of an irreducible polynomial to a field without destroying its field-ness: Namely, if we have a field F and some irreducible polynomial $b \in F[x]$, then the quotient ring $F[x]/b$ will be a field that contains F as a subring and that contains a root of b. This generalizes Cardano's definition of $\mathbb{C}$, but can also be applied to adjoin roots to fields other than $\mathbb{R}$.

Example 4.6.5. The polynomial $x^2+1 \in (\mathbb{Z}/3)[x]$ is irreducible. (Indeed, $\mathbb{Z}/3$ being a finite field, we could verify this by going through all nonconstant polynomials of degree < 2 and checking that none of them divides x^2+1.)

Thus, Theorem 4.6.3 yields that $(\mathbb{Z}/3)[x] / \left(x^2+1\right)$ is a field. This field is a free $\mathbb{Z}/3$-module of rank 2 (by Theorem 4.5.9 **(b)**), and thus is isomorphic to $(\mathbb{Z}/3)^2 = (\mathbb{Z}/3) \times (\mathbb{Z}/3)$ as a $\mathbb{Z}/3$-module (but not as a ring, of course). Hence, the size of this field is $\left|(\mathbb{Z}/3)^2\right| = |\mathbb{Z}/3|^2 = 3^2 = 9$.

Thus, we have found a finite field of size 9. We have obtained it from $\mathbb{Z}/3$ in the same way as $\mathbb{C}$ was obtained from $\mathbb{R}$: by adjoining a square root of -1.

Incidentally, this field can also be constructed as $\mathbb{Z}[i]/3$.

5. Finite fields

5.1. Basics

Example 4.6.5 may make you wonder: what finite fields can we find? We know that for each prime p, the quotient ring $\mathbb{Z}/p$ is a field of size p; thus, we know a finite field of any prime size. Now we have found a finite field of size 9, too. What other finite fields exist?

Let's first grab the low-hanging fruit:

Proposition 5.1.1. Let p be a prime number. Then:

(a) There exists an irreducible polynomial $b \in (\mathbb{Z}/p)[x]$ of degree 2 over $\mathbb{Z}/p$.

(b) There exists a finite field of size p^2.

Example 5.1.2.

(a) Let $p = 2$. Then, Proposition 5.1.1 **(a)** yields that there exists an irreducible polynomial $b \in (\mathbb{Z}/2)[x]$ of degree 2 over $\mathbb{Z}/2$. It is easy to see that this polynomial b is actually unique; it is $b = x^2 + x + 1$. Furthermore, Proposition 5.1.1 **(b)** yields that there exists a finite field of size $p^2 = 2^2 = 4$. As we will see in the proof of the proposition, this latter field can be obtained as $F[x]/b$ for the afore-mentioned polynomial b. It has four elements $\overline{0}, \overline{1}, \overline{x}, \overline{x+1}$. It is easy to see that this field is actually isomorphic to the four-element ring F_4 constructed in Subsection 2.1.2. (One possible isomorphism sends its four elements $\overline{0}, \overline{1}, \overline{x}, \overline{x+1}$ to the four elements $0, 1, a, b$ of the latter.) This explains why the F_4 from Subsection 2.1.2 is a ring!

(b) Let us now take $p = 3$ instead. Then, Proposition 5.1.1 **(a)** yields that there exists an irreducible polynomial $b \in (\mathbb{Z}/3)[x]$ of degree 2 over $\mathbb{Z}/3$. Actually, there are three such polynomials:

$$b_1 = x^2 + 1; \qquad b_2 = x^2 + x + 2; \qquad b_3 = x^2 + 2x + 2.$$

We can use them to construct a finite field of size $p^2 = 3^2 = 9$. Actually, the three fields obtained turn out to be mutually isomorphic.

Proof of Proposition 5.1.1. We write F for $\mathbb{Z}/p$. Thus, F is a field and satisfies $|F| = |\mathbb{Z}/p| = p$.

(a) If $p = 2$, then we can take $b = x^2 + x + 1$; it is easy to check that this b is irreducible.

Thus, WLOG assume that $p \neq 2$. Hence, $p > 2$. Thus, $\overline{1} \neq \overline{-1}$ in $\mathbb{Z}/p$. In other words, $\overline{1} \neq \overline{-1}$ in F (since $\mathbb{Z}/p = F$). The map

$$F \to F,$$
$$a \mapsto a^2$$

is not injective (since $\overline{1}^2 = \overline{-1}^2$ but $\overline{1} \neq \overline{-1}$), and thus cannot be surjective (by the pigeonhole principle). Thus, there exists some $u \in F$ that is not in the image of this map. In other words, there exists some $u \in F$ that is not a square. Consider such a u. Then, the polynomial $x^2 - u$ has no roots in F.

Now it is not hard to prove that the polynomial $x^2 - u$ is irreducible.[147] This proves Proposition 5.1.1 **(a)** (since $x^2 - u \in (\mathbb{Z}/p)[x]$ is an irreducible polynomial of degree 2).

(b) Proposition 5.1.1 **(a)** yields that there exists an irreducible polynomial $b \in F[x]$ of degree 2 over F (since $\mathbb{Z}/p = F$). Consider this b. Theorem 4.6.3 (applied to b instead of p) then yields that the ring $F[x]/b$ is a field. Moreover, $F[x]/b$ is a free F-module of rank 2 (by Theorem 4.5.9 **(b)**), and thus is isomorphic to F^2 as a F-module, and therefore has size $\left|F^2\right| = |F|^2 = p^2$ (since $|F| = p$). Hence, $F[x]/b$ is a finite field of size p^2. This proves Proposition 5.1.1 **(b)**. □

By more complicated but somewhat similar arguments[148], we can also see that there exists a finite field of size p^3 for any prime p. This suggests general-

[147] *Proof.* Assume that we have written $x^2 - u$ as a product fg of two non-constant polynomials $f, g \in F[x]$. We shall derive a contradiction.

Indeed, we have assumed that $x^2 - u = fg$; hence, $\deg\left(x^2 - u\right) = \deg(fg) = \deg f + \deg g$ (since F is an integral domain). Thus, $\deg f + \deg g = \deg\left(x^2 - u\right) = 2$. Since $\deg f$ and $\deg g$ are positive integers (because f and g are non-constant), this entails that $\deg f$ and $\deg g$ must equal 1 (since the only pair of positive integers that add up to 2 is $(1,1)$). Thus, in particular, $\deg f = 1$. Hence, $f = ax + b$ for some $a, b \in F$ with $a \neq 0$. Consider these a, b. From $f = ax + b$, we obtain $f\left[\dfrac{-b}{a}\right] = a \cdot \dfrac{-b}{a} + b = 0$. Thus, the polynomial f has a root in F (namely, $\dfrac{-b}{a}$). Hence, the polynomial $x^2 - u$ has a root in F as well (indeed, $f \mid fg = x^2 - u$, so that every root of f is also a root of $x^2 - u$). This contradicts the fact that the polynomial $x^2 - u$ has no roots in F.

Thus, we have found a contradiction stemming from our assumption that $x^2 - u$ is a product fg of two non-constant polynomials $f, g \in F[x]$. Hence, $x^2 - u$ cannot be written as such a product. In other words, $x^2 - u$ is irreducible (since $x^2 - u$ is a non-constant polynomial). Qed.

[148] Not too similar! It is not true that the map

$$F \to F,$$
$$a \mapsto a^3$$

is always non-surjective when $F = \mathbb{Z}/p$ for $p > 3$. Instead, you have to argue the existence of an irreducible polynomial $b \in (\mathbb{Z}/p)[x]$ of degree 3 over $\mathbb{Z}/p$ by a counting argument: Show that the total number of monic degree-3 polynomials in $(\mathbb{Z}/p)[x]$ is p^3, whereas the

izing to p^m; but this is much harder. Indeed, a nonconstant polynomial over F of degree ≤ 3 will always be irreducible if it has no roots in F (check this![149]); however, for polynomials of degree ≥ 4, this is no longer the case (fun exercise: prove that the polynomial $x^4 + 4 \in \mathbb{Q}[x]$ is not irreducible, despite of course not having any roots over $\mathbb{Q}$). Thus, our trick for finding irreducible polynomials will no longer work for degrees > 3. We can still find a field of size p^4 by applying our trick twice (first get a finite field of size p^2, then proceed to find an irreducible polynomial of degree 2 over that field), and by induction we can find fields of sizes $p^8, p^{16}, p^{32}, \ldots$. But we don't get a field of size p^5 this way.

So do such fields exist?

5.2. The characteristic of a field

Leaving prime powers aside for a moment, what about fields of size 6 ? It turns out that such fields don't exist, for a fairly simple reason. Fields have an important invariant, the so-called **characteristic**:

Definition 5.2.1. Let F be a field. The **characteristic** of F is an integer called $\operatorname{char} F$, which is defined as follows:

- If there exists a positive integer n such that $n \cdot 1_F = 0_F$, then $\operatorname{char} F$ is defined to be the **smallest** such n.
- If such an n does not exist, then $\operatorname{char} F$ is defined to be 0.

Roughly speaking, $\operatorname{char} F$ is "how often you have to add 1_F to itself to obtain 0_F" (with the caveat that we define it to be 0 if you never obtain 0_F by adding 1_F to itself). Here are some examples:

- We have $\operatorname{char} \mathbb{Q} = 0$, since there exists no positive integer n such that $n \cdot 1_{\mathbb{Q}} = 0_{\mathbb{Q}}$. For the same reason, $\operatorname{char} \mathbb{R} = 0$ and $\operatorname{char} \mathbb{C} = 0$.
- For any prime p, we have $\operatorname{char}(\mathbb{Z}/p) = p$. Indeed, $p \cdot 1_{\mathbb{Z}/p} = p \cdot \overline{1} = \overline{p \cdot 1} = \overline{p} = \overline{0}$ in $\mathbb{Z}/p$, but every positive integer $n < p$ satisfies $n \cdot 1_{\mathbb{Z}/p} = n \cdot \overline{1} = \overline{n \cdot 1} = \overline{n} \neq \overline{0}$ in $\mathbb{Z}/p$.
- For our fields F of size p^2 or p^3, we also have $\operatorname{char} F = p$, since they contain $\mathbb{Z}/p$ as subrings.

Let us now see what the characteristic of a field satisfies in general, and what it can tell us about the field.

total number of monic degree-3 polynomials in $(\mathbb{Z}/p)[x]$ that can be written as a product of a degree-1 and a degree-2 polynomial is smaller than p^3; thus, at least one monic degree-3 polynomial cannot be written as such a product.

[149] See Exercise 5.2.1 **(a)**.

Theorem 5.2.2 (Properties of characteristics)**.** Let F be a field. Let $p = \operatorname{char} F$. Then:

(a) The field F is a $\mathbb{Z}/p$-algebra. (Remember: $\mathbb{Z}/0 \cong \mathbb{Z}$.)

(b) We have $pa = 0$ for each $a \in F$.

(c) The number p is either prime or 0.

(d) If F is finite, then p is a prime.

(e) If F is finite, then $|F| = p^m$ for some positive integer m.

(f) If p is a prime, then F contains "a copy of $\mathbb{Z}/p$" (meaning: a subring isomorphic to $\mathbb{Z}/p$).

(g) If $p = 0$, then F contains "a copy of $\mathbb{Q}$" (meaning: a subring isomorphic to $\mathbb{Q}$): namely, the map

$$\begin{aligned} &\mathbb{Q} \to F, \\ &\frac{a}{b} \mapsto \frac{a \cdot 1_F}{b \cdot 1_F} \qquad (\text{for } a, b \in \mathbb{Z} \text{ with } b \neq 0) \end{aligned}$$

is an injective ring morphism.

Proof. We have $p \cdot 1_F = 0_F$. Indeed, if $p = 0$, then this is obvious; but otherwise it follows from the definition of $\operatorname{char} F$.

(b) Let $a \in F$. Then, $a = 1_F \cdot a$. Thus,

$$pa = p\left(1_F \cdot a\right) = \underbrace{\left(p \cdot 1_F\right)}_{=0_F} \cdot a = 0_F \cdot a = 0_F = 0.$$

This proves Theorem 5.2.2 **(b)**.

(a) We define an action of the ring $\mathbb{Z}/p$ on F by

$$\overline{k} \cdot a = ka \qquad \text{for all } k \in \mathbb{Z} \text{ and } a \in F.$$

Why is this well-defined? In other words, why is it true that if two integers k and ℓ satisfy $\overline{k} = \overline{\ell}$, then $ka = \ell a$ for all $a \in F$?

Let us check this directly: Let k and ℓ be two integers satisfying $\overline{k} = \overline{\ell}$ in $\mathbb{Z}/p$. This means $k \equiv \ell \bmod p$, so that $k - \ell$ is a multiple of p. That is, $k - \ell = pu$ for some $u \in \mathbb{Z}$. Consider this u. Now,

$$ka - \ell a = \underbrace{\left(k - \ell\right)}_{=pu} a = pua = 0$$

(by Theorem 5.2.2 **(b)**, applied to ua instead of a). Thus, $ka = \ell a$, which is precisely what we wanted to prove.

Thus, the action of $\mathbb{Z}/p$ on F is well-defined. Now, it remains to show that F is a $\mathbb{Z}/p$-module, and that the "scale-invariance" axiom is satisfied. All of this is easy and LTTR[150]. Thus, F becomes a $\mathbb{Z}/p$-algebra. This proves Theorem 5.2.2 **(a)**.

(c) Assume the contrary. Thus, p is neither a prime nor 0. Hence, p is either 1 or a composite[151] positive integer (since p is always a nonnegative integer).

Since F is a field, we have $1 \neq 0$ in F. In other words, $1_F \neq 0_F$. If we had $p = 1$, then we would thus have $\underbrace{p}_{=1} \cdot 1_F = 1 \cdot 1_F = 1_F \neq 0_F$, which would contradict $p \cdot 1_F = 0_F$. Thus, we cannot have $p = 1$. Hence, p must be composite (since p is either 1 or composite). In other words, $p = uv$ for some integers $u > 1$ and $v > 1$. Consider these integers u and v.

From $u > 1$ and $v > 1$ and $p = uv$, we see that both integers u and v are smaller than p. Hence, neither $u \cdot 1_F$ nor $v \cdot 1_F$ can be 0_F (since $p = \operatorname{char} F$ was defined to be the **smallest** positive integer n such that $n \cdot 1_F = 0_F$). Since F is an integral domain (because F is a field), this yields that the product $(u \cdot 1_F) \cdot (v \cdot 1_F)$ is also nonzero.

Now, $p \cdot 1_F = 0_F$, so

$$0_F = \underbrace{p}_{=uv} \cdot 1_F = uv \cdot 1_F = (u \cdot 1_F) \cdot (v \cdot 1_F).$$

This contradicts the fact that the product $(u \cdot 1_F) \cdot (v \cdot 1_F)$ is nonzero. This proves Theorem 5.2.2 **(c)**.

(d) Assume that F is finite. We must show that p is a prime.

According to Theorem 5.2.2 **(c)**, it suffices to show that $p \neq 0$. So let us show this. Assume the contrary. Then, $p = 0$. Hence, none of the elements $1 \cdot 1_F$, $2 \cdot 1_F$, $3 \cdot 1_F$, ... of F is 0_F (by the definition of $\operatorname{char} F$). But F is finite, so two of these elements must be equal (by the Pigeonhole Principle). In other words, there exist positive integers $u < v$ such that $u \cdot 1_F = v \cdot 1_F$. Consider these u and

[150] For example, let us prove the associativity law, which says that $(rs)\, m = r\,(sm)$ for all $r, s \in \mathbb{Z}/p$ and $m \in F$. Indeed, let $r, s \in \mathbb{Z}/p$ and $m \in F$. Write r and s as $\overline{k}$ and $\overline{\ell}$ for some integers k and ℓ. Then, $rs = \overline{k} \cdot \overline{\ell} = \overline{k\ell}$, so that $(rs)\, m = \overline{k\ell} \cdot m = k\ell m$ (by our definition of the action of $\mathbb{Z}/p$ on F). Also, from $r = \overline{k}$ and $s = \overline{\ell}$, we obtain

$$\begin{aligned} r\,(sm) &= \overline{k} \cdot \left(\overline{\ell} \cdot m\right) = k\left(\overline{\ell} \cdot m\right) && \text{(by our definition of the action)} \\ &= k\,(\ell m) && \left(\text{since our definition of the action yields } \overline{\ell} \cdot m = \ell m\right) \\ &= k\ell m. \end{aligned}$$

Comparing this with $(rs)\, m = k\ell m$, we obtain $(rs)\, m = r\,(sm)$, qed.

[151] A positive integer is said to be **composite** if it can be written as a product of two integers each larger than 1.

v. Then, $v-u$ is a positive integer, and we have $(v-u)\cdot 1_F = v\cdot 1_F - u\cdot 1_F = 0_F$ (since $u\cdot 1_F = v\cdot 1_F$). But $(v-u)\cdot 1_F$ is one of the elements $1\cdot 1_F$, $2\cdot 1_F$, $3\cdot 1_F$, ... (since $u < v$), and we just said that none of these elements is 0_F. This contradicts $(v-u)\cdot 1_F = 0_F$. Thus, our assumption was false; hence, Theorem 5.2.2 **(d)** is proven.

(e) *First proof of part **(e)**:* Assume that F is finite. Thus, by Theorem 5.2.2 **(d)**, we know that p is prime.

Since F is a field, we have $1 \neq 0$ in F. Hence, $|F| > 1$.

From Theorem 5.2.2 **(a)**, we know that F is a $\mathbb{Z}/p$-algebra. Thus, in particular, F is a $\mathbb{Z}/p$-module. But since p is prime, $\mathbb{Z}/p$ is a field.

Now, recall that a module over a field is nothing but a vector space. In particular, every module over a field is free (since any vector space has a basis[152]). Thus, in particular, the $\mathbb{Z}/p$-module F is free. In other words, the $\mathbb{Z}/p$-module F has a basis. This basis must be finite (since F itself is finite). Thus, $F \cong (\mathbb{Z}/p)^m$ as $\mathbb{Z}/p$-modules for some $m \in \mathbb{N}$. Consider this m. From $F \cong (\mathbb{Z}/p)^m$, we obtain $|F| = \left|(\mathbb{Z}/p)^m\right| = |\mathbb{Z}/p|^m = p^m$. It remains to prove that m is positive. But this is easy: If m was 0, then $|F| = p^m$ would imply $|F| = p^0 = 1$, which would contradict $|F| > 1$. Thus, the proof of Theorem 5.2.2 **(e)** is complete.

*Second proof of part **(e)**:* There is an alternative proof of Theorem 5.2.2 **(e)**, which avoids any use of linear algebra but instead uses some group theory. Specifically, we will use **Cauchy's theorem**, which says the following: If G is a finite group, and if q is a prime number that divides the size $|G|$, then G has an element of order q. Proofs of this theorem can be found, e.g., in `https://kconrad.math.uconn.edu/blurbs/grouptheory/cauchypf.pdf` or in [Sharif22, Theorem 4.9.4] or [Knapp16, Remark after Theorem 4.59] or [Elman22, Theorem 21.22] or [Ford22, Corollary 2.4.14], just to mention some freely available sources. (It is also an easy consequence of the first Sylow theorem.)

Now, assume that F is finite. Thus, by Theorem 5.2.2 **(d)**, we know that p is prime.

Since F is a field, we have $1 \neq 0$ in F. Hence, $|F| > 1$.

Assume (for the sake of contradiction) that the integer $|F|$ has a prime divisor q distinct from p. Thus, Cauchy's theorem (applied to G being the additive group $(F,+,0)$) yields that the additive group $(F,+,0)$ has an element of order q. Let a be this element. Then, $a \neq 0$ but $qa = 0$ (since a has order q). However,

[152] This fact is Theorem 3.7.6.

Once again, I haven't actually proved this fact in this course, but you can easily bridge this gap yourself or look it up in any text on linear algebra (or in Keith Conrad's `https://kconrad.math.uconn.edu/blurbs/linmultialg/dimension.pdf`). Our situation is simpler than the general case, since we know that F is finite, so it is clear that there is a finite list of vectors in F that span F (because you can just take a list of **all** elements of F). In order to obtain a basis from such a list, you only need to successively remove vectors that are linear combinations of other vectors; once no such vectors remain, the list will be a basis (make sure you understand why!).

Theorem 5.2.2 **(b)** yields $pa = 0$.

However, p and q are two distinct primes, and thus are coprime. Thus, $\gcd(p,q) = 1$. But Bezout's theorem shows that there exist two integers x and y such that $xp + yq = \gcd(p,q)$. Consider these x and y. Then,

$$\underbrace{(xp+yq)}_{=\gcd(p,q)=1} a = 1a = a \neq 0$$

contradicts

$$(xp+yq)\,a = x\underbrace{pa}_{=0} + y\underbrace{qa}_{=0} = x0 + y0 = 0.$$

This contradiction shows that our assumption (that the integer $|F|$ has a prime divisor q distinct from p) is false.

Hence, the integer $|F|$ has no prime divisor distinct from p. Thus, the only prime divisor of $|F|$ is p. Therefore, $|F| = p^m$ for some $m \in \mathbb{N}$. This m must furthermore be positive (since $|F| > 1$). Thus, Theorem 5.2.2 **(e)** is proven again.

(f) Assume that p is a prime. Then, F is a $\mathbb{Z}/p$-algebra (by Theorem 5.2.2 **(a)**), so we can define a map

$$\begin{aligned} \mathbb{Z}/p &\to F, \\ \alpha &\mapsto \alpha \cdot 1_F. \end{aligned}$$

It is straightforward to check that this map is a ring morphism[153]; furthermore, it is easily seen to be injective[154]. Hence, its image is a subring of F that is isomorphic to $\mathbb{Z}/p$ (by Proposition 2.7.11 **(a)**). This proves Theorem 5.2.2 **(f)**.

[153]For instance, it respects multiplication because $(\alpha \cdot 1_F)(\beta \cdot 1_F) = \alpha\beta \cdot \underbrace{1_F 1_F}_{=1_F} = \alpha\beta \cdot 1_F$ for any $\alpha, \beta \in \mathbb{Z}/p$.

[154]This is actually best understood as a particular case of the following general fact: **Any** ring morphism from a field to a nontrivial ring is injective!

The proof of this general fact is pretty easy: Let $f : K \to R$ be a ring morphism from a field K to a nontrivial ring R. We must show that f is injective.

Assume that a is a nonzero element of $\operatorname{Ker} f$. Then, a is a unit of K (since K is a field, and thus any nonzero element of K is a unit), and thus a^{-1} exists. Since f is a ring morphism, we have

$$f\left(aa^{-1}\right) = \underbrace{f(a)}_{\substack{=0 \\ (\text{since } a \in \operatorname{Ker} f)}} \cdot f\left(a^{-1}\right) = 0,$$

so that $0 = f\left(\underbrace{aa^{-1}}_{=1}\right) = f(1) = 1$ (since f is a ring morphism). This entails that the ring R is trivial, which contradicts our assumption that R is nontrivial.

Forget that we fixed a. We thus obtained a contradiction for any nonzero element a of $\operatorname{Ker} f$. Hence, no such element exists. In other words, any $a \in \operatorname{Ker} f$ must be 0. Thus, $\operatorname{Ker} f \subseteq \{0\}$, so that $\operatorname{Ker} f = \{0\}$, and therefore f is injective (by Lemma 2.9.7). This completes our proof.

(g) We will be very brief, since we won't use Theorem 5.2.2 **(g)** in what follows.

Assume that $p = 0$. Then, for any nonzero integer b, the element $b \cdot 1_F$ of F is nonzero (why?) and therefore a unit of F (since F is a field). Hence, for any rational number $\frac{a}{b} \in \mathbb{Q}$ (written in such a way that $a, b \in \mathbb{Z}$ and $b \neq 0$), the element $\frac{a \cdot 1_F}{b \cdot 1_F} \in F$ is well-defined. Now, of course, the representation of a rational number as $\frac{a}{b}$ with $a, b \in \mathbb{Z}$ is not unique (for instance, $\frac{6}{4}$ and $\frac{3}{2}$ are the same rational number); however, it is not hard to show that $\frac{a \cdot 1_F}{b \cdot 1_F}$ is uniquely determined by $\frac{a}{b}$ (meaning that if $a, b, c, d \in \mathbb{Z}$ satisfy $\frac{a}{b} = \frac{c}{d}$, then we also have $\frac{a \cdot 1_F}{b \cdot 1_F} = \frac{c \cdot 1_F}{d \cdot 1_F}$). Thus, the map

$$\begin{aligned} &\mathbb{Q} \to F, \\ &\frac{a}{b} \mapsto \frac{a \cdot 1_F}{b \cdot 1_F} \qquad (\text{for } a, b \in \mathbb{Z} \text{ with } b \neq 0) \end{aligned}$$

is well-defined. Next, it can be shown that this map is a ring morphism and is injective[155]. Hence, its image is a subring of F that is isomorphic to $\mathbb{Q}$. This proves Theorem 5.2.2 **(g)**. □

Parts **(f)** and **(g)** of Theorem 5.2.2 show that any field F has at its "core" a "small" field: either (a copy of) $\mathbb{Z}/p$ (if its characteristic is a prime p) or (a copy of) $\mathbb{Q}$ (if its characteristic is 0).

Parts **(d)** and **(e)** of Theorem 5.2.2 (in combination) show that the size of any finite field is a power of a prime. Thus, there are no finite fields of size 6 or 10 or 12.

Hence, we can limit our search for finite fields to those of size p^m for p prime and $m > 0$. We have already found such fields for $m = 1$ and for $m = 2$ (for all p), and briefly hinted at the cases $m = 3$ and $m = 4$, but we are still missing the case of general m.

Exercise 5.2.1.

(a) Let F be any field, and let $p \in F[x]$ be a polynomial of degree 2 or 3. Prove that p is irreducible if and only if p has no root in F.

(b) Let $r \in \mathbb{Q}$ be a rational number that is not the cube of any rational number. Prove that the polynomial $x^3 - r \in \mathbb{Q}[x]$ is irreducible.

[155] The injectivity follows just as in part **(f)**.

(c) Prove that there is an injective ring morphism

$$\mathbb{Q}[x] / \left(x^3 - 5\right) \to \mathbb{R},$$
$$\overline{p} \mapsto p\left(\sqrt[3]{5}\right).$$

(d) In Subsection 2.1.2, we claimed that there are no $a, b \in \mathbb{Q}$ that satisfy $1 + 2\sqrt[3]{5} + \left(\sqrt[3]{5}\right)^2 = a + b\sqrt[3]{5}$. Prove this claim.

5.3. Tools

5.3.1. Splitting polynomials

We are still trying to find finite fields of sizes p^m for p prime and $m > 0$. We will approach the general case indirectly (no easy and direct proofs are known). We will need a bunch of tools. The first is the notion of a **splitting field**. We begin with a definition:

Definition 5.3.1. Let R be a commutative ring. Let $b \in R[x]$ be a polynomial over R. We say that b **splits** over R if there exist elements $r_1, r_2, \ldots, r_m$ of R such that

$$b = (x - r_1)(x - r_2) \cdots (x - r_m).$$

Note that in this definition, we must necessarily have $\deg b = m$ (unless R is trivial). Also, a polynomial cannot split unless it is monic. This might differ from how other authors define the notion of "splitting", but it is sufficient for what we will do with it.

Example 5.3.2.

(a) The polynomial $x^2 - 1$ splits over $\mathbb{Q}$, since

$$x^2 - 1 = (x - 1)(x + 1) = (x - 1)(x - (-1)).$$

(b) The polynomial $x^2 + 1$ does not split over $\mathbb{R}$ (since it has no roots in $\mathbb{R}$), but it splits over $\mathbb{C}$, since

$$x^2 + 1 = (x - i)(x + i) = (x - i)(x - (-i)).$$

(c) The polynomial x^2 splits over $\mathbb{Q}$, since $x^2 = xx = (x - 0)(x - 0)$.

(d) The polynomial $x^4 - 9$ does not split over $\mathbb{R}$. Indeed, it has a factorization

$$x^4 - 9 = \left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right)\left(x^2 + 3\right),$$

but the x^2+3 factor is still not of the form $x-r$ and cannot be factored further over $\mathbb{R}$. However, this polynomial does split over $\mathbb{C}$, since

$$x^4-9=\left(x-\sqrt{3}\right)\left(x+\sqrt{3}\right)\left(x-\sqrt{3}i\right)\left(x+\sqrt{3}i\right).$$

(e) Any monic polynomial of degree 1 automatically splits over whatever commutative ring it is defined over. So does the constant polynomial 1 (since it is an empty product).

When a polynomial splits over a field, its roots can be read off directly from the splitting:

Proposition 5.3.3. Let F be a field. Let $r_1, r_2, \ldots, r_m \in F$. Then,

$$\begin{aligned}&\{\text{the roots of the polynomial } (x-r_1)(x-r_2)\cdots(x-r_m)\in F[x] \text{ in } F\}\\&=\{r_1,r_2,\ldots,r_m\}.\end{aligned}$$

Proof. The ring F is a field, thus an integral domain. Thus, a product uv of two elements $u, v \in F$ is zero if and only if one of its factors is zero. Hence, a finite product $u_1u_2\cdots u_k$ of elements of F is zero if and only if one of its factors is zero[156].

Now, we have

$$\begin{aligned}&\{\text{the roots of the polynomial } (x-r_1)(x-r_2)\cdots(x-r_m)\in F[x] \text{ in } F\}\\&=\{a\in F \mid ((x-r_1)(x-r_2)\cdots(x-r_m))[a]=0\}\\&\qquad\qquad\text{(by the definition of a ``root'')}\\&=\{a\in F \mid (a-r_1)(a-r_2)\cdots(a-r_m)=0\}\\&\qquad\qquad\left(\begin{array}{c}\text{since the evaluation } ((x-r_1)(x-r_2)\cdots(x-r_m))[a]\\ \text{equals } (a-r_1)(a-r_2)\cdots(a-r_m)\end{array}\right)\\&=\{a\in F \mid \text{one of } a-r_1, a-r_2, \ldots, a-r_m \text{ is zero}\}\\&\qquad\qquad\left(\begin{array}{c}\text{since a finite product } u_1u_2\cdots u_k \text{ of elements of } F \text{ is zero}\\ \text{if and only if one of its factors is zero}\end{array}\right)\\&=\{a\in F \mid a=r_1 \text{ or } a=r_2 \text{ or } \cdots \text{ or } a=r_m\}\\&=\{r_1,r_2,\ldots,r_m\}.\end{aligned}$$

This proves Proposition 5.3.3. □

[156] Indeed, this follows easily by induction on k, using the preceding sentence in the induction step.

Remark 5.3.4. It is worth noting that Proposition 5.3.3 still holds if we replace "field" by "integral domain" (and the same proof applies); but it does not hold when F is just a general commutative ring. For example, if $F = \mathbb{Z}/4$, then the polynomial $(x-0)(x-0)(x-1)(x-3) \in F[x]$ has roots $0, 1, 2, 3$, rather than just $0, 1, 3$ as Proposition 5.3.3 would predict. A similar construction works for $\mathbb{Z}/n$ where n is any composite integer > 1 (see Exercise 5.3.1).

Exercise 5.3.1. Let $n > 1$ be a composite integer (i.e., an integer that is not prime). Prove the following:

(a) Each element of $\mathbb{Z}/n$ is a root of the polynomial $\prod_{i=1}^{n-1} \left(x - \overline{i}\right)^2 \in (\mathbb{Z}/n)[x]$.

(b) If $n > 4$, then each element of $\mathbb{Z}/n$ is a root of the polynomial $\prod_{i=1}^{n-1} \left(x - \overline{i}\right) \in (\mathbb{Z}/n)[x]$.

5.3.2. Splitting fields

The Fundamental Theorem of Algebra says that each monic univariate polynomial over $\mathbb{C}$ splits over $\mathbb{C}$. This is not actually a theorem of algebra, since it relies on the definition of $\mathbb{C}$ (which is analytic); however, it explains some of the significance of $\mathbb{C}$. In general, a field F is said to be **algebraically closed** if each monic univariate polynomial over F splits over F. The field $\mathbb{C}$ is not the only algebraically closed field, but it is perhaps the best-known.

We won't need algebraically closed fields in this course; we will need a more "local" notion: that of a splitting field. To introduce it, we make a simple observation, which we have already (tacitly) used in Example 5.3.2 (as we have been treating the same polynomial $x^2 + 1$ first as a polynomial in $\mathbb{R}[x]$ and then as a polynomial in $\mathbb{C}[x]$):

Proposition 5.3.5. Let S be a commutative ring. Let R be a subring of S. Then, any polynomial over R automatically is a polynomial over S as well (since its coefficients lie in R and therefore also lie in S), and thus the polynomial ring $R[x]$ becomes a subring of $S[x]$.

For example, $\mathbb{R}[x]$ is a subring of $\mathbb{C}[x]$. Polynomials like $x^2 + 1$ might not split over $\mathbb{R}$, but they split over $\mathbb{C}$. This suggests that if a monic polynomial does not split over a ring, we might fix this by making the ring larger ("extending" the ring, possibly by "adjoining" some roots), just as $\mathbb{C}$ was constructed from $\mathbb{R}$ in order to make $x^2 + 1$ split. Thus we make the following definition:

Definition 5.3.6. Let F be a field. Let $b \in F[x]$ be a monic polynomial over F. Then, a **splitting field** of b (over F) means a field S such that

- F is a subring of S;
- the polynomial b (regarded as a polynomial in $S[x]$) splits over S.

Examples:

- $\mathbb{C}$ is a splitting field of x^2+1 over $\mathbb{R}$.
- $\mathbb{C}$ is a splitting field of x^2-2 over $\mathbb{Q}$, but so is $\mathbb{R}$ (since x^2-2 already splits over $\mathbb{R}$) or even the smaller field $\mathbb{Q}\left[\sqrt{2}\right] = \left\{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\right\}$.
- $\mathbb{Q}$ itself is a splitting field of x^2-1 over $\mathbb{Q}$.

(Be careful with the literature: Many authors have a more restrictive concept of a "splitting field", which requires not only that the polynomial split over it, but also that the field – in some reasonable way – is minimal with this property. For example, these authors do not accept $\mathbb{R}$ as a splitting field of x^2-2 over $\mathbb{Q}$, since the much smaller field $\mathbb{Q}\left[\sqrt{2}\right]$ suffices to split the polynomial. But our definition suffices for our purposes.)

The most important fact about splitting fields is that they always exist:

Theorem 5.3.7. Let F be a field. Let $b \in F[x]$ be a monic polynomial over F. Then:

(a) We can write b as a product $b = c_1 c_2 \cdots c_k$ of monic irreducible polynomials $c_1, c_2, \ldots, c_k \in F[x]$.

(b) If $\deg b > 0$, then there is a field that contains F as a subring and that contains a root of b.

(c) There exists a splitting field of b over F.

Proof. **(a)** Any nonzero polynomial in $F[x]$ can be made monic by scaling it with a nonzero scalar (namely, if $g \in F[x]$ is a nonzero polynomial, and if c is its leading coefficient, then $c^{-1}g$ is a monic polynomial). This scaling does not interfere with its divisibility properties; thus, if g is irreducible, then it remains so after the scaling.

Hence, it suffices to show that we can write b as a product $b = c_1 c_2 \cdots c_k$ of irreducible polynomials $c_1, c_2, \ldots, c_k \in F[x]$.

Abstractly, this follows easily from the fact that $F[x]$ is a UFD. In a more down-to-earth manner, this can be shown just like the classical fact that each

positive integer can be written as a product of primes. The proof proceeds by strong induction on $\deg b$; the main idea is "either b is itself irreducible, in which case we are done; or b can be written as a product of two polynomials of smaller degree, in which case the induction hypothesis applies".

(Note that this proof is constructive when F is finite, since we can actually try out all polynomials of degree smaller than $\deg b$ and check which of them divide b.)

Theorem 5.3.7 **(a)** is thus proved.

(b) Assume that $\deg b > 0$. We must find a field that contains F as a subring and that contains a root of b.

It is tempting to take $F[x]/b$, but this might fail to be a field (since b might fail to be irreducible).

Instead, we use Theorem 5.3.7 **(a)** to write b as a product $b = c_1 c_2 \cdots c_k$ of monic irreducible polynomials $c_1, c_2, \ldots, c_k \in F[x]$, and then we take the field $F[x]/c_1$ (which is indeed a field, because c_1 is irreducible[157]). This field will contain a root of c_1, and thus also contain a root of b (since a root of c_1 is always a root of b). So Theorem 5.3.7 **(b)** is proved.

(Where did I use the assumption $\deg b > 0$ in this proof? Hint: Why is there a c_1 ?)

(c) Here is a proof by example: Assume that $\deg b = 3$.

Theorem 5.3.7 **(b)** says that there is a field F' that contains F as a subring and that contains a root of b. Consider this F', and let r_1 be the root of b that it contains. Thus, $x - r_1 \mid b$ in $F'[x]$ (since r_1 is a root of b). Hence, the polynomial $\dfrac{b}{x - r_1} \in F'[x]$ is well-defined. Moreover, this polynomial $\dfrac{b}{x - r_1}$ has degree $3 - 1 = 2$ and is monic[158].

Now, we apply Theorem 5.3.7 **(b)** again, but this time to the field F' and the monic polynomial $\dfrac{b}{x - r_1}$ over it. Thus we conclude that there is a field F'' that contains F' as a subring and that contains a root of $\dfrac{b}{x - r_1}$. Consider this F'', and let r_2 be the root of $\dfrac{b}{x - r_1}$ that it contains. Thus, $x - r_2 \mid \dfrac{b}{x - r_1}$ in $F''[x]$ (since r_2 is a root of $\dfrac{b}{x - r_1}$). Hence, the polynomial $\dfrac{b}{x - r_1} / (x - r_2) \in F''[x]$ is well-defined. In other words, the polynomial $\dfrac{b}{(x - r_1)(x - r_2)} \in F''[x]$ is well-defined. Moreover, this polynomial $\dfrac{b}{(x - r_1)(x - r_2)}$ has degree $3 - 2 = 1$ and is monic.

[157] We are using Theorem 4.6.3 here.

[158] Here, we are using the fact that when we divide a monic polynomial f by a monic polynomial g with $\deg g \leq \deg f$, the quotient will again be monic. (The proof is LTTR. Note that this holds even if there is a remainder!)

Now, we apply Theorem 5.3.7 **(b)** again, but this time to the field F'' and the monic polynomial $\dfrac{b}{(x-r_1)(x-r_2)}$ over it. Thus we conclude that there is a field F''' that contains F'' as a subring and that contains a root of $\dfrac{b}{(x-r_1)(x-r_2)}$. Consider this F''', and let r_3 be the root of $\dfrac{b}{(x-r_1)(x-r_2)}$ that it contains. Thus, $x-r_3 \mid \dfrac{b}{(x-r_1)(x-r_2)}$ in $F'''[x]$. Hence, the polynomial $\dfrac{b}{(x-r_1)(x-r_2)(x-r_3)} \in F'''[x]$ is well-defined. Furthermore, this polynomial has degree $3-3=0$ and is monic. In other words, this polynomial equals 1. In other words, $b = (x-r_1)(x-r_2)(x-r_3)$ in $F'''[x]$. This shows that b splits over F'''. Moreover, by construction, F''' is a field that contains F as a subring (since $F \subseteq F' \subseteq F'' \subseteq F'''$, and each of these "$\subseteq$" signs is not just a subset but actually a subring).

Thus, we have proved Theorem 5.3.7 **(c)** in our example. Proving it in the general case is just a matter of formalizing what we did as an induction on $\deg b$. □

5.3.3. The Idiot's Binomial Formula and the Frobenius endomorphism

Next, to something different. A rather surprising property of fields of positive characteristic is the following theorem (often called **Freshman's Dream** or **Idiot's Binomial Formula** due to its similarity to a popular student mistake):

Theorem 5.3.8 (Idiot's Binomial Formula, aka Freshman's Dream)**.** Let p be a prime number. Let F be a field of characteristic p, or, more generally, any commutative $\mathbb{Z}/p$-algebra. Then:

(a) We have $(a+b)^p = a^p + b^p$ for any $a, b \in F$.

(b) We have $(a+b)^{p^m} = a^{p^m} + b^{p^m}$ for any $a, b \in F$ and $m \in \mathbb{N}$.

(c) We have $(a-b)^p = a^p - b^p$ for any $a, b \in F$.

(d) We have $(a-b)^{p^m} = a^{p^m} - b^{p^m}$ for any $a, b \in F$ and $m \in \mathbb{N}$.

For example, for $p=3$, Theorem 5.3.8 **(a)** says that $(a+b)^3 = a^3 + b^3$. And indeed, we can show this directly: Theorem 5.2.2 **(b)** shows that $3u = 0$ for any $u \in F$ (for $p=3$), and the binomial formula yields

$$(a+b)^3 = a^3 + \underbrace{3a^2b}_{\substack{=0 \\ \text{(since } 3u=0 \\ \text{for any } u \in F\text{)}}} + \underbrace{3ab^2}_{\substack{=0 \\ \text{(since } 3u=0 \\ \text{for any } u \in F\text{)}}} + b^3 = a^3 + b^3.$$

We note that Theorem 5.3.8 says nothing about powers other than p-th or p^m-th powers. So it is not a replacement for the binomial formula!

To prove Theorem 5.3.8 **(a)** in general, we will argue in the same way as in the $p = 3$ example we just showed; we will just need to know that all but the leftmost and rightmost addends in the binomial formula vanish. This is a consequence of the following property of binomial coefficients:

Lemma 5.3.9. Let p be a prime number. Let $k \in \{1, 2, \ldots, p-1\}$. Then, $p \mid \dbinom{p}{k}$.

Note that this does indeed depend on p being a prime. For example, the number 4 is not prime, and we **do not** have $4 \mid \dbinom{4}{2}$ (since $\dbinom{4}{2} = 6$).

Proof of Lemma 5.3.9. There is an easy-to-prove formula (see, e.g., [Grinbe15, Proposition 3.22]) saying that

$$\binom{p}{k} = \frac{p}{k} \cdot \binom{p-1}{k-1}.$$

Hence,

$$k\binom{p}{k} = p\binom{p-1}{k-1}.$$

Hence, $k\dbinom{p}{k}$ is divisible by p. But k is coprime to p (since p is prime), so we can cancel k from this divisibility, and conclude that $\dbinom{p}{k}$ is divisible by p. Lemma 5.3.9 is proved. (See [Grinbe21, discussion of Exercise 9.1.6] for another proof.) □

Proof of Theorem 5.3.8. **(a)** Let $a, b \in F$. Then, $ab = ba$ (since F is commutative); thus, the Binomial Formula yields

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p. \tag{101}$$

Now, we claim that all the addends in the sum $\sum_{k=1}^{p-1} \dbinom{p}{k} a^k b^{p-k}$ vanish. Indeed, let $k \in \{1, 2, \ldots, p-1\}$. Then, Lemma 5.3.9 tells us that $\dbinom{p}{k} = mp$ for some $m \in \mathbb{Z}$. Consider this m. Then, each $u \in F$ satisfies $\dbinom{p}{k} u =$

$m \underbrace{pu}_{\substack{=0 \\ \text{(by Theorem 5.2.2 \textbf{(b)})}}} = m \cdot 0 = 0$. Hence, in particular, we have

$$\binom{p}{k} a^k b^{p-k} = 0. \tag{102}$$

Now, forget that we fixed k. We thus have shown that (102) holds for each $k \in \{1, 2, \ldots, p-1\}$. Hence, (101) becomes

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k} a^k b^{p-k}}_{\substack{=0 \\ \text{(by (102))}}} + b^p = a^p + b^p.$$

This proves Theorem 5.3.8 **(a)**.

(b) This follows by induction on m using Theorem 5.3.8 **(a)**, since any $u \in F$ satisfies $u^{p^m} = \left(u^{p^{m-1}}\right)^p$.

(c) Let $a, b \in F$. Applying Theorem 5.3.8 **(a)** to $a - b$ instead of a, we get

$$((a-b)+b)^p = (a-b)^p + b^p.$$

Solving this for $(a-b)^p$, we get

$$(a-b)^p = \left(\underbrace{(a-b)+b}_{=a}\right)^p - b^p = a^p - b^p.$$

This proves Theorem 5.3.8 **(c)**.

(d) This follows by induction on m using Theorem 5.3.8 **(c)**. □

Corollary 5.3.10. Let p be a prime number. Let F be a field of characteristic p, or, more generally, any commutative $\mathbb{Z}/p$-algebra. Then, the map

$$\begin{aligned} F &\to F, \\ a &\mapsto a^p \end{aligned}$$

is a ring morphism.

Proof. Theorem 5.3.8 **(a)** says that this map respects addition. But it is also clear that this map respects multiplication (since $(ab)^p = a^p b^p$ for any $a, b \in F$) and respects zero and unity (since $0^p = 0$ and $1^p = 1$). Thus, it is a ring morphism. □

The ring morphism in Corollary 5.3.10 is known as the **Frobenius endomorphism** of F. It exists for arbitrary commutative $\mathbb{Z}/p$-algebras, but it is particularly well-behaved for finite fields. In particular, it is bijective when F is a finite field:

Exercise 5.3.2. Let p be a prime number. Let F be a finite field of characteristic p. Let f be the Frobenius endomorphism of F (that is, the map $F \to F,\ a \mapsto a^p$). Recall that f is a ring morphism (by Corollary 5.3.10).

(a) Prove that f is a ring isomorphism from F to F (so it is invertible).

(b) Now, replace the words "field of characteristic p" by the (more general) "commutative $\mathbb{Z}/p$-algebra" in the above. Find an example where the claim of part **(a)** becomes false.

We will use the Idiot's Binomial Formula to construct finite fields, but it has many other applications. Here is just one:

Exercise 5.3.3. Let p be a prime number.

(a) Prove that $(1+x)^{ap+c} = (1+x^p)^a (1+x)^c$ in the polynomial ring $(\mathbb{Z}/p)[x]$ for any $a, c \in \mathbb{N}$.

(b) Prove **Lucas's congruence**: Any $a, b \in \mathbb{N}$ and any $c, d \in \{0, 1, \ldots, p-1\}$ satisfy

$$\binom{ap+c}{bp+d} \equiv \binom{a}{b}\binom{c}{d} \bmod p.$$

The following exercise is a converse to Lemma 5.3.9:

Exercise 5.3.4. Let $n > 1$ be an integer that is not prime. Prove that there exists some $k \in \{1, 2, \ldots, n-1\}$ such that $n \nmid \binom{n}{k}$.

[**Hint:** Let k be a prime divisor of n.]

5.3.4. The derivative of a polynomial

Our last tool is optional, as we will use it in one proof but avoid it in an alternative proof of the same claim. Nevertheless, it is worth seeing, since its usefulness is not limited to the cursory use we will put it to. This tool is the notion of the "formal" (i.e., purely algebraic) **derivative** of a polynomial (which is defined over an arbitrary commutative ring, not just over the real or complex numbers):

Definition 5.3.11. Let R be a commutative ring. Let $f \in R[x]$ be a polynomial. The **derivative** f' of f is a polynomial in $R[x]$ defined as follows: Writing f in the form

$$f = \sum_{k \in \mathbb{N}} f_k x^k = f_0 x^0 + f_1 x^1 + f_2 x^2 + f_3 x^3 + \cdots$$

for some $f_0, f_1, f_2, \ldots \in R$, we set

$$f' = \sum_{k>0} f_k k x^{k-1} = f_1 \cdot 1 x^0 + f_2 \cdot 2 x^1 + f_3 \cdot 3 x^2 + f_4 \cdot 4 x^3 + \cdots$$

For example, if $f = 7x^4 + 2x + 3$, then $f' = 7 \cdot 4x^3 + 2 \cdot 1x^0 = 28x^3 + 2$ (where we have, of course, ignored zero coefficients).

Definition 5.3.11 is obviously inspired by the formula for the derivative of a polynomial function in calculus. Unlike in calculus, we are not wasting our time with little εs and convergence issues; instead, we are just defining f' using the explicit formula that probably took you some time to prove back in calculus. There is no free lunch here – with this definition, you cannot re-use anything you have learned about derivatives in your analysis classes (already because you are working in a much more general setting now, with a commutative ring R instead of the real numbers); thus, a host of basic properties of derivatives need to be proven before the notion becomes useful. In particular, the following needs to be shown:

Proposition 5.3.12. Let R be a commutative ring. Let $f, g \in R[x]$. Then:

(a) We have $(f+g)' = f' + g'$.

(b) We have $(fg)' = f'g + fg'$. (This is called the **Leibniz rule**.)

Exercise 5.3.5. Prove Proposition 5.3.12.

[**Hint:** For part **(b)**, it is easiest to first prove it in the particular case when $f = x^a$ and $g = x^b$ for some a and b, and then obtain the general case by interchanging summations.]

The following corollary is an algebraic analogue of the well-known fact "a double root of a polynomial is a root of its derivative":

Corollary 5.3.13. Let R be a commutative ring. Let $f \in R[x]$ and $r \in R$. If $(x-r)^2 \mid f$ in $R[x]$, then $x - r \mid f'$ in $R[x]$.

Proof. Assume that $(x-r)^2 \mid f$. Thus, we can write f as $f = (x-r)^2 g$ for some $g \in R[x]$. Consider this g. From $f = (x-r)^2 g$, we obtain

$$f' = \left((x-r)^2 g\right)' = \underbrace{\left((x-r)^2\right)'}_{\substack{=2(x-r) \\ \text{(this is easy to} \\ \text{check directly)}}} g + (x-r)^2 g' \qquad \text{(by the Leibniz rule)}$$

$$= 2(x-r) g + (x-r)^2 g' = (x-r)\left(2g + (x-r) g'\right).$$

Thus, $x - r \mid f'$, so that Corollary 5.3.13 is proven. □

Corollary 5.3.13 can be applied (in its contrapositive) as a sufficient criterion for a polynomial to have distinct roots. This is exactly how we will soon apply it. We note that Corollary 5.3.13 also has a converse:

Exercise 5.3.6. Let R be a commutative ring. Let $f \in R[x]$ and $r \in R$. If r is a root of both f and f', then prove that $(x-r)^2 \mid f$ in $R[x]$.

Here are some further properties of derivatives of polynomials:

Exercise 5.3.7. Let R be a commutative ring. Let $f \in R[x]$ be any polynomial. Prove the following:

(a) We have $\deg(f') \leq \deg f - 1$.

(b) If R is a $\mathbb{Q}$-algebra and f is not constant, then $\deg(f') = \deg f - 1$.

Exercise 5.3.8.

(a) Let R be a commutative ring. Let $f, g \in R[x]$ be any two polynomials. Prove that $(f[g])' = f'[g] \cdot g'$. (This is called the **chain rule for polynomials**, and is the algebraic analogue of the chain rule in calculus.)

(b) Use this chain rule to give a different proof of the equality $\left((x-r)^2\right)' = 2(x-r)$ in the above proof of Corollary 5.3.13.

Exercise 5.3.9. Let R be a commutative ring. Let $f \in R[x]$ be a polynomial. Consider also the polynomial ring $R[x,y]$ in two indeterminates x and y.

(a) Prove that there is a unique polynomial $g \in R[x,y]$ satisfying $f[y] - f[x] = (y-x) \cdot g$.

(b) Prove that this polynomial g satisfies $g[x,x] = f'$.

(Because of its definition, the polynomial g can be written as $\dfrac{f[y]-f[x]}{y-x}$, even though $y-x$ is not a unit of $R[x,y]$. However, when computing $g[x,x]$, we cannot just set y to x in the fraction $\dfrac{f[y]-f[x]}{y-x}$; instead, we must first expand this fraction into a polynomial. Thus, the claim of part **(b)** is the algebraic analogue of the formula $f'(x) = \lim\limits_{y\to x} \dfrac{f(y)-f(x)}{y-x}$ from calculus.)

Exercise 5.3.10. Let R be a commutative ring. Recall the R-algebra $\mathbb{D}_R$ of R-dual numbers from Exercise 3.11.2. Let ε be the element $(0,1)$ of $\mathbb{D}_R$. Let $f \in R[x]$ be an arbitrary polynomial. Prove that

$$f[(a,b)] = \left(f[a],\ bf'[a]\right) \qquad \text{in } \mathbb{D}_R.$$

(In other words, prove that $f[a+b\varepsilon] = f[a] + bf'[a]\,\varepsilon$, where we are identifying each element $r \in R$ with the R-dual number $(r,0) \in \mathbb{D}_R$.)

Exercise 5.3.11. Let R be a commutative ring.

Let $D : R[x] \to R[x]$ be the map sending each polynomial f to its derivative f'. We refer to D as **(formal) differentiation**. As usual, for any $n \in \mathbb{N}$, we let D^n denote $\underbrace{D \circ D \circ \cdots \circ D}_{n \text{ times}}$ (which means id if $n = 0$).

Prove the following:

(a) The map $D : R[x] \to R[x]$ is R-linear.

(b) We have $D^n\left(x^k\right) = n!\dbinom{k}{n} x^{k-n}$ for all $n \in \mathbb{N}$ and $k \in \mathbb{N}$. Here, the expression "$\dbinom{k}{n} x^{k-n}$" is to be understood as 0 when $k < n$.

(c) If $\mathbb{Q}$ is a subring of R, then every polynomial $f \in R[x]$ satisfies

$$f[x+a] = \sum_{n\in\mathbb{N}} \frac{1}{n!} \left(D^n(f)\right)[a] \cdot x^n \qquad \text{for all } a \in R.$$

(The infinite sum on the right hand side has only finitely many nonzero addends.)

(d) If p is a prime such that $p \cdot 1_R = 0$ (for example, this happens if $R = \mathbb{Z}/p$), then $D^p(f) = 0$ for each $f \in R[x]$.

Exercise 5.3.12. Let R be a commutative ring such that $\mathbb{Q}$ is a subring of R. For each polynomial

$$f = \sum_{k\in\mathbb{N}} f_k x^k = f_0 x^0 + f_1 x^1 + f_2 x^2 + \cdots \in R[x] \qquad (\text{where } f_i \in R),$$

we define the **(formal) integral** $\int f$ of f to be the polynomial

$$\sum_{k\in\mathbb{N}} \frac{1}{k+1} f_k x^{k+1} = \frac{1}{1} f_0 x^1 + \frac{1}{2} f_1 x^2 + \frac{1}{3} f_2 x^3 + \cdots \in R[x].$$

(This definition imitates the standard procedure for integrating power series in analysis, but again works for any commutative ring R that contains $\mathbb{Q}$ as subring.)

Let $J : R[x] \to R[x]$ be the map sending each polynomial f to its integral $\int f$. Prove the following:

(a) The map $J : R[x] \to R[x]$ is R-linear.

(b) We have $D \circ J = \mathrm{id}$ (where D is as in Exercise 5.3.11).

(c) We have $J \circ D \neq \mathrm{id}$.

5.4. Existence of finite fields

Now we are in walking distance of the existence of fields of size p^m:

Theorem 5.4.1. Let p be a prime number. Let m be a positive integer. Then, there exists a finite field of size p^m.

Proof. From $p > 1$ and $m > 0$, we obtain $p^m > 1$. Hence, the polynomial $x^{p^m} - x$ is monic. Thus, by Theorem 5.3.7 **(c)**, there exists a splitting field of this polynomial over $\mathbb{Z}/p$. Let S be such a splitting field. Thus, the polynomial $x^{p^m} - x$ splits over S. In other words, there exist elements $r_1, r_2, \ldots, r_{p^m}$ of S such that

$$x^{p^m} - x = (x - r_1)(x - r_2) \cdots \left(x - r_{p^m}\right). \tag{103}$$

Consider these $r_1, r_2, \ldots, r_{p^m}$.

Let

$$L = \left\{r_1, r_2, \ldots, r_{p^m}\right\}.$$

Our goal will be to show that L is a finite field of size p^m.

Everything in this statement needs proof![159] Even the size is not obvious, let alone that L is a field. Let us start with the size:

Claim 1: We have $|L| = p^m$.

Let us give two proofs of Claim 1:

[*First proof of Claim 1:* This amounts to showing that $r_1, r_2, \ldots, r_{p^m}$ are distinct (since this will immediately yield that $L = \left\{r_1, r_2, \ldots, r_{p^m}\right\}$ is a p^m-element set). Let us thus do this. Indeed, assume the contrary. Then, $r_i = r_j$ for some $i < j$. Hence, the $x - r_i$ and $x - r_j$ factors on the right hand side of (103) are identical.

[159] Except for the "finite" part, which is obvious but not overly helpful by itself.

Thus, $x - r_i$ appears twice as a factor on this right hand side; consequently, (103) entails that $(x - r_i)^2 \mid x^{p^m} - x$. Hence, Corollary 5.3.13 (applied to $R = S$ and $f = x^{p^m} - x$ and $r = r_i$) yields $x - r_i \mid \left(x^{p^m} - x\right)'$. But Definition 5.3.11 yields

$$\left(x^{p^m} - x\right)' = \underbrace{p^m x^{p^m - 1}}_{\substack{=0 \\ \text{(since } pu = 0 \\ \text{for any } u \in S\text{)}}} - 1 = -1.$$

Thus, $x - r_i \mid \left(x^{p^m} - x\right)' = -1 \mid 1$. But it is impossible for the degree-1 polynomial $x - r_i$ to divide the degree-0 polynomial 1 (for degree reasons). So we have found a contradiction.]

[*Second proof of Claim 1:* The following proof of Claim 1 (which I have learnt from [Shifri96, Chapter 5, Theorem 3.3]) avoids the use of derivatives.

Again, it suffices to show that $r_1, r_2, \ldots, r_{p^m}$ are distinct. Again, assume the contrary. Then, $r_i = r_j$ for some $i < j$. As before, we then find that $(x - r_i)^2 \mid x^{p^m} - x$. In other words, $x^{p^m} - x = (x - r_i)^2 \cdot g$ for some polynomial $g \in S[x]$. Consider this g. Substituting r_i for x in the equality $x^{p^m} - x = (x - r_i)^2 \cdot g$, we obtain $r_i^{p^m} - r_i = \underbrace{(r_i - r_i)^2}_{=0} \cdot g[r_i] = 0$. In other words, $r_i^{p^m} = r_i$.

Substituting $x + r_i$ for x in the equality $x^{p^m} - x = (x - r_i)^2 \cdot g$, we obtain

$$(x + r_i)^{p^m} - (x + r_i) = \left(\underbrace{x + r_i - r_i}_{=x}\right)^2 \cdot g[x + r_i] = x^2 \cdot g[x + r_i].$$

In view of

$$\underbrace{(x + r_i)^{p^m}}_{\substack{=x^{p^m} + r_i^{p^m} \\ \text{(by Theorem 5.3.8 \textbf{(b)})}}} - (x + r_i) = x^{p^m} + \underbrace{r_i^{p^m}}_{=r_i} - (x + r_i) = x^{p^m} + r_i - (x + r_i) = x^{p^m} - x,$$

we can rewrite this as $x^{p^m} - x = x^2 \cdot g[x + r_i]$. Thus, $x^2 \mid x^{p^m} - x$. But this is visibly absurd. Thus, we have found a contradiction again.]

Next, let us characterize L somewhat differently:

Claim 2: We have

$$L = \left\{\text{the roots of } x^{p^m} - x \text{ in } S\right\} = \left\{a \in S \mid a^{p^m} - a = 0\right\}$$
$$= \left\{a \in S \mid a^{p^m} = a\right\}.$$

[*Proof of Claim 2:* The equation (103) yields that

$$\begin{aligned}
&\left\{\text{the roots of } x^{p^m} - x \text{ in } S\right\} \\
&= \left\{\text{the roots of } (x - r_1)(x - r_2) \cdots \left(x - r_{p^m}\right) \text{ in } S\right\} \\
&= \left\{r_1, r_2, \ldots, r_{p^m}\right\} \qquad \text{(by Proposition 5.3.3)} \\
&= L.
\end{aligned}$$

Hence,

$$\begin{aligned}
L &= \left\{\text{the roots of } x^{p^m} - x \text{ in } S\right\} = \left\{a \in S \mid a^{p^m} - a = 0\right\} \\
&= \left\{a \in S \mid a^{p^m} = a\right\}.
\end{aligned}$$

This proves Claim 2.]

Now, why is L a field? First, let us check that L is a ring:

Claim 3: The set L is a subring of S.

[*Proof of Claim 3:* Claim 2 yields that

$$L = \left\{a \in S \mid a^{p^m} = a\right\}. \tag{104}$$

Hence, $0 \in L$ (since $0^{p^m} = 0$) and $1 \in L$ (since $1^{p^m} = 1$). Furthermore, I claim that L is closed under addition. Indeed, if $a, b \in L$, then (104) yields $a^{p^m} = a$ and $b^{p^m} = b$, so that

$$\begin{aligned}
(a+b)^{p^m} &= \underbrace{a^{p^m}}_{=a} + \underbrace{b^{p^m}}_{=b} \qquad \text{(by Theorem 5.3.8 \textbf{(b)})} \\
&= a + b,
\end{aligned}$$

and this means $a + b \in L$ (again because of (104)). This shows that L is closed under addition. For a similar reason, L is closed under subtraction[160], so that L is closed under negation. Finally, L is closed under multiplication, since $(ab)^{p^m} = a^{p^m} b^{p^m}$ for any $a, b \in L$. Hence, L is a subring of S.]

Thus, in particular, L is a commutative ring (since S is a field, thus a commutative ring). Now, let us see that L is a field:

Claim 4: The ring L is a field.

[*Proof of Claim 4:* We know that S is a field, so that $0 \neq 1$ in S, and this of course means that $0 \neq 1$ in L. It thus remains to show that every nonzero element of L is a unit.

[160] Use Theorem 5.3.8 **(d)** instead of Theorem 5.3.8 **(b)** here.

Let $a \in L$ be nonzero. Then, a has an inverse in S, since S is a field. This inverse a^{-1} satisfies $\left(a^{-1}\right)^{p^m} = \left(a^{p^m}\right)^{-1}$ (indeed, this is a particular case of the identity $\left(g^{-1}\right)^k = \left(g^k\right)^{-1}$, which holds whenever g is an element of a group and k is an integer). But $a \in L$ and thus $a^{p^m} = a$ (by (104)). Hence,

$$\left(a^{-1}\right)^{p^m} = \left(\underbrace{a^{p^m}}_{=a}\right)^{-1} = a^{-1},$$

so that $a^{-1} \in L$ (by (104) again). Thus, a has an inverse in L; in other words, a is a unit of L.

Thus, we have shown that every nonzero element of L is a unit. As we said, this finishes the proof of Claim 4.]

Combining Claims 1 and 4, we conclude that L is a field of size p^m. Thus, such a field exists. This proves Theorem 5.4.1. □

So we are done with the first deep result of this course! But some further questions suggest themselves:

- We have obtained L rather indirectly: First, we took a splitting field S of the huge polynomial $x^{p^m} - x$; then we carved L out of it by taking the roots of this polynomial. Could we get L more directly? For example, if there is an irreducible polynomial f of degree m over $\mathbb{Z}/p$, then we can just take the field $(\mathbb{Z}/p)[x]/f$. Is there such an f ?

- Can there be several non-isomorphic fields of size p^m (for fixed p and m)? For example, can there be two non-isomorphic fields of size p^2 ? It is not hard to see that any field of size p^2 can be obtained (up to isomorphism) by adjoining a root of an irreducible quadratic polynomial to $\mathbb{Z}/p$; thus, the question is whether different such polynomials can lead to different fields.

  If we were working with infinite fields, examples of such behavior would be easy to find. For example, adjoining a root of $x^2 - 2$ to $\mathbb{Q}$ yields the field $\mathbb{Q}\left[\sqrt{2}\right]$, whereas adjoining a root of $x^2 - 3$ to $\mathbb{Q}$ yields the field $\mathbb{Q}\left[\sqrt{3}\right]$. It is not hard to see that $\mathbb{Q}\left[\sqrt{2}\right]$ is not isomorphic to $\mathbb{Q}\left[\sqrt{3}\right]$ (for example, you can show that 2 is a square in $\mathbb{Q}\left[\sqrt{2}\right]$ but not in $\mathbb{Q}\left[\sqrt{3}\right]$). Can this happen with $\mathbb{Z}/p$ instead of $\mathbb{Q}$?

These questions will be answered in the next section.

5.5. Uniqueness of finite fields

Theorem 5.4.1 shows that for any prime power p^m, there exists a finite field of size p^m. The next natural question is: How many such fields are there? Literally, of course, there are infinitely many, since each one has infinitely many isomorphic (but not literally identical) copies. Of course, the right question to ask is how many non-isomorphic finite fields there are of a given size.

The answer is surprisingly simple: There is only one. Proving this will take us some work. (This section is more abstract and notationally dense than many others, and can be skipped.)

5.5.1. Annihilating polynomials and minimal polynomials

We begin with two fundamental concepts of Galois theory: the notions of "annihilating polynomials" and of "minimal polynomials". We will not delve deeper than this into Galois theory, but we will explore these notions in some detail.

Roughly speaking, the main problem of classical algebra is solving polynomial equations: Given a polynomial f, what are its roots? Our abstract viewpoint has allowed us to extend the field over which the polynomial is defined, and in such an extension we can always find a root for any non-constant univariate polynomial (see Theorem 5.3.7 **(b)**).

We now turn the question around: Given an element a of a field F, what are the polynomials f that have a as a root? If we want f to belong to $F[x]$, then this is an easy question, and the answer is "exactly those polynomials that are divisible by $x - a$" (see Proposition 4.3.14). But this question becomes more interesting if we require f to belong to $S[x]$, where S is a smaller field than F. For instance, a could be the imaginary unit $i = \sqrt{-1} \in \mathbb{C}$, and S could be the field $\mathbb{R}$, so we would be asking about the real polynomials that have i as a root. Clearly, $x^2 + 1$ is one of these, and thus any multiple of $x^2 + 1$ qualifies as well. Are there any others?

To study this kind of question, we introduce the notions of annihilating and minimal polynomials:[161]

Definition 5.5.1. Let S and F be two fields such that S is a subring of F. (For example, we can take $S = \mathbb{Q}$ and $F = \mathbb{R}$.)

Let $a \in F$ be an arbitrary element.

(a) An **annihilating polynomial** of a shall mean a polynomial $f \in S[x]$ such that a is a root of f. For instance:

- If $a \in S$, then $x - a$ is an annihilating polynomial of a.
- If a is a square root of an element $v \in S$, then $x^2 - v$ is an annihilating polynomial of a.

[161] Mnemonic: The letters S and F refer to "subfield" and "field".

- If $S = \mathbb{Q}$ and $F = \mathbb{R}$, then $x^4 - 10x^2 + 1$ is an annihilating polynomial of $\sqrt{2} + \sqrt{3}$.
- The real number π is known to be transcendental; this means that there exists no nonzero annihilating polynomial of π (for $S = \mathbb{Q}$ and $F = \mathbb{R}$).

(b) The **minimal polynomial** of a (over the subfield S) is defined to be the monic annihilating polynomial of a of smallest possible degree (if such a polynomial exists).[162]

It is not yet clear that the minimal polynomial of a really deserves the definite article! Couldn't there be several monic annihilating polynomials of a of smallest possible degree? Which of them deserves to be called "the" minimal polynomial?

Fortunately, this question never arises, since there is only one:

Theorem 5.5.2. Let S and F be two fields such that S is a subring of F. Let $a \in F$. Then:

(a) The minimal polynomial of a is unique if it exists. That is, if there is at least one monic annihilating polynomial of a, then only one of these polynomials has smallest possible degree.

(b) The minimal polynomial of a is always irreducible if it exists.

(c) If f is the minimal polynomial of a, then the map

$$\begin{aligned} S[x]/f &\to F, \\ \overline{g} &\mapsto g[a] \end{aligned}$$

is a (well-defined) S-algebra morphism, and is injective.

(d) Assume that a has a minimal polynomial. Let f be the minimal polynomial of a. Then, the annihilating polynomials of a are precisely the polynomials $g \in S[x]$ that are divisible by f.

Before we prove this, let us show a lemma:

[162] Thus, the minimal polynomial of a is defined in the exact same way as the minimal polynomial of a square matrix was defined in linear algebra. However, the minimal polynomial of a matrix is not always irreducible, whereas in our case the minimal polynomial will be irreducible (see below).

Lemma 5.5.3. Let S and F be two fields such that S is a subring of F. Let $a \in F$.

Let $f \in S[x]$ be a minimal polynomial of a. (We could say "**the** minimal polynomial of a" if we knew that it is unique, but we don't know this yet; we will prove this soon.)

Let $g \in S[x]$ be any polynomial. Then:

(a) If $g[a] = 0$, then $f \mid g$.

(b) If $f \mid g$, then $g[a] = 0$.

Proof of Lemma 5.5.3. We know that f is a minimal polynomial of a. Thus, f is a monic annihilating polynomial of a. Hence, a is a root of f; in other words, $f[a] = 0$. Also, the leading coefficient of f is 1 (since f is monic), and thus is a unit of S. Hence, Theorem 4.3.7 **(a)** (applied to S, f and g instead of R, b and a) yields that there is a unique pair (q, r) of polynomials in $S[x]$ such that

$$g = qf + r \qquad \text{and} \qquad \deg r < \deg f.$$

Consider this pair (q, r).

(a) Assume that $g[a] = 0$. Thus,

$$\begin{aligned} 0 = g[a] &= (qf + r)[a] \qquad (\text{since } g = qf + r) \\ &= q[a] \cdot \underbrace{f[a]}_{=0} + r[a] = r[a]. \end{aligned}$$

Hence, $r[a] = 0$.

We assume (for the sake of contradiction) that $r \neq 0$. Hence, r has a leading coefficient λ. Consider this λ. This λ is nonzero, and thus is a unit of S (since S is a field). Hence, the polynomial $\lambda^{-1} r$ is well-defined. Moreover, since λ^{-1} is a nonzero constant, we have $\deg\left(\lambda^{-1} r\right) = \deg r < \deg f$.

However, $\left(\lambda^{-1} r\right)[a] = \lambda^{-1} \cdot \underbrace{r[a]}_{=0} = 0$. In other words, a is a root of $\lambda^{-1} r$. Thus, $\lambda^{-1} r$ is an annihilating polynomial of a. Furthermore, this polynomial $\lambda^{-1} r$ is monic (since λ is the leading coefficient of r, so that scaling r by λ^{-1} turns the leading coefficient into 1).

Now, recall that f is a minimal polynomial of a. In other words, f is a monic annihilating polynomial of a of smallest possible degree. Therefore, $\deg\left(\lambda^{-1} r\right) \geq \deg f$ (since $\lambda^{-1} r$, too, is a monic annihilating polynomial of a). This contradicts $\deg\left(\lambda^{-1} r\right) < \deg f$. This contradiction shows that our assumption (that $r \neq 0$) was false. Hence, $r = 0$.

Now, $g = qf + \underbrace{r}_{=0} = qf$, so that $f \mid g$. This proves Lemma 5.5.3 **(a)**.

(b) Assume that $f \mid g$. Thus, $g = fq$ for some $q \in S[x]$. Consider this q. From $g = fq$, we obtain $g[a] = (fq)[a] = \underbrace{f[a]}_{=0} \cdot q[a] = 0$. Thus, Lemma 5.5.3 **(b)** is proved. □

Proof of Theorem 5.5.2. **(a)** Assume that a has a minimal polynomial. We must show that the minimal polynomial of a is unique.

Assume the contrary. Thus, there exist two distinct minimal polynomials f and g of a. Consider these f and g. Both f and g are minimal polynomials of a, and thus are monic annihilating polynomials of a. In particular, we have $g[a] = 0$ (since g is an annihilating polynomial of a). Hence, Lemma 5.5.3 **(a)** yields $f \mid g$. The same argument (but with the roles of f and g interchanged) yields $g \mid f$.

We have $f \mid g$. In other words, there exists a polynomial $q \in S[x]$ such that $g = fq$. Consider this q. We have $fq = g \neq 0$ (since g is monic) and thus $q \neq 0$. Also, $f \neq 0$ (since f is monic). But F is a field and thus an integral domain. Hence, Proposition 4.3.5 **(c)** yields $\deg(fq) = \deg f + \deg q$. In view of $g = fq$, this rewrites as $\deg g = \deg f + \deg q$. Hence, $\deg g \geq \deg f$ (since $q \neq 0$ entails $\deg q \geq 0$). Similarly, $\deg f \geq \deg g$. Combining these two inequalities, we find $\deg f = \deg g$.

Thus, $\deg f = \deg g = \deg f + \deg q$, so that $\deg q = 0$ (since $f \neq 0$ entails $\deg f \geq 0$). In other words, q is a nonzero constant.

The leading coefficient of f is 1 (since f is monic). Thus, the leading coefficient of fq is q (since q is a nonzero constant). In view of $fq = g$, this rewrites as follows: The leading coefficient of g is q. However, the leading coefficient of g is 1 (since g is monic). Comparing the previous two sentences, we conclude that $q = 1$. Hence, $g = f \underbrace{q}_{=1} = f$. This contradicts our assumption that f and g are distinct. This contradiction shows that our assumption was wrong. Theorem 5.5.2 **(a)** is thus proved.

(b) Assume that a has a minimal polynomial. Let f be the minimal polynomial of a. We must show that f is irreducible.

Recall that f is the minimal polynomial of a. In other words, f is a monic annihilating polynomial of a of smallest possible degree. Thus, a is a root of f (since f is an annihilating polynomial of a); in other words, $f[a] = 0$. Thus, f cannot be a nonzero constant (because this would entail $f[a] = f \neq 0$, contradicting $f[a] = 0$). Hence, f is not a unit of the ring $S[x]$. (This is something that needs to be checked if you want to show that f is irreducible. Don't forget about this!)

Now, let $u, v \in S[x]$ be such that $uv = f$. We shall show that at least one of u and v is a unit of $S[x]$.

Indeed, assume the contrary. Thus, neither u nor v is a unit of $S[x]$. Moreover, neither u nor v equals 0 (since $uv = f \neq 0$). Hence, neither u nor v is constant (since a constant polynomial is either a unit of $S[x]$ or equals 0). Thus, $\deg u \geq$

1 and $\deg v \geq 1$. However, $f = uv$ and thus $\deg f = \deg(uv) = \deg u + \deg v$ (since F is a field and thus an integral domain). Hence, $\deg f = \deg u + \underbrace{\deg v}_{\geq 1 > 0} > \deg u$, so that $\deg u < \deg f$.

Now, $f = uv$, so that $f[a] = (uv)[a] = u[a] \cdot v[a]$ and therefore $u[a] \cdot v[a] = f[a] = 0$. Since F is a field and thus an integral domain, this entails that $u[a] = 0$ or $v[a] = 0$. We WLOG assume that $u[a] = 0$ (since otherwise, we can simply swap u with v). Let λ denote the leading coefficient of u (this is well-defined, since u does not equal 0). Then, the polynomial $\lambda^{-1}u$ is monic, and is an annihilating polynomial of a (since $\left(\lambda^{-1}u\right)[a] = \lambda^{-1} \cdot \underbrace{u[a]}_{=0} = 0$). Thus, the degree of this polynomial $\lambda^{-1}u$ must be at least as large as that of f (since f is a monic annihilating polynomial of a of smallest possible degree). In other words, $\deg\left(\lambda^{-1}u\right) \geq \deg f$. This contradicts $\deg\left(\lambda^{-1}u\right) = \deg u < \deg f$.

This contradiction shows that our assumption was wrong. Hence, at least one of u and v is a unit of $S[x]$.

Forget that we fixed u, v. We thus have shown that whenever $u, v \in S[x]$ satisfy $uv = f$, at least one of u and v is a unit of $S[x]$. Thus, f is irreducible (since f is not a unit of $S[x]$). This proves Theorem 5.5.2 **(b)**.

(c) Assume that a has a minimal polynomial. Let f be the minimal polynomial of a. Thus, f is a monic annihilating polynomial of a. Hence, $f[a] = 0$.

We know that F is an S-algebra (since F is a commutative ring, and S is a subring of F). The map

$$\begin{aligned} \varphi : S[x] &\to F, \\ g &\mapsto g[a] \end{aligned}$$

is an S-algebra morphism (by Theorem 4.2.8). This map φ sends the principal ideal $fS[x]$ to 0, because for each $q \in S[x]$, we have

$$\varphi(fq) = (fq)[a] = \underbrace{f[a]}_{=0} \cdot q[a] = 0.$$

Hence, the universal property of quotient algebras (Theorem 4.4.3, applied to S, $S[x]$, $fS[x]$, F and φ instead of R, A, I, B and f) yields that the map

$$\begin{aligned} \varphi' : S[x]/f &\to F, \\ \overline{g} &\mapsto \varphi(g) \qquad \text{(for all } g \in S[x]\text{)} \end{aligned}$$

is well-defined and is an S-algebra morphism. Consider this φ'. Thus, each $g \in S[x]$ satisfies

$$\begin{aligned} \varphi'(\overline{g}) &= \varphi(g) \qquad \text{(by the definition of } \varphi'\text{)} \\ &= g[a] \qquad \text{(by the definition of } \varphi\text{)}. \end{aligned} \tag{105}$$

Thus, φ' is precisely the map

$$\begin{aligned} S[x]/f &\to F, \\ \overline{g} &\mapsto g[a] \end{aligned}$$

that Theorem 5.5.2 **(c)** is talking about. In particular, we now know that this map is well-defined and is an S-algebra morphism. It remains to prove that this map φ' is injective.

Since φ' is S-linear, it suffices to show that $\operatorname{Ker}(\varphi') = \{0\}$ (by Lemma 3.5.10).

Let $u \in \operatorname{Ker}(\varphi')$. We shall prove that $u = 0$.

Indeed, we have $u \in \operatorname{Ker}(\varphi') \subseteq S[x]/f$, so that $u = \overline{g}$ for some $g \in S[x]$. Consider this g. We have $\varphi'(\overline{g}) = 0$ (since $\overline{g} = u \in \operatorname{Ker}(\varphi')$), so that $0 = \varphi'(\overline{g}) = g[a]$ (by (105)). Hence, Lemma 5.5.3 **(a)** yields $f \mid g$. In other words, $\overline{g} = 0$ in $S[x]/f$. Hence, $u = \overline{g} = 0 \in \{0\}$.

Forget that we fixed u. We thus have shown that $u \in \{0\}$ for each $u \in \operatorname{Ker}(\varphi')$. In other words, $\operatorname{Ker}(\varphi') \subseteq \{0\}$. Since the reverse inclusion $\{0\} \subseteq \operatorname{Ker}(\varphi')$ is obvious, we thus conclude that $\operatorname{Ker}(\varphi') = \{0\}$. As we have said, this entails that φ' is injective. This completes the proof of Theorem 5.5.2 **(c)**.

(d) We must show that the annihilating polynomials of a are precisely the polynomials $g \in S[x]$ that are divisible by f. In other words, we must prove the following two statements:

> *Statement 1:* Any annihilating polynomial of a is divisible by f.
>
> *Statement 2:* Any polynomial $g \in S[x]$ that is divisible by f is an annihilating polynomial of a.

Fortunately, Statement 1 is just a restatement of Lemma 5.5.3 **(a)** (since an annihilating polynomial of a is precisely a polynomial $g \in S[x]$ such that $g[a] = 0$), and Statement 2 is likewise a restatement of Lemma 5.5.3 **(b)**. Thus, both Statements 1 and 2 have already been proven, and Theorem 5.5.2 **(d)** is proved. □

Corollary 5.5.4. Let S and F be two fields such that S is a subring of F. Let $a \in F$.

Let $g \in S[x]$ be a monic irreducible polynomial such that $g[a] = 0$. Then, g is the minimal polynomial of a (over S).

Proof. We have $g[a] = 0$. In other words, a is a root of g. In other words, g is an annihilating polynomial of a. We thus conclude that a has a monic annihilating polynomial in $S[x]$ (namely, g). Hence, there exists at least one monic annihilating polynomial of a in $S[x]$. Thus, there also exists such a polynomial of smallest degree. In other words, a has a minimal polynomial.

Let f be this minimal polynomial. Thus, f is monic. Moreover, f is irreducible (by Theorem 5.5.2 **(b)**), and hence cannot be a unit of $S[x]$.

Furthermore, Lemma 5.5.3 **(a)** yields that $f \mid g$ (since $g[a] = 0$). In other words, there exists a polynomial $q \in S[x]$ such that $g = fq$. Consider this q. Since g is irreducible, we conclude that one of f and q is a unit (since $g = fq$). Since f cannot be a unit, we thus conclude that q is a unit. In other words, q is a nonzero scalar. This scalar q must be 1 (since both f and $fq = g$ are monic). Thus, $g = f \underbrace{q}_{=1} = f$. Hence, g is the minimal polynomial of a (since f is the minimal polynomial of a). This proves Corollary 5.5.4. □

Exercise 5.5.1. Let $S = \mathbb{Q}$ and $F = \mathbb{C}$. Let $d \in \mathbb{Q}$. Prove the following:

(a) The minimal polynomial of $\sqrt{d}$ (over the field $S = \mathbb{Q}$) is $\begin{cases} x - \sqrt{d}, & \text{if } \sqrt{d} \in \mathbb{Q}; \\ x^2 - d, & \text{otherwise.} \end{cases}$

(In particular, the minimal polynomial of the imaginary unit $i = \sqrt{-1}$ is $x^2 + 1$.)

(b) The minimal polynomial of $\sqrt[3]{d}$ (over the field $S = \mathbb{Q}$) is $\begin{cases} x - \sqrt[3]{d}, & \text{if } \sqrt[3]{d} \in \mathbb{Q}; \\ x^3 - d, & \text{otherwise.} \end{cases}$

(c) If $\sqrt{d} \notin \mathbb{Q}$, then the minimal polynomial of $\sqrt[4]{d}$ (over the field $S = \mathbb{Q}$) is $x^4 - d$.

(d) What is the minimal polynomial of $\sqrt[4]{-4}$ (over the field $S = \mathbb{Q}$) ?

(e) Describe the minimal polynomial of $\sqrt[4]{d}$ in general.

[**Hint:** In part **(d)**, the answer is neither a degree-1 polynomial nor a degree-4 polynomial. In part **(e)**, there are three cases.]

Exercise 5.5.2. Let $S = \mathbb{Q}$ and $F = \mathbb{R}$. Let p and q be two positive integers such that none of p, q and pq is a perfect square (i.e., a square in $\mathbb{Z}$). (For example, we can take $p = 5$ and $q = 8$.) Let $a = \sqrt{p} + \sqrt{q} \in F$.

Let f denote the polynomial

$$\left(x^2 - p - q\right)^2 - 4pq = x^4 - 2(p+q)x^2 + (p-q)^2 \in S[x].$$

(a) Show that f is an annihilating polynomial of a (that is, $f[a] = 0$).

(b) Show that f has no rational root.

(c) Show that f is irreducible (in $S[x]$).

(d) Conclude that f is the minimal polynomial of a (over the field $S = \mathbb{Q}$).

[**Hint:** Part **(c)** is the tricky one. One way to prove it is to decompose f as

$$f = \left(x - \left(\sqrt{p} + \sqrt{q}\right)\right)\left(x - \left(\sqrt{p} - \sqrt{q}\right)\right)\left(x - \left(-\sqrt{p} + \sqrt{q}\right)\right)\left(x - \left(-\sqrt{p} - \sqrt{q}\right)\right)$$

in $\mathbb{R}[x]$, and show that no two of the four factors here yield a polynomial in $\mathbb{Q}[x]$ when multiplied. Another approach uses the fact that the polynomial f is **even** –

meaning that $f[-x] = f$, or, equivalently (since S has characteristic 0) that no odd powers of x appear in f. This can be used to argue that if $f = g_1 g_2 \cdots g_k$ is the factorization of f into monic irreducible polynomials, then substituting $-x$ for x into it must yield another factorization $f = f[-x] = g_1[-x]\, g_2[-x] \cdots g_k[-x]$ of f into monic irreducible polynomials (why are they still monic?). Since $S[x]$ is a UFD, the two factorizations must be identical (up to the order of the factors). This narrows down the possibilities for $g_1, g_2, \ldots, g_k$ substantially.]

Exercise 5.5.3. Let S and F be the subrings

$$S := \left\{ \begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix} \mid u \in \mathbb{Z}/4 \right\} \qquad \text{and} \qquad F := \left\{ \begin{pmatrix} u & v \\ 0 & u \end{pmatrix} \mid u, v \in \mathbb{Z}/4 \right\}$$

of the matrix ring $(\mathbb{Z}/4)^{2\times 2}$. It is easy to see that F is a commutative ring, and that S is a subring of F.

Let a be the element $\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix}$ of F.

(a) Prove that $a^2 = 2a = 0_{2\times 2}$.

(b) Let us extend Definition 5.5.1 from fields to commutative rings in the obvious way (i.e., replacing "field" by "commutative ring" throughout this definition). Prove that the element a of F has two minimal polynomials, namely x^2 and $x^2 + 2x$.

(c) Conclude that Theorem 5.5.2 **(a)** no longer holds if we generalize it from fields to commutative rings.

5.5.2. Minimal polynomials in finite fields

Next, we apply the notion of minimal polynomials to finite fields:

Proposition 5.5.5. Let p be a prime number. Let S be the field $\mathbb{Z}/p$.

Let F be a finite field of characteristic p. Assume that $S = \mathbb{Z}/p$ is a subring of F.

We shall use the terminology from Definition 5.5.1.

Let $a \in F$ be arbitrary. Then:

(a) The minimal polynomial of a (over S) exists (i.e., there is always at least one monic annihilating polynomial of a).

(b) If the minimal polynomial of a has degree k, then $a^{p^k} = a$.

(c) Let m be a positive integer satisfying $|F| \leq p^m$. If the minimal polynomial of a has degree k, then $k \leq m$.

Proof. First, we note that $0 \neq 1$ in F (since F is a field). Thus, F has at least two distinct elements; that is, we have $|F| > 1$.

Note also that $|S| = p$ (since $S = \mathbb{Z}/p$).

(a) Proposition 2.6.6 yields $a^{|F|} = a$. Thus, a is a root of the polynomial $x^{|F|} - x \in S[x]$. In other words, $x^{|F|} - x \in S[x]$ is an annihilating polynomial of a. Since this polynomial is monic, we thus conclude that a has a monic annihilating polynomial in $S[x]$ (namely, $x^{|F|} - x$). Hence, there exists at least one monic annihilating polynomial of a in $S[x]$. Thus, there also exists such a polynomial of smallest degree. In other words, a has a minimal polynomial. This proves Proposition 5.5.5 **(a)**.

(b) Let f be the minimal polynomial of a. Let $k = \deg f$. We must show that $a^{p^k} = a$.

Theorem 5.5.2 **(b)** shows that the polynomial f is irreducible. Hence, the quotient ring $S[x]/f$ is a field (by Theorem 4.6.3). On the other hand, the leading coefficient of f is a unit (since f is monic). Thus, as an S-module, $S[x]/f$ is free of rank $k = \deg f$ (by Theorem 4.5.9 **(b)**). Hence, $S[x]/f \cong S^k$ as an S-module. Hence, $|S[x]/f| = \left|S^k\right| = |S|^k = p^k$ (since $|S| = p$). Therefore, the field $S[x]/f$ is finite.

Now, $\overline{x} \in S[x]/f$ is an element of this finite field $S[x]/f$. Hence, Proposition 2.6.6 (applied to $S[x]/f$ and $\overline{x}$ instead of F and u) yields $\overline{x}^{|S[x]/f|} = \overline{x}$. In view of $|S[x]/f| = p^k$, this rewrites as $\overline{x}^{p^k} = \overline{x}$. In other words, $\overline{x^{p^k}} = \overline{x}$ (since $\overline{x^{p^k}} = \overline{x}^{p^k}$).

Theorem 5.5.2 **(c)** shows that the map

$$\begin{aligned} S[x]/f &\to F, \\ \overline{g} &\mapsto g[a] \end{aligned}$$

is a (well-defined) S-algebra morphism, and is injective. Applying this map to both sides of the equality $\overline{x^{p^k}} = \overline{x}$, we obtain $x^{p^k}[a] = x[a]$. In other words, $a^{p^k} = a$. This proves Proposition 5.5.5 **(b)**.

(c) Let f be the minimal polynomial of a. Let $k = \deg f$. We must show that $k \leq m$.

We have already shown (in the above proof of part **(b)**) that $|S[x]/f| = p^k$. Moreover, we have already shown (in the above proof of part **(b)**) that the map

$$\begin{aligned} S[x]/f &\to F, \\ \overline{g} &\mapsto g[a] \end{aligned}$$

is injective. Hence, $|S[x]/f| \leq |F|$ (because if U and V are two finite sets, and if there exists an injective map from U to V, then $|U| \leq |V|$). In view of $|S[x]/f| = p^k$, this rewrites as $p^k \leq |F|$. Hence, $p^k \leq |F| \leq p^m$, and therefore $k \leq m$ (since $p > 1$). This proves Proposition 5.5.5 **(c)**. □

Remark 5.5.6. Proposition 5.5.5 can be proved in many other ways. For example, part **(a)** can also be obtained from the pigeonhole principle (to wit: the principle shows that two of the $|F|+1$ elements $a^0, a^1, a^2, \ldots, a^{|F|}$ are equal; thus, a has an annihilating polynomial of the form $x^i - x^j$ for some $i > j \geq 0$). For parts **(b)** and **(c)**, it helps to look at the subset

$$A := \{g[a] \mid g \in S[x]\}$$

of F. This subset A is easily seen to be a subring of F, and thus a field (indeed, any subring of F is a finite integral domain and therefore a field). Moreover, it has size p^k (since the division-with-remainder theorem for polynomials shows that it is a free $\mathbb{Z}/p$-module with basis $\left(a^0, a^1, \ldots, a^{k-1}\right)$). Thus, $p^k = |A| \leq |F| \leq p^m$, so that $k \leq m$, and this yields part **(c)** of Proposition 5.5.5. Moreover, part **(b)** follows by applying Proposition 2.6.6 to A instead of F (since $a \in A$).

Exercise 5.5.4. Let p, S, F and a be as in Proposition 5.5.5.

Assume that the minimal polynomial of a has degree k. Prove that this minimal polynomial is

$$\left(x - a^{p^0}\right)\left(x - a^{p^1}\right)\cdots\left(x - a^{p^{k-1}}\right) = \prod_{i=0}^{k-1}\left(x - a^{p^i}\right).$$

[**Hint:** First prove that not only a, but all the k powers $a^{p^0}, a^{p^1}, \ldots, a^{p^{k-1}}$ are roots of the minimal polynomial. Then prove that these k powers are distinct. To do the latter, consider two integers i, j with $0 \leq i < j < k$. Then, show that the set

$$F_{i,j} := \left\{u \in F \mid u^{p^i} = u^{p^j}\right\}$$

is a subring of F (why?) and thus is a field (why?), but has size $\left|F_{i,j}\right| \leq p^j$ (why?). Now apply Proposition 5.5.5 **(c)** to $F_{i,j}$ and j instead of F and m to obtain a contradiction if $a \in F_{i,j}$.]

Lemma 5.5.7. Let p be a prime number. Let F be a finite field of characteristic p. Let m be the positive integer satisfying $|F| = p^m$. (We know from Theorem 5.2.2 **(e)** that this m exists.)

Then, there exists at least one $a \in F$ such that none of the $m-1$ powers $a^{p^1}, a^{p^2}, \ldots, a^{p^{m-1}}$ equals a.

Proof. Assume the contrary. Thus, each $a \in F$ satisfies at least one of the $m-1$ equations

$$a^{p^1} = a, \qquad a^{p^2} = a, \qquad \ldots, \qquad a^{p^{m-1}} = a.$$

In other words, each $a \in F$ is a root of the polynomial

$$\left(x^{p^1} - x\right)\left(x^{p^2} - x\right)\cdots\left(x^{p^{m-1}} - x\right) \in F[x].$$

But this polynomial has degree $p^1 + p^2 + \cdots + p^{m-1}$, and thus has at most $p^1 + p^2 + \cdots + p^{m-1}$ many roots (by Theorem 4.3.15). Hence, it has fewer than p^m roots (since it is easy to see that $p^1 + p^2 + \cdots + p^{m-1} = \dfrac{p^m - 1}{p-1} - 1 < \dfrac{p^m - 1}{p-1} \leq p^m - 1 < p^m$). However, we just found out that each $a \in F$ is a root of this polynomial; thus, this polynomial has at least p^m roots (since $|F| = p^m$). The preceding two sentences contradict each other. This contradiction shows that our assumption was wrong; hence, Lemma 5.5.7 is proved. □

5.5.3. Each finite field is obtained from $\mathbb{Z}/p$ by a single root adjunction

The above results lead to a first interesting property of finite fields:

Theorem 5.5.8. Let p be a prime number. Let S be the field $\mathbb{Z}/p$.

Let F be a finite field of characteristic p.

Let m be the positive integer satisfying $|F| = p^m$. (We know from Theorem 5.2.2 **(e)** that this m exists.)

Then, there exists at least one monic irreducible polynomial $f \in S[x] = (\mathbb{Z}/p)[x]$ of degree m that satisfies $F \cong S[x]/f$.

This theorem shows that any finite field can be constructed (up to isomorphism) by adjoining a (single) root of an irreducible polynomial to a field of the form $\mathbb{Z}/p$. It also shows that for any prime p and any positive integer m, there exists an irreducible polynomial of degree m over $\mathbb{Z}/p$ (because Theorem 5.4.1 says that there exists a finite field F of size $|F| = p^m$).

Proof of Theorem 5.5.8. Theorem 5.2.2 **(f)** shows that the field F contains "a copy of $\mathbb{Z}/p$" (that is, a subring isomorphic to $\mathbb{Z}/p$). By renaming the elements of F accordingly, we WLOG assume that this copy is $\mathbb{Z}/p$ itself, i.e., that $\mathbb{Z}/p$ is a subring of F. In other words, S is a subring of F (since $S = \mathbb{Z}/p$).

Lemma 5.5.7 shows that there exists at least one $a \in F$ such that none of the $m-1$ powers $a^{p^1}, a^{p^2}, \ldots, a^{p^{m-1}}$ equals a. Consider this a. Proposition 5.5.5 **(a)** shows that a has a minimal polynomial (over S). Let $f \in S[x]$ be this polynomial, and let $k = \deg f$ be its degree. Theorem 5.5.2 **(b)** shows that this minimal polynomial f is irreducible. Thus, f is not constant; hence, its degree k is positive. That is, we have $k \neq 0$.

Proposition 5.5.5 **(b)** shows that $a^{p^k} = a$; therefore, $k \notin \{1, 2, \ldots, m-1\}$ (since none of the $m-1$ powers $a^{p^1}, a^{p^2}, \ldots, a^{p^{m-1}}$ equals a). Combining this with $k \neq 0$, we thus obtain $k \notin \{0, 1, \ldots, m-1\}$, so that $k \geq m$. However, Proposition 5.5.5 **(c)** shows that $k \leq m$. Combined with $k \geq m$, this yields $k = m$. Thus, f has degree m (since f has degree $\deg f = k = m$).

It remains to show that $F \cong S[x]/f$ (as S-algebras).

As in the proof of Proposition 5.5.5 **(b)**, we can see that $|S[x]/f| = p^k$. In view of $k = m$, this rewrites as $|S[x]/f| = p^m$. Compared with $|F| = p^m$, this yields $|S[x]/f| = |F|$. Hence, $S[x]/f$ and F are two finite sets of the same size.

Theorem 5.5.2 **(c)** yields that the map

$$\begin{aligned} S[x]/f &\to F, \\ \overline{g} &\mapsto g[a] \end{aligned}$$

is a (well-defined) S-algebra morphism, and is injective. This map is thus an injective map between two finite sets of the same size (since $S[x]/f$ and F are two finite sets of the same size), and therefore is bijective (since the pigeonhole principle shows that any injective map between two finite sets of the same size is bijective). In other words, this map is invertible. Since it is an S-algebra morphism, it is thus an S-algebra isomorphism (by Proposition 3.11.8). Hence, $F \cong S[x]/f$ (as S-algebras). This completes the proof of Theorem 5.5.8. □

We also observe the following curious fact:

Theorem 5.5.9. Let p be a prime number. Let S be the field $\mathbb{Z}/p$.

Let m be a positive integer.

Then, any irreducible polynomial $f \in S[x]$ of degree m divides $x^{p^m} - x \in S[x]$.

Proof. Let $f \in S[x]$ be an irreducible polynomial of degree m. We must show that $f \mid x^{p^m} - x$ in $S[x]$.

The quotient ring $S[x]/f$ is a field (by Theorem 4.6.3, since f is irreducible). On the other hand, the leading coefficient of f is a unit (since S is a field, so that every nonzero element of S is a unit). Thus, as an S-module, $S[x]/f$ is free of rank $m = \deg f$ (by Theorem 4.5.9 **(b)**). Hence, $S[x]/f \cong S^m$ as an S-module. Thus, $|S[x]/f| = |S^m| = |S|^m = p^m$ (since $|S| = p$). Therefore, the field $S[x]/f$ is finite.

Now, let F be this finite field $S[x]/f$. Let a be the element $\overline{x} \in S[x]/f = F$. Then, Proposition 2.6.6 yields $a^{|F|} = a$. However, $F = S[x]/f$, so that $|F| = |S[x]/f| = p^m$. Hence,

$$\begin{aligned} a^{|F|} &= a^{p^m} = \overline{x}^{p^m} \qquad (\text{since } a = \overline{x}) \\ &= \overline{x^{p^m}}, \end{aligned}$$

so that $\overline{x^{p^m}} = a^{|F|} = a = \overline{x}$. In other words, $x^{p^m} - x \in fS[x]$. In other words, $f \mid x^{p^m} - x$ in $S[x]$. This proves Theorem 5.5.9. □

As a consequence of this theorem, we can show that Theorem 5.5.8 can be strengthened: Not only is there **some** monic irreducible polynomial $f \in S[x] = (\mathbb{Z}/p)[x]$ of degree m that satisfies $F \cong S[x]/f$, but actually **any** monic irreducible polynomial of this degree will do! Let us state this more carefully:

Corollary 5.5.10. Let p be a prime number. Let S be the field $\mathbb{Z}/p$.

Let m be a positive integer. Let F be a finite field of characteristic p such that $|F| = p^m$.

Let $f \in S[x]$ be a monic irreducible polynomial of degree m. Then, $F \cong S[x]/f$ (as S-algebras).

Proof. We have $\deg f = m > 0$. Hence, Theorem 5.3.7 **(b)** (applied to $b = f$) shows that there is a field that contains F as a subring and that contains a root of f. Let F' be this field, and let a be this root. Thus, $a \in F'$ and $f[a] = 0$.

Our first goal is to prove that a actually belongs to F.

Indeed, Theorem 5.5.9 shows that f divides $x^{p^m} - x$ in $S[x]$. Hence, a is a root of the polynomial $x^{p^m} - x$ (since a is a root of f). In other words, $a^{p^m} - a = 0$.

On the other hand, Proposition 2.6.6 yields that $u^{|F|} = u$ for each $u \in F$. In other words, $u^{p^m} = u$ for each $u \in F$ (since $|F| = p^m$). In other words, $u^{p^m} - u = 0$ holds for each $u \in F$. This equality $u^{p^m} - u = 0$ holds for $u = a$ as well (since $a^{p^m} - a = 0$). Thus, we conclude that $u^{p^m} - u = 0$ holds for each $u \in F \cup \{a\}$. In other words, each $u \in F \cup \{a\}$ is a root of the polynomial $x^{p^m} - x$. Therefore, the polynomial $x^{p^m} - x$ has at least $|F \cup \{a\}|$ many roots in F'. But this polynomial $x^{p^m} - x$ has degree p^m (since $p^m > 1$), and thus has at most p^m roots in F' (by Theorem 4.3.15, applied to F', p^m and $x^{p^m} - x$ instead of R, n and f). Confronting the preceding two sentences with each other, we obtain $|F \cup \{a\}| \leq p^m$. In view of $p^m = |F|$, this rewrites as $|F \cup \{a\}| \leq |F|$. Since F is a finite set, this inequality yields $a \in F$ (since otherwise, we would have $|F \cup \{a\}| = |F| + 1 > |F|$). Thus, we have shown that a belongs to F. We can now forget about F'.

We have $\deg f = m$, and the leading coefficient of f is a unit (since S is a field, so that every nonzero element of S is a unit). Thus, as an S-module, $S[x]/f$ is free of rank $\deg f = m$ (by Theorem 4.5.9 **(b)**). Hence, $S[x]/f \cong S^m$ as an S-module. Hence, $|S[x]/f| = |S^m| = |S|^m = p^m$ (since $|S| = p$). Comparing this with $|F| = p^m$, we obtain $|S[x]/f| = |F|$. In other words, $S[x]/f$ and F are two finite sets of the same size.

Theorem 5.2.2 **(f)** shows that the field F contains "a copy of $\mathbb{Z}/p$" (that is, a subring isomorphic to $\mathbb{Z}/p$). By renaming the elements of F accordingly, we WLOG assume that this copy is $\mathbb{Z}/p$ itself, i.e., that $\mathbb{Z}/p$ is a subring of F. In other words, S is a subring of F (since $S = \mathbb{Z}/p$).

The polynomial f is monic and irreducible, and satisfies $f[a] = 0$. Hence, Corollary 5.5.4 (applied to $g = f$) shows that f is the minimal polynomial of a (over S). Thus, Theorem 5.5.2 **(c)** yields that the map

$$\begin{aligned} S[x]/f &\to F, \\ \overline{g} &\mapsto g[a] \end{aligned}$$

is a (well-defined) S-algebra morphism, and is injective. This map is thus an injective map between two finite sets of the same size (since $S[x]/f$ and F are

two finite sets of the same size), and therefore is bijective (since the pigeonhole principle shows that any injective map between two finite sets of the same size is bijective). In other words, this map is invertible. Since it is an S-algebra morphism, it is thus an S-algebra isomorphism (by Proposition 3.11.8). Hence, $F \cong S[x]/f$ (as S-algebras). This proves Corollary 5.5.10. □

Exercise 5.5.5. Let p be a prime number. Let S be the field $\mathbb{Z}/p$.
Let m be a positive integer. Let $f \in S[x]$ be an irreducible polynomial.
Prove the following:

(a) If $\deg f \mid m$, then $f \mid x^{p^m} - x$ in $S[x]$.
(Note that this generalizes Theorem 5.5.9.)

(b) Conversely, if $f \mid x^{p^m} - x$ in $S[x]$, then $\deg f \mid m$.

Exercise 5.5.6. Let p be a prime number. Let S be the field $\mathbb{Z}/p$. Let m be a positive integer. Prove that the polynomial $x^{p^m} - x \in S[x]$ equals the product of all monic irreducible polynomials $f \in S[x]$ satisfying $\deg f \mid m$.
(For example, for $p = 2$ and $m = 3$, this yields

$$x^8 - x = \underbrace{x(x+1)}_{\substack{\text{irreducible}\\ \text{polynomials}\\ \text{of degree 1}}} \underbrace{\left(x^3+x+1\right)\left(x^3+x^2+1\right)}_{\substack{\text{irreducible}\\ \text{polynomials}\\ \text{of degree 3}}}$$

and

$$x^{16} - x = \underbrace{x(x+1)}_{\substack{\text{irreducible}\\ \text{polynomials}\\ \text{of degree 1}}} \underbrace{\left(x^2+x+1\right)}_{\substack{\text{irreducible}\\ \text{polynomials}\\ \text{of degree 2}}} \underbrace{\left(x^4+x+1\right)\left(x^4+x^3+1\right)\left(x^4+x^3+x^2+x+1\right)}_{\substack{\text{irreducible}\\ \text{polynomials}\\ \text{of degree 4}}}$$

in $(\mathbb{Z}/2)[x]$.)

[**Hint:** First argue that the factorization of $x^{p^m} - x$ into monic irreducible polynomials contains no factor more than once. Then use Exercise 5.5.5.]

5.5.4. Proof of the uniqueness

We can now easily prove the uniqueness of a finite field of given size (up to isomorphism):

Theorem 5.5.11. Any two finite fields that have the same size are isomorphic.

Proof. Let F and F' be two finite fields that have the same size. Thus, $|F| = |F'|$. Our goal is to prove that $F \cong F'$.

Let $p = \operatorname{char} F$. Then, Theorem 5.2.2 **(d)** shows that p is a prime. Also, Theorem 5.2.2 **(e)** shows that $|F| = p^m$ for some positive integer m. Consider this m. Comparing $|F| = p^m$ with $|F| = |F'|$, we find $|F'| = p^m$.

Let $q = \operatorname{char}(F')$. Then, Theorem 5.2.2 **(d)** shows that q is a prime. Also, Theorem 5.2.2 **(e)** shows that $|F'| = q^n$ for some positive integer n. Consider this n. Now, $p^m = |F| = |F'| = q^n$. Since p and q are primes (and m and n are positive integers), this can only happen if $p = q$ and $m = n$. Thus, we obtain $p = q$ and $m = n$. Hence, F' has characteristic p (since $p = q = \operatorname{char}(F')$).

Set $S = \mathbb{Z}/p$. Theorem 5.5.8 yields that there exists at least one monic irreducible polynomial $f \in S[x] = (\mathbb{Z}/p)[x]$ of degree m that satisfies $F \cong S[x]/f$. Consider this f. Recall that $|F'| = p^m$. Hence, Corollary 5.5.10 (applied to F' instead of F) yields that $F' \cong S[x]/f$ (as S-algebras). Combining this with $F \cong S[x]/f$, we obtain $F \cong S[x]/f \cong F'$. As we said, this proves Theorem 5.5.11. □

As we observed after Theorem 5.5.8, there exists an irreducible polynomial of any positive degree m over $\mathbb{Z}/p$ for any prime p. Explicitly finding such polynomials is not at all easy; I am not aware of any general method other than "try all the polynomials and check for irreducibility" (a finite algorithm, although a rather laborious one).[163] However, for specific degrees, there are better methods. In particular, for $m = p$, there is an explicit choice:

Exercise 5.5.7. Let p be a prime number. Let S be the field $\mathbb{Z}/p$. Let $a \in S$ be nonzero. Prove that the polynomial $x^p - x + a \in S[x]$ is irreducible.

[**Hint:** Assume that $x^p - x + a = fg$ for two non-units $f, g \in S[x]$. Argue that $\overline{x}^p = \overline{x} - a$ in the quotient ring $S[x]/f$. Use this to show that $\overline{x}^{p^i} = \overline{x} - ia$ for all $i \in \mathbb{N}$. On the other hand, let $k = \deg f \in \{1, 2, \ldots, p-1\}$, and argue that $\overline{x}^{p^k} = \overline{x}$ in $S[x]/f$. Can these formulas coexist?]

5.6. Lemmas on p-th powers

The following lemma will be used twice in the next section:

Lemma 5.6.1. Let p be a prime. Let F be a field such that $\mathbb{Z}/p$ is a subring of F. Then,

$$\{a \in F \mid a^p = a\} = \mathbb{Z}/p.$$

This lemma gives a criterion for showing that an element of F lies in $\mathbb{Z}/p$: namely, just show that $a^p = a$.

Proof of Lemma 5.6.1. For each $u \in \mathbb{Z}/p$, we have $u^p = u$ (by Proposition 2.6.4) and thus $u \in \{a \in F \mid a^p = a\}$. In other words, $\mathbb{Z}/p \subseteq \{a \in F \mid a^p = a\}$.

[163] A popular method for choosing these polynomials is known as "Conway polynomials".

Now, I claim that $|\{a \in F \mid a^p = a\}| \leq p$. Indeed, F is an integral domain. Thus, the easy half of the FTA (Theorem 4.3.15) yields that if n is a nonnegative integer, then any nonzero polynomial of degree $\leq n$ over F has at most n roots in F. Applying this to the polynomial $x^p - x$ (which is nonzero and has degree p), we conclude that the polynomial $x^p - x$ has at most p roots in F. But the set of all roots of this polynomial $x^p - x$ in F is $\{a \in F \mid a^p = a\}$; hence, the preceding sentence says that $|\{a \in F \mid a^p = a\}| \leq p$. Thus, in particular, the set $\{a \in F \mid a^p = a\}$ is finite.

However, an easy and fundamental fact in combinatorics says that if X and Y are two finite sets with $X \subseteq Y$ and $|Y| \leq |X|$, then $X = Y$. Applying this to $X = \mathbb{Z}/p$ and $Y = \{a \in F \mid a^p = a\}$, we obtain $\mathbb{Z}/p = \{a \in F \mid a^p = a\}$ (since $\mathbb{Z}/p \subseteq \{a \in F \mid a^p = a\}$ and $|\{a \in F \mid a^p = a\}| \leq p = |\mathbb{Z}/p|$). This proves Lemma 5.6.1. □

Exercise 5.6.1. Let p be a prime. Let F be a finite field of size p^m, where m is a positive integer. Assume that $\mathbb{Z}/p$ is a subring of F. Let $a \in F$.

(a) Let $r = p^0 + p^1 + \cdots + p^{m-1}$. Prove that $a^r \in \mathbb{Z}/p$.

(b) Let $b = a^{p^0} + a^{p^1} + \cdots + a^{p^{m-1}}$. Prove that $b \in \mathbb{Z}/p$.

Another useful lemma says (in terms of Subsection 5.3.3) that the Frobenius endomorphism of a field of characteristic p is always injective:

Lemma 5.6.2. Let p be a prime. Let F be a field of characteristic p. Let $a, b \in F$ satisfy $a \neq b$. Then, $a^p \neq b^p$.

Note that this would fail for $F = \mathbb{R}$ and $p = 2$ (because, for example, $1 \neq -1$ but $1^2 = (-1)^2$), and also fail for $F = \mathbb{C}$ and any $p > 1$. Thus, this marks one more of the situations where fields of prime characteristic p behave better than fields of characteristic 0.

Proof of Lemma 5.6.2. From $a \neq b$, we see that the element $a - b$ of F is nonzero. But F is a field, and thus an integral domain. Hence, it is easy to see (by induction on k) that any finite product $u_1 u_2 \cdots u_k$ of nonzero elements of F is nonzero. Thus, in particular, the product $\underbrace{(a-b)(a-b)\cdots(a-b)}_{p \text{ times}}$ is nonzero (since $a - b$ is nonzero). In other words, $(a-b)^p$ is nonzero.

However, Theorem 5.3.8 **(c)** yields $(a-b)^p = a^p - b^p$, so that $a^p - b^p = (a-b)^p \neq 0$ (since $(a-b)^p$ is nonzero). In other words, $a^p \neq b^p$. This proves Lemma 5.6.2. □

At this point, we end (at least for a while) our theoretical study of finite fields, and instead focus on some of their applications. The reader can learn more about finite fields from texts such as [LidNie00] and [MulMum07].

5.7. An application of root adjunction

What are finite fields (particularly the ones that are not just $\mathbb{Z}/p$) good for? Known applications include error-correcting codes (BCH codes), group theory (many finite simple groups can be constructed as matrix groups over finite fields), block designs (roughly speaking, finite structures with symmetries that resemble geometries) and, of course, number theory (not unexpectedly; number theory uses everything). Various applications along these lines can be found in [MulMum07]. Let me show a more humble – but also more self-contained – application. Namely, by adjoining roots of polynomials to $\mathbb{Z}/p$, we will prove a curious fact about Fibonacci numbers ([Vorobi02, §25]):

Theorem 5.7.1. Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence (as defined in Definition 2.3.4).

Let p be a prime. Then:

(a) If $p \equiv \pm 1 \bmod 5$ (meaning that p is congruent to one of 1 and -1 modulo 5), then $p \mid f_{p-1}$.

(b) If $p \equiv \pm 2 \bmod 5$ (meaning that p is congruent to one of 2 and -2 modulo 5), then $p \mid f_{p+1}$.

For example:

- For $p = 2$, Theorem 5.7.1 **(b)** says that $2 \mid f_3$ (since $2 \equiv 2 \bmod 5$), and indeed we have $f_3 = 2$.
- For $p = 7$, Theorem 5.7.1 **(b)** says that $7 \mid f_8$ (since $7 \equiv 2 \bmod 5$), and indeed we have $f_8 = 21 = 3 \cdot 7$.
- For $p = 11$, Theorem 5.7.1 **(a)** says that $11 \mid f_{10}$ (since $11 \equiv 1 \bmod 5$), and indeed we have $f_{10} = 55 = 5 \cdot 11$.

Our proof of Theorem 5.7.1 will be inspired by the famous **Binet formula** for Fibonacci numbers:

Theorem 5.7.2 (Binet formula for Fibonacci numbers)**.** Let

$$\varphi = \frac{1+\sqrt{5}}{2} \approx 1.618 \qquad \text{and} \qquad \psi = \frac{1-\sqrt{5}}{2} \approx -0.618$$

be the two roots of the quadratic polynomial $x^2 - x - 1$ in $\mathbb{R}$. Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence. Then,

$$f_n = \frac{1}{\sqrt{5}}\varphi^n - \frac{1}{\sqrt{5}}\psi^n \qquad \text{for each } n \in \mathbb{N}.$$

This is somewhat mysterious – why should irrational numbers like $\sqrt{5}$ appear in a formula for an integer sequence like $(f_0, f_1, f_2, \ldots)$? Proving Theorem 5.7.2 is an easy exercise in strong induction[164]. Finding it is trickier – the matrix approach from Exercise 2.3.6 can help here. Indeed, once you know that the matrix $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{R}^{2\times 2}$ satisfies $A^n = f_n A + f_{n-1} I_2$ for each n (this was proven in Exercise 2.3.6), you can boil down the computation of f_n to the computation of A^n. But there is a famous trick for computing powers of a matrix: namely, you diagonalize the matrix and take the powers of its diagonal entries[165]. This trick only works if the matrix is diagonalizable; but fortunately, our matrix A is diagonalizable, so we can compute A^n using this trick, ultimately obtaining Theorem 5.7.2 stated above. This demystifies the formula: $x^2 - x - 1$ is just the characteristic polynomial of the matrix A, and φ and ψ are its eigenvalues.

Anyway, how does this help us proving Theorem 5.7.1? The Binet formula involves irrational numbers and division; we thus cannot directly draw any conclusions about divisibility from it.

We can, however, use it as an inspiration. To wit, we shall introduce analogues of φ and ψ in "characteristic p". These should be roots of the same polynomial $x^2 - x - 1$, but regarded as a polynomial over $\mathbb{Z}/p$ instead of $\mathbb{R}$. Depending on p, this polynomial may or may not have roots in $\mathbb{Z}/p$, but we can always construct a splitting field in which it will have roots (see Theorem 5.3.7 **(c)**). Let us use this to attempt a proof of Theorem 5.7.1:

Proof of Theorem 5.7.1, part 1. First, we WLOG assume that $p \neq 5$ (since Theorem 5.7.1 makes no statement about $p = 5$). Hence, $p \nmid 5$ (since p is prime), so that $\overline{5} \neq \overline{0}$ in $\mathbb{Z}/p$. Furthermore, from $p \neq 5$, we obtain $5 \nmid p$ (since p is prime); thus, the remainder of p upon division by 5 must be 1, 2, 3 or 4. Therefore, p must satisfy one of the conditions $p \equiv \pm 1 \bmod 5$ and $p \equiv \pm 2 \bmod 5$.

Let F be a splitting field of the polynomial $x^2 - x - 1$ over $\mathbb{Z}/p$. (We know from Theorem 5.3.7 **(c)** that such an F exists, since the polynomial is monic.) Thus,

$$x^2 - x - 1 = (x - \varphi)(x - \psi) \qquad \text{for some } \varphi, \psi \in F.$$

Consider these φ, ψ. Comparing coefficients in front of the monomials x^1 and x^0 in the polynomial identity

$$x^2 - x - 1 = (x - \varphi)(x - \psi) = x^2 - (\varphi + \psi)\, x + \varphi\psi$$

yields[166]

$$-1 = -(\varphi + \psi) \qquad \text{and} \qquad -1 = \varphi\psi.$$

[164] See [Grinbe21, Proof of Theorem 2.3.1] for the proof in detail.

[165] Namely: If $A = QDQ^{-1}$, then $A^n = QD^nQ^{-1}$ for any $n \in \mathbb{N}$. If the matrix D is diagonal, then D^n is easily computed by taking its diagonal entries to the n-th powers; thus, A^n can be obtained as well.

[166] This is perhaps a good time to recall the warnings about evaluating polynomials over finite

(Of course, the "1" here stands for 1_F.) In other words,

$$\varphi + \psi = 1 \qquad \text{and} \qquad \varphi\psi = -1.$$

Define an element $\sqrt{5}$ of F by $\sqrt{5} = \varphi - \psi$. This is certainly a strange notation (this $\sqrt{5}$ is not the actual number $\sqrt{5}$ but just an analogue of it in our field F), but it is harmless (as we won't deal with the actual number $\sqrt{5}$ in this proof, but only with the element $\sqrt{5} = \varphi - \psi$ that we just introduced). Moreover, it is justified because

$$(\varphi - \psi)^2 = \varphi^2 - 2\varphi\psi + \psi^2 = \left(\underbrace{\varphi + \psi}_{=1}\right)^2 - 4\underbrace{\varphi\psi}_{=-1} = 1^2 - 4(-1) = \overline{5}.$$

As a consequence, $\left(\sqrt{5}\right)^2 = \overline{5} \neq \overline{0}$, so that $\sqrt{5} \neq \overline{0}$. Thus, $\sqrt{5}$ is a unit of F (since F is a field), so we can divide by $\sqrt{5}$.

Now, we claim that an analogue of the Binet formula holds in F: Namely, we have

$$\overline{f_n} = \frac{1}{\sqrt{5}}\varphi^n - \frac{1}{\sqrt{5}}\psi^n \qquad \text{for each } n \in \mathbb{N}. \tag{106}$$

This can be proved by the same strong induction argument as the original Binet formula (Theorem 5.7.2).

Now, we want to show that $p \mid f_{p-1}$ for some primes p and that $p \mid f_{p+1}$ for other primes p (remember: we have already gotten rid of the $p = 5$ case). In other words, we want to show that $\overline{f_{p-1}} = 0$ for some primes p, and that $\overline{f_{p+1}} = 0$ for other primes p. For now, let us ignore the question of which primes p satisfy which of these.

Here comes a trick that will look magical, but is actually an instance of a general method. We have $\varphi^2 - \varphi - 1 = 0$ (since φ is a root of the polynomial $x^2 - x - 1$), so that $\varphi^2 = \varphi + 1$. Taking this equality to the p-th power, we obtain

$$\begin{aligned} \varphi^{2p} &= (\varphi + 1)^p = \varphi^p + 1^p \qquad \text{(by Theorem 5.3.8 \textbf{(a)})} \\ &= \varphi^p + 1. \end{aligned}$$

In other words, $\varphi^{2p} - \varphi^p - 1 = 0$. Thus, φ^p is a root of the polynomial $x^2 - x - 1 = (x - \varphi)(x - \psi)$. In other words, $(\varphi^p - \varphi)(\varphi^p - \psi) = 0$. Since F is an integral domain, this entails $\varphi^p - \varphi = 0$ or $\varphi^p - \psi = 0$. In other words, $\varphi^p = \varphi$ or $\varphi^p = \psi$. In other words, $\varphi^p \in \{\varphi, \psi\}$. Similarly, $\psi^p \in \{\varphi, \psi\}$.

fields. Two polynomials f and g over a finite field F do not need to be identical just because their evaluations at all elements of F are identical (for example, the polynomials x^2 and x over $\mathbb{Z}/2$ are not identical, but their evaluations on both elements $\overline{0}$ and $\overline{1}$ of $\mathbb{Z}/2$ are identical). However, our two polynomials $x^2 - x - 1$ and $x^2 - (\varphi + \psi)x + \varphi\psi$ (whose coefficients we are comparing here) are known to be identical (not just their evaluations but the polynomials themselves); thus, we can compare their coefficients.

Moreover, $\varphi - \psi = \sqrt{5} \neq \overline{0}$, so that $\varphi \neq \psi$ and therefore $\varphi^p \neq \psi^p$ (by Lemma 5.6.2, since F has characteristic p). Combining this with $\varphi^p \in \{\varphi, \psi\}$ and $\psi^p \in \{\varphi, \psi\}$, we conclude that φ^p and ψ^p are two **distinct** elements of the set $\{\varphi, \psi\}$. Thus, $\{\varphi^p, \psi^p\} = \{\varphi, \psi\}$. So we are in one of the following two cases:

Case 1: We have $\varphi^p = \varphi$ and $\psi^p = \psi$.

Case 2: We have $\varphi^p = \psi$ and $\psi^p = \varphi$.

Let us consider Case 1. In this case, we have $\varphi^p = \varphi$ and $\psi^p = \psi$. Now, $\varphi \neq 0$ (since $\varphi^2 = \varphi + 1$ would turn into the absurd equality $0 = 1$ if φ was 0); thus, we can cancel φ from the equality $\varphi^p = \varphi$ (since F is a field). As a result, we obtain $\varphi^{p-1} = 1$. Similarly, $\psi^{p-1} = 1$. Now, (106) yields

$$\overline{f_{p-1}} = \frac{1}{\sqrt{5}} \underbrace{\varphi^{p-1}}_{=1} - \frac{1}{\sqrt{5}} \underbrace{\psi^{p-1}}_{=1} = \frac{1}{\sqrt{5}} \cdot 1 - \frac{1}{\sqrt{5}} \cdot 1 = 0.$$

Thus, we have shown that $\overline{f_{p-1}} = 0$ (that is, $p \mid f_{p-1}$) in Case 1.

Let us next consider Case 2. In this case, we have $\varphi^p = \psi$ and $\psi^p = \varphi$. Thus, $\varphi^{p+1} = \underbrace{\varphi^p}_{=\psi} \varphi = \psi\varphi = \varphi\psi = -1$ and similarly $\psi^{p+1} = -1$. Now, (106) yields

$$\overline{f_{p+1}} = \frac{1}{\sqrt{5}} \underbrace{\varphi^{p+1}}_{=-1} - \frac{1}{\sqrt{5}} \underbrace{\psi^{p+1}}_{=-1} = \frac{1}{\sqrt{5}} (-1) - \frac{1}{\sqrt{5}} (-1) = 0.$$

Thus, we have shown that $\overline{f_{p+1}} = 0$ (that is, $p \mid f_{p+1}$) in Case 2.

So we have shown that we always have $p \mid f_{p-1}$ or $p \mid f_{p+1}$. But why does the former hold for $p \equiv \pm 1 \bmod 5$ and the latter for $p \equiv \pm 2 \bmod 5$? In other words, why does our Case 1 correspond to $p \equiv \pm 1 \bmod 5$ and our Case 2 to $p \equiv \pm 2 \bmod 5$?

This will take some more work. We have the following chain of equivalences:

$$\begin{aligned}
&(\text{we are in Case 1}) \\
&\iff (\varphi^p = \varphi \text{ and } \psi^p = \psi) \\
&\iff (\varphi^p = \varphi) \qquad \left(\begin{array}{c} \text{because if } \varphi^p = \varphi, \\ \text{then } \psi^p \text{ cannot be } \varphi \text{ (since } \varphi^p \neq \psi^p\text{)} \\ \text{and thus must be } \psi \text{ (since } \psi^p \in \{\varphi, \psi\}\text{)} \end{array} \right) \\
&\iff (\varphi \in \{a \in F \mid a^p = a\}) \\
&\iff (\varphi \in \mathbb{Z}/p) \qquad (\text{by Lemma 5.6.1}) \\
&\iff \left(\text{the polynomial } x^2 - x - 1 \text{ has a root in } \mathbb{Z}/p\right). \qquad (107)
\end{aligned}$$

(In the last equivalence sign, the "$\Longrightarrow$" part is obvious (since φ is a root of $x^2 - x - 1$). The "$\Longleftarrow$" part can be proved as follows: If the polynomial $x^2 - x - 1$ has a root in $\mathbb{Z}/p$, then this root must be either φ or ψ (because $x^2 - x - 1 =$

$(x-\varphi)(x-\psi)$); however, in either of these cases, we obtain $\varphi \in \mathbb{Z}/p$ (because if $\psi \in \mathbb{Z}/p$, then $\varphi = \underbrace{(\varphi+\psi)}_{=1 \in \mathbb{Z}/p} - \underbrace{\psi}_{\in \mathbb{Z}/p} \in \mathbb{Z}/p$).)

Thus, our question is reduced to asking when the polynomial $x^2 - x - 1$ has a root in $\mathbb{Z}/p$. In other words, when can we find our φ and ψ in $\mathbb{Z}/p$, and when do we have to go into a larger field to find them?

We WLOG assume that $p \neq 2$ (since the case $p = 2$ is trivial to do by hand). Thus, $\overline{2} \in \mathbb{Z}/p$ is nonzero and thus has an inverse. This allows us to complete the square (just as in high school, but over the field $\mathbb{Z}/p$ now):

$$x^2 - x - 1 = \left(x - \frac{\overline{1}}{\overline{2}}\right)^2 - \frac{\overline{5}}{\overline{4}}. \tag{108}$$

Thus, the polynomial $x^2 - x - 1$ has a root in $\mathbb{Z}/p$ if and only if $\dfrac{\overline{5}}{\overline{4}}$ is a square in $\mathbb{Z}/p$. Obviously, $\dfrac{\overline{5}}{\overline{4}}$ is a square in $\mathbb{Z}/p$ if and only if $\overline{5}$ is a square in $\mathbb{Z}/p$ (since $\overline{4} = \overline{2}^2$ is always a square in $\mathbb{Z}/p$). Thus, in order to prove Theorem 5.7.1, it remains to prove the following: □

Theorem 5.7.3. Let p be a prime such that $p \neq 2$. Then:

(a) If $p \equiv \pm 1 \bmod 5$ (meaning that p is congruent to one of 1 and -1 modulo 5), then $\overline{5}$ is a square in $\mathbb{Z}/p$.

(b) If $p \equiv \pm 2 \bmod 5$ (meaning that p is congruent to one of 2 and -2 modulo 5), then $\overline{5}$ is not a square in $\mathbb{Z}/p$.

For example, $\overline{5} \in \mathbb{Z}/p$ is not a square for $p = 7$, but is a square for $p = 11$ (namely, $\overline{5} = \overline{4}^2$).

I will now prove Theorem 5.7.3; then, I will explain how it helps complete the above proof of Theorem 5.7.1, and afterwards (perhaps most interestingly) discuss how to generalize it to other numbers instead of 5.

Proof of Theorem 5.7.3. The following proof (due to Gauss) will again use field extensions. We WLOG assume that $p \neq 5$ (since Theorem 5.7.3 makes no claim about the case $p = 5$).

An element z of a field F is said to be a **primitive 5-th root of unity** if it satisfies $z^5 = 1$ but $z \neq 1$. In other words, the element z is a primitive 5-th root of unity if it is nonzero and its order in the group $F^\times$ (this is the group of units of F) is 5.

For example, $\mathbb{R}$ has no primitive 5-th roots of unity (since a real number z satisfying $z^5 = 1$ must necessarily satisfy $z = 1$), but $\mathbb{C}$ has four of them: namely, $e^{2\pi i k/5}$ for $k \in \{1,2,3,4\}$. (See `https://upload.wikimedia.org/wikipedia/`

`commons/4/40/One5Root.svg` for an illustration of the latter on the Argand diagram: The 5 blue points, which are the vertices of a regular pentagon, all satisfy $z^5 = 1$, and all but one of them are primitive 5-th roots of unity.)

Does $\mathbb{Z}/p$ have any primitive 5-th roots of unity? Sometimes yes (e.g., for $p = 11$); sometimes no (e.g., for $p = 7$). We don't care – we shall just adjoin one.

To see how, we notice the following: If F is a field of characteristic p, then a primitive 5-th root of unity in F is just an element $z \in F$ that satisfies $z^4 + z^3 + z^2 + z + 1 = 0$. [167] Knowing this, we can easily adjoin a primitive 5-th root of unity to $\mathbb{Z}/p$: Namely, $x^4 + x^3 + x^2 + x + 1 \in (\mathbb{Z}/p)[x]$ is a monic polynomial of degree 4 over $\mathbb{Z}/p$. Thus, by Theorem 5.3.7 **(b)**, there exists a field that contains $\mathbb{Z}/p$ as a subring and that contains a root of this polynomial. Let S be such a field, and let z be this root. Thus, $z \in S$ satisfies $z^4 + z^3 + z^2 + z + 1 = 0$, and therefore is a primitive 5-th root of unity (by what we have just said). That is, we have $z^5 = 1$ and $z \neq 1$.

Now comes the magic: Set $\tau = z - z^2 - z^3 + z^4 \in S$. Then,

$$\begin{aligned}
\tau^2 &= \left(z - z^2 - z^3 + z^4\right)^2 \\
&= z^2 + z^4 + z^6 + z^8 - 2zz^2 - 2zz^3 + 2zz^4 + 2z^2z^3 - 2z^2z^4 - 2z^3z^4 \\
&\qquad \text{(by expanding the square)} \\
&= z^2 + z^4 + z^6 + z^8 - 2z^3 - 2z^4 + 2z^5 + 2z^5 - 2z^6 - 2z^7 \\
&= z^2 + z^4 + z + z^3 - 2z^3 - 2z^4 + \overline{2} + \overline{2} - 2z - 2z^2 \\
&\qquad \left(\text{since } z^5 = 1 \text{ and thus } z^6 = z \text{ and } z^7 = z^2\right) \\
&= \overline{4} - \left(z + z^2 + z^3 + z^4\right) = \overline{5} - \underbrace{\left(z^4 + z^3 + z^2 + z + 1\right)}_{=0} = \overline{5}.
\end{aligned}$$

Thus, τ is a "square root" of $\overline{5}$ in S (meaning: an element of S whose square is $\overline{5}$). Hence, the only "square roots" of $\overline{5}$ in S are τ and $-\tau$ [168].

---

[167] *Proof.* If z is a primitive 5-th root of unity in F, then $z^5 = 1$ but $z \neq 1$, so that $\dfrac{z^5 - 1}{z - 1} = 0$ (since the numerator $z^5 - 1$ is 0 but the denominator $z - 1$ is nonzero), and therefore $z^4 + z^3 + z^2 + z + 1 = 0$ (since $z^4 + z^3 + z^2 + z + 1 = \dfrac{z^5 - 1}{z - 1}$).

Conversely, assume that $z^4 + z^3 + z^2 + z + 1 = 0$. Then, $z^5 - 1 = (z - 1)\underbrace{\left(z^4 + z^3 + z^2 + z + 1\right)}_{=0} = 0$, so that $z^5 = 1$. However, if we had $z = 1$, then we would have $z^4 + z^3 + z^2 + z + 1 = 1^4 + 1^3 + 1^2 + 1 + 1 = \overline{5} \neq \overline{0}$, which would contradict $z^4 + z^3 + z^2 + z + 1 = 0 = \overline{0}$. Hence, we must have $z \neq 1$. Thus we have shown that $z^5 = 1$ and $z \neq 1$; in other words, z is a primitive 5-th root of unity.

[168] This is a particular case of the following general fact: If R is an integral domain, and if $u, v \in R$ satisfy $u^2 = v$, then the only "square roots" of v in R are u and $-u$. (To check this, argue

This suggests that studying τ should help understand whether $\overline{5}$ is a square in $\mathbb{Z}/p$. Indeed, if τ belongs to $\mathbb{Z}/p$, then $\overline{5}$ is a square in $\mathbb{Z}/p$ (since $\tau^2 = \overline{5}$). Conversely (but less obviously), if τ does **not** belong to $\mathbb{Z}/p$, then $\overline{5}$ is not a square in $\mathbb{Z}/p$ (because the only "square roots" of $\overline{5}$ in S are τ and $-\tau$, and neither of them belongs to $\mathbb{Z}/p$ [169]). Now, how can we tell whether τ belongs to $\mathbb{Z}/p$?

Inspired by Lemma 5.6.1, we compute τ^p. From $\tau = z - z^2 - z^3 + z^4$, we obtain

$$\tau^p = \left(z - z^2 - z^3 + z^4\right)^p = z^p - z^{2p} - z^{3p} + z^{4p}$$

(by parts **(a)** and **(c)** of Theorem 5.3.8, applied several times). The right hand side of this can be greatly simplified if you know the remainder of p upon division by 5. Indeed, we have $z^5 = 1$, so that $z^6 = z$ and $z^7 = z^2$ and more generally $z^k = z^\ell$ for any two integers k and ℓ satisfying $k \equiv \ell \bmod 5$. Hence, in order to simplify the right hand side, we distinguish the following four cases:

Case 1: We have $p \equiv 1 \bmod 5$.

Case 2: We have $p \equiv 2 \bmod 5$.

Case 3: We have $p \equiv 3 \bmod 5$.

Case 4: We have $p \equiv 4 \bmod 5$.

(There is no Case 0, since $5 \nmid p$ entails $p \not\equiv 0 \bmod 5$.)

In Case 2, we have

$$\begin{aligned}\tau^p &= \underbrace{z^p}_{\substack{=z^2 \\ (\text{since } p \equiv 2 \bmod 5)}} - \underbrace{z^{2p}}_{\substack{=z^4 \\ (\text{since } 2p \equiv 4 \bmod 5)}} - \underbrace{z^{3p}}_{\substack{=z^1 \\ (\text{since } 3p \equiv 1 \bmod 5)}} + \underbrace{z^{4p}}_{\substack{=z^3 \\ (\text{since } 4p \equiv 3 \bmod 5)}} \\ &= z^2 - z^4 - z^1 + z^3 = \underbrace{-\left(z - z^2 - z^3 + z^4\right)}_{=\tau} = -\tau.\end{aligned}$$

Similarly, we get $\tau^p = -\tau$ in Case 3, and we get $\tau^p = \tau$ in Cases 1 and 4.

Thus, in Cases 1 and 4, we have $\tau^p = \tau$ and therefore $\tau \in \{a \in F \mid a^p = a\} = \mathbb{Z}/p$ (by Lemma 5.6.1), and thus $\overline{5}$ is a square in $\mathbb{Z}/p$ (since $\tau^2 = \overline{5}$). On the other hand, in Cases 2 and 3, we have $\tau^p = -\tau \neq \tau$ (since $2\tau \neq 0$ [170]) and therefore $\tau \notin \{a \in F \mid a^p = a\} = \mathbb{Z}/p$ (by Lemma 5.6.1), and thus $\overline{5}$ is not a square in $\mathbb{Z}/p$ (as explained above). This proves Theorem 5.7.3. □

The "magical" use of z (a primitive 5-th root of unity) to construct a square root of $\sqrt{5}$ is connected to the ubiquity of $\sqrt{5}$ in the geometry of regular pentagons. But it is not specific to the number 5: Gauss has shown that $\sqrt{p}$ can be

---

as follows: If w is a square root of v in R, then $(w-u)(w+u) = \underbrace{w^2}_{=v} - \underbrace{u^2}_{=v} = v - v = 0$, so that $w - u = 0$ or $w + u = 0$ (since R is an integral domain), so that $w = u$ or $w = -u$.)

[169] Indeed, from $\tau \notin \mathbb{Z}/p$, we obtain $-\tau \notin \mathbb{Z}/p$ (since otherwise, $\tau = -(-\tau)$ would yield $\tau \in \mathbb{Z}/p$).

[170] This can be shown as follows: From $\tau^2 = \overline{5} \neq 0$, we obtain $\tau \neq 0$. Moreover, $p \neq 2$ shows that $\overline{2} \neq 0$ in $\mathbb{Z}/p$. Now, F is an integral domain; hence, from $\overline{2} \neq 0$ and $\tau \neq 0$, we obtain $\overline{2}\tau \neq 0$. In other words, $2\tau \neq 0$.

similarly constructed from a primitive p-th root of unity for any prime $p > 2$. This will be explained in Theorem 5.8.12 **(c)** below.[171]

Next, let us use Theorem 5.7.3 to complete our above proof of Theorem 5.7.1:

Proof of Theorem 5.7.1, part 2. Recall the two Cases 1 and 2 that appeared in part 1 of this proof. We extend the equivalence (107) as follows:

$$\begin{aligned}
&\left(\text{we are in Case 1}\right) \\
&\iff \left(\text{the polynomial } x^2 - x - 1 \text{ has a root in } \mathbb{Z}/p\right) \\
&\iff \left(\text{the polynomial } \left(x - \frac{\overline{1}}{\overline{2}}\right)^2 - \frac{\overline{5}}{\overline{4}} \text{ has a root in } \mathbb{Z}/p\right) \\
&\qquad\qquad \left(\text{by (108)}\right) \\
&\iff \left(\frac{\overline{5}}{\overline{4}} \text{ is a square in } \mathbb{Z}/p\right) \\
&\iff \left(\overline{5} \text{ is a square in } \mathbb{Z}/p\right) \\
&\qquad\qquad \left(\text{since } \frac{\overline{5}}{\overline{4}} = a^2 \text{ is equivalent to } \overline{5} = (2a)^2\right) \\
&\iff \left(p \equiv \pm 1 \bmod 5\right) \qquad (109)
\end{aligned}$$

(by Theorem 5.7.3, since p must satisfy one of the conditions $p \equiv \pm 1 \bmod 5$ and $p \equiv \pm 2 \bmod 5$). But we have shown that if we are in Case 1, then $p \mid f_{p-1}$. Thus, we conclude using (109) that if $p \equiv \pm 1 \bmod 5$, then $p \mid f_{p-1}$. This proves Theorem 5.7.1 **(a)**. Likewise, if $p \equiv \pm 2 \bmod 5$, then we do **not** have $p \equiv \pm 1 \bmod 5$, so that we are **not** in Case 1 (by (109)), and thus we are in Case 2; hence, as we proved above, we must have $p \mid f_{p+1}$ in this case. Thus, Theorem 5.7.1 **(b)** is proved again. □

5.8. Quadratic residues: an introduction

5.8.1. Definitions and examples

We have touched upon an interesting subject, so let us delve deeper. Theorem 5.7.3 answers the question for which primes p the residue class $\overline{5} \in \mathbb{Z}/p$ is a square in $\mathbb{Z}/p$; but we can ask the same question about the residue class $\overline{a}$ of any $a \in \mathbb{Z}$.

[171] A reasonably elementary exposition of the connection between primitive p-th roots of unity and the square root $\sqrt{p}$ can be found in [Stein09, §4.4] (where it is only stated for the field $\mathbb{C}$, but most other fields can be handled similarly).

Just to whet your appetite a bit more: Recall that the equilateral triangle inscribed in the unit circle has sidelength $\sqrt{3}/2$. This is the $p = 3$ case of this connection.

Definition 5.8.1. Let p be a prime. Let a be an integer not divisible by p.

Then, a is said to be a **quadratic residue modulo** p (short: a **QR mod** p) if the residue class $\overline{a} \in \mathbb{Z}/p$ is a square (or, equivalently, if there is an integer b such that $a \equiv b^2 \bmod p$).

Otherwise, a is said to be a **quadratic nonresidue modulo** p (short: a **QNR mod** p).

For instance, if $p = 7$, then the three integers 1, 2 and 4 are QRs mod 7 (since $\overline{1} = \overline{1}^2$ and $\overline{2} = \overline{3}^2$ and $\overline{4} = \overline{2}^2$ in $\mathbb{Z}/7$), and therefore any integers that are congruent to any of these three integers modulo 7 are QRs mod 7 as well. The integers 3, 5 and 6 (and any integers congruent to them modulo 7) are QNRs mod 7. Integers divisible by 7 (such as 0) count neither as QRs nor as QNRs mod 7.

Definition 5.8.2. Let p be a prime. Let a be an integer. The **Legendre symbol** $\left(\frac{a}{p}\right)$ (do not mistake this for a fraction! this is not a fraction!) is the integer defined as follows:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{if } p \mid a; \\ 1, & \text{if } a \text{ is a QR mod } p; \\ -1, & \text{if } a \text{ is a QNR mod } p. \end{cases}$$

Note that the Legendre symbol $\left(\frac{a}{p}\right)$ depends only on the prime p and on the residue class $\overline{a} \in \mathbb{Z}/p$, but not on the integer a itself. In other words, if a prime $p \neq 2$ and two integers a and b satisfy $a \equiv b \bmod p$, then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \bmod p. \tag{110}$$

For example, $\left(\frac{-1}{p}\right) = \left(\frac{p-1}{p}\right)$ for any prime p. Here are some more examples of Legendre symbols:

- 2 is a QR mod 7, since $2 \equiv 3^2 \bmod 7$. Thus, $\left(\frac{2}{7}\right) = 1$.
- 2 is a QNR mod 5, since the squares in $\mathbb{Z}/5$ are $\overline{0}, \overline{1}, \overline{4}$. Thus, $\left(\frac{2}{5}\right) = -1$.
- -1 is a QR mod 5, since $-1 \equiv 2^2 \bmod 5$. Thus, $\left(\frac{-1}{5}\right) = 1$.
- -1 is a QNR mod 3. Thus, $\left(\frac{-1}{3}\right) = -1$.

- Theorem 5.7.3 says that every prime $p \neq 2$ satisfies

$$\left(\frac{5}{p}\right) = \begin{cases} 0, & \text{if } p = 5; \\ 1, & \text{if } p \equiv \pm 1 \bmod 5; \\ -1, & \text{if } p \equiv \pm 2 \bmod 5. \end{cases}$$

This might whet an appetite: can we find similarly simple expressions for $\left(\frac{2}{p}\right)$ or $\left(\frac{3}{p}\right)$ or $\left(\frac{-1}{p}\right)$? What can we say about Legendre symbols in general?

5.8.2. Counting squares

We begin by counting the squares in $\mathbb{Z}/p$:

Proposition 5.8.3. Let $p \neq 2$ be a prime. Then:

(a) The number of nonzero squares in $\mathbb{Z}/p$ is $(p-1)/2$.

(b) The number of squares in $\mathbb{Z}/p$ is $(p+1)/2$.

(c) The number of elements of $\mathbb{Z}/p$ that are not squares is $(p-1)/2$.

Proof. This is a particular case of something that was proved in the solution of Exercise 2.12.3 **(c)**; but let us show the proof here to keep this section self-contained:

(a) Given any element $v \in \mathbb{Z}/p$, we define a **square root** of v to be an element $u \in \mathbb{Z}/p$ that satisfies $u^2 = v$. It is easy to see that each nonzero square $v \in \mathbb{Z}/p$ has exactly two (distinct) square roots[172], and these two square roots are themselves nonzero (since $\overline{0}^2 = \overline{0}$). Thus, each nonzero square $v \in \mathbb{Z}/p$ has exactly two nonzero square roots.

[172] *Proof.* Let $v \in \mathbb{Z}/p$ be a nonzero square. Then, $v = c^2$ for some $c \in \mathbb{Z}/p$. Consider this c. Since $c^2 = v$ is nonzero, we see that c is nonzero. However, $\overline{2} \in \mathbb{Z}/p$ is also nonzero (since $p \neq 2$ is a prime), and thus $\overline{2} \cdot c \neq 0$ (since $\mathbb{Z}/p$ is an integral domain, and since $\overline{2}$ and c are nonzero). Thus, $c + c = 2 \underbrace{c}_{=1_{\mathbb{Z}/p} c} = \underbrace{2 \cdot 1_{\mathbb{Z}/p}}_{=\overline{2}} c = \overline{2} \cdot c \neq 0$. Subtracting c from both sides of this non-equality, we obtain $c \neq -c$.

Now, both c and $-c$ are square roots of v (since $c^2 = v$ and $(-c)^2 = c^2 = v$). Conversely, any square root d of v must be one of c and $-c$ (because it satisfies $d^2 = v$ and thus $(d-c)(d+c) = \underbrace{d^2}_{=v} - \underbrace{c^2}_{=v} = v - v = 0$, which entails (since $\mathbb{Z}/p$ is an integral domain) that $d - c$ or $d + c$ must be 0, which in turn means that d is either c or $-c$). This shows that c and $-c$ are the only square roots of v. Since $c \neq -c$, we thus conclude that v has exactly two square roots. Qed.

If $c \in \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}$, then $c \neq 0$ and thus $c^2 \neq 0$ (since $\mathbb{Z}/p$ is an integral domain), so that c^2 is a nonzero square. Hence, there is a map

$$\begin{aligned} \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} &\to \{\text{nonzero squares } v \in \mathbb{Z}/p\}, \\ c &\mapsto c^2. \end{aligned}$$

This map is a 2-to-1 correspondence (i.e., each element of the set $\{\text{nonzero squares } v \in \mathbb{Z}/p\}$ has exactly two preimages under this map), because each nonzero square $v \in \mathbb{Z}/p$ has exactly two nonzero square roots. Thus,

$$\left|\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}\right| = 2 \cdot \left|\{\text{nonzero squares } v \in \mathbb{Z}/p\}\right|.$$

Therefore,

$$\left|\{\text{nonzero squares } v \in \mathbb{Z}/p\}\right| = \frac{1}{2} \cdot \underbrace{\left|\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}\right|}_{=p-1} = \frac{1}{2} \cdot (p-1) = (p-1)/2.$$

This proves Proposition 5.8.3 **(a)**.

(b) The squares in $\mathbb{Z}/p$ are of two kinds: the zero squares and the nonzero squares. Of the former kind, there is only one (namely, $\overline{0}$, which is a square because $\overline{0} = \overline{0}^2$). Of the latter kind, there are $(p-1)/2$ (by Proposition 5.8.3 **(a)**). Thus, in total, there are $1 + (p-1)/2 = (p+1)/2$ squares in $\mathbb{Z}/p$. This proves Proposition 5.8.3 **(b)**.

(c) The ring $\mathbb{Z}/p$ has p elements, and exactly $(p+1)/2$ of them are squares (by Proposition 5.8.3 **(b)**). Hence, exactly $p - (p+1)/2 = (p-1)/2$ of its elements are not squares. This proves Proposition 5.8.3 **(c)**. □

5.8.3. Euler's QR criterion

Next, we will show a simple yet surprising rule, which was discovered by Euler:

Theorem 5.8.4 (Euler's QR criterion)**.** Let $p \neq 2$ be a prime. Let a be an integer. Then,

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p.$$

Proof. Since p is prime and satisfies $p \neq 2$, we see that p is odd and ≥ 3. Hence, $(p-1)/2$ is a positive integer. Thus, $0^{(p-1)/2} = 0$.

We must prove that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$. If $p \mid a$, then this boils down to showing that $0 \equiv 0 \bmod p$ (since $0^{(p-1)/2} = 0$). Thus, we WLOG assume that $p \nmid a$.

Let $u = \overline{a} \in \mathbb{Z}/p$; thus, u is nonzero (since $p \nmid a$). Hence, the definition of $\left(\frac{a}{p}\right)$ yields

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a QR mod } p; \\ -1, & \text{if } a \text{ is a QNR mod } p \end{cases} = \begin{cases} 1, & \text{if } u \text{ is a square;} \\ -1, & \text{if } u \text{ is not a square} \end{cases}$$

(by the definition of QRs and QNRs) and thus

$$\overline{\left(\frac{a}{p}\right)} = \begin{cases} \overline{1}, & \text{if } u \text{ is a square;} \\ \overline{-1}, & \text{if } u \text{ is not a square.} \end{cases} \tag{111}$$

Also,

$$\overline{a^{(p-1)/2}} = \overline{a}^{(p-1)/2} = u^{(p-1)/2} \tag{112}$$

(since $\overline{a} = u$). Now, we have the following chain of equivalences.

$$\begin{aligned} &\left(\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p\right) \qquad \text{(this is the claim we are proving)} \\ &\iff \left(\overline{\left(\frac{a}{p}\right)} = \overline{a^{(p-1)/2}}\right) \iff \left(\overline{a^{(p-1)/2}} = \overline{\left(\frac{a}{p}\right)}\right) \\ &\iff \left(u^{(p-1)/2} = \begin{cases} \overline{1}, & \text{if } u \text{ is a square;} \\ \overline{-1}, & \text{if } u \text{ is not a square} \end{cases}\right) \end{aligned}$$

(by (111) and (112)). Hence, it remains to prove that

- we have $u^{(p-1)/2} = \overline{1}$ if u is a square;
- we have $u^{(p-1)/2} = \overline{-1}$ if u is not a square.

Equivalently, we shall prove the following three claims:

> *Claim 1:* Any nonzero element $v \in \mathbb{Z}/p$ satisfies $v^{(p-1)/2} = \overline{1}$ or $v^{(p-1)/2} = \overline{-1}$.
>
> *Claim 2:* Any nonzero square $v \in \mathbb{Z}/p$ satisfies $v^{(p-1)/2} = \overline{1}$.
>
> *Claim 3:* Any element $v \in \mathbb{Z}/p$ that is not a square satisfies $v^{(p-1)/2} \neq \overline{1}$.

This will prove the two bullet points we claimed above: The first bullet point will follow from Claim 2, while the second will follow from Claims 1 and 3. So it remains to prove the three Claims 1, 2 and 3.

Proof of Claim 1. Let $v \in \mathbb{Z}/p$ be a nonzero element. Then, Proposition 2.6.4 (applied to v instead of u) yields $v^p = v$. We can cancel v from this equality (since v is nonzero and $\mathbb{Z}/p$ is a field), and thus obtain $v^{p-1} = 1$. Since $p-1$ is even, we have $\left(v^{(p-1)/2}\right)^2 = v^{p-1} = 1$, so that $\left(v^{(p-1)/2}\right)^2 - 1 = 0$. In view of $\left(v^{(p-1)/2}\right)^2 - 1 = \left(v^{(p-1)/2} - 1\right)\left(v^{(p-1)/2} + 1\right)$, this rewrites as $\left(v^{(p-1)/2} - 1\right)\left(v^{(p-1)/2} + 1\right) = 0$. Since $\mathbb{Z}/p$ is an integral domain, this entails $v^{(p-1)/2} - 1 = 0$ or $v^{(p-1)/2} + 1 = 0$. In other words, $v^{(p-1)/2} = \overline{1}$ or $v^{(p-1)/2} = \overline{-1}$. This proves Claim 1. □

Proof of Claim 2. Let $v \in \mathbb{Z}/p$ be a nonzero square. Thus, $v = w^2$ for some $w \in \mathbb{Z}/p$. Consider this w. Now, $w \neq 0$ (since $w^2 = v$ is nonzero). But Proposition 2.6.4 (applied to w instead of u) yields $w^p = w$. We can cancel w from this equality (since $w \neq 0$ and $\mathbb{Z}/p$ is a field), and thus obtain $w^{p-1} = 1$. Now, from $v = w^2$, we obtain $v^{(p-1)/2} = \left(w^2\right)^{(p-1)/2} = w^{p-1} = 1 = \overline{1}$. This proves Claim 2. □

Proof of Claim 3. Here we take a bird's eye view (as in our above proof of Lemma 5.6.1), rather than treating a single element v. Indeed, $\mathbb{Z}/p$ is an integral domain. Thus, the easy half of the FTA (Theorem 4.3.15) yields that if n is a nonnegative integer, then any nonzero polynomial of degree $\leq n$ over $\mathbb{Z}/p$ has at most n roots in $\mathbb{Z}/p$. Applying this to the polynomial $x^{(p-1)/2} - 1$ (which is nonzero and has degree $(p-1)/2$), we conclude that the polynomial $x^{(p-1)/2} - 1$ has at most $(p-1)/2$ roots in $\mathbb{Z}/p$. But the set of all roots of this polynomial $x^{(p-1)/2} - 1$ in $\mathbb{Z}/p$ is $\left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}$; hence, the preceding sentence says that $\left|\left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}\right| \leq (p-1)/2$.

On the other hand, $\{\text{nonzero squares } v \in \mathbb{Z}/p\} \subseteq \left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}$ (by Claim 2) and $|\{\text{nonzero squares } v \in \mathbb{Z}/p\}| = (p-1)/2$ (by Proposition 5.8.3 **(a)**).

However, an easy and fundamental fact in combinatorics says that if X and Y are two finite sets with $X \subseteq Y$ and $|Y| \leq |X|$, then $X = Y$. Applying this to $X = \{\text{nonzero squares } v \in \mathbb{Z}/p\}$ and $Y = \left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}$, we obtain

$$\{\text{nonzero squares } v \in \mathbb{Z}/p\} = \left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}$$

(since $\{\text{nonzero squares } v \in \mathbb{Z}/p\} \subseteq \left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}$ and $\left|\left\{v \in \mathbb{Z}/p \mid v^{(p-1)/2} = \overline{1}\right\}\right| \leq (p-1)/2 = |\{\text{nonzero squares } v \in \mathbb{Z}/p\}|$). Thus, every $v \in \mathbb{Z}/p$ satisfying $v^{(p-1)/2} = \overline{1}$ must be a nonzero square. By taking the contrapositive of this statement, we obtain Claim 3. □

Having proved Claims 1, 2 and 3, we thus have completed the proof of Theorem 5.8.4. □

We note that Theorem 5.8.4 has a generalization to squares in arbitrary finite fields:

Exercise 5.8.1. Let F be a finite field of size q, where q is odd. Let $u \in F$ be a nonzero element. Prove that:

(a) If u is a square in F (that is, if $u = v^2$ for some $v \in F$), then $u^{(q-1)/2} = 1$.

(b) If u is not a square in F, then $u^{(q-1)/2} = -1$.

5.8.4. The arithmetic of Legendre symbols

Euler's criterion has a surprising corollary:

Corollary 5.8.5 (Multiplicativity of the Legendre symbol)**.** Let $p \neq 2$ be a prime. Let $a, b \in \mathbb{Z}$. Then,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

To prove this, we will need the following near-trivial lemma (yes, we will; just wait):

Lemma 5.8.6. Let $p \neq 2$ be a prime. Let $u, v \in \{0, 1, -1\}$ be two integers satisfying $u \equiv v \bmod p$. Then, $u = v$.

Proof. We have $p > 2$ (since $p \neq 2$ and since p is a prime). Thus, neither 1 nor 2 nor -1 nor -2 is divisible by p. Therefore, the three integers $0, 1, -1$ are pairwise incongruent[173] modulo p. In other words, if two of them are congruent modulo p, then these two integers are just equal. Hence, from $u \equiv v \bmod p$, we obtain $u = v$ (since $u, v \in \{0, 1, -1\}$). This proves Lemma 5.8.6. □

Proof of Corollary 5.8.5. Theorem 5.8.4 yields

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} = a^{(p-1)/2} b^{(p-1)/2} \bmod p. \tag{113}$$

But Theorem 5.8.4 also yields $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \bmod p$ and $\left(\frac{b}{p}\right) \equiv b^{(p-1)/2} \bmod p$. Multiplying these two congruences, we obtain

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{(p-1)/2} b^{(p-1)/2} \bmod p.$$

[173] "Incongruent" means "not congruent".

Comparing this congruence with (113), we find

$$\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \bmod p. \tag{114}$$

But we want an equality, not a congruence! Luckily, the congruence (114) turns out to entail the equality. Indeed, both sides of the congruence (114) equal 0 or 1 or -1 (since any Legendre symbol is either 0 or 1 or -1, and the same holds for a product of Legendre symbols). Hence, their congruence implies their equality (by Lemma 5.8.6). This proves Corollary 5.8.5. □

Corollary 5.8.5 has two nice corollaries of its own:

Corollary 5.8.7. Let $p \neq 2$ be a prime. The map

$$\begin{aligned} (\mathbb{Z}/p)^\times &\to \{1,-1\}, \\ \overline{a} &\mapsto \left(\frac{a}{p}\right) \end{aligned}$$

is a group morphism (i.e., a homomorphism of groups).

Proof. The map is well-defined, since (as we have explained above) $\left(\frac{a}{p}\right)$ depends only on p and on $\overline{a} \in \mathbb{Z}/p$ (but not on a itself). Let us now show that this map is a group morphism.

In order to show that a map between two groups is a group morphism, it suffices to show that this map respects multiplication (this is well-known). Thus, it suffices to show that our map respects multiplication. In other words, it suffices to show that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for any $a, b \in \mathbb{Z}$ that are not divisible by p (since any two elements of the group $(\mathbb{Z}/p)^\times$ can be written in the forms $\overline{a}$ and $\overline{b}$ for two such $a, b \in \mathbb{Z}$, and then their product will be $\overline{ab}$). But this follows from Corollary 5.8.5. □

Corollary 5.8.8. Let $p \neq 2$ be a prime. Let $u, v \in \mathbb{Z}/p$ be two nonzero residue classes. Then:

(a) If u and v are squares, then uv is a square.

(b) If only one of u and v is a square, then uv is not a square.

(c) If none of u and v is a square, then uv is a square.

Note that Corollary 5.8.8 **(c)** would fail if we replaced $\mathbb{Z}/p$ by $\mathbb{Q}$. For example, none of the rational numbers 2 and 3 is a square, but neither is $2 \cdot 3$. But it

does hold in $\mathbb{Z}/p$ (as we shall now show), and (more generally) in finite fields, as well as in $\mathbb{R}$ (since the non-squares in $\mathbb{R}$ are precisely the negative reals, but a product of two negative reals is always positive).

Proof of Corollary 5.8.8. We shall only prove part **(c)**, for two reasons: First of all, parts **(a)** and **(b)** hold for any field (unlike part **(c)**, as we just discussed), and can easily be proved using nothing but the field axioms. Also, the proof we will give for part **(c)** can easily be adapted to the other two parts.

(c) Assume that none of u and v is a square. Write u and v in the form $u = \overline{a}$ and $v = \overline{b}$ for some integers a and b. Then, a is a QNR mod p (since $\overline{a} = u$ is not a square and thus nonzero), and thus $\left(\frac{a}{p}\right) = -1$ (by the definition of the Legendre symbol). Similarly, $\left(\frac{b}{p}\right) = -1$. Hence, Corollary 5.8.5 yields $\left(\frac{ab}{p}\right) = \underbrace{\left(\frac{a}{p}\right)}_{=-1}\underbrace{\left(\frac{b}{p}\right)}_{=-1} = (-1)(-1) = 1$. In other words, ab is a QR mod p (by the definition of the Legendre symbol). In other words, $\overline{ab}$ is nonzero and a square. In view of $\overline{ab} = \overline{a} \cdot \overline{b} = uv$ (since $\overline{a} = u$ and $\overline{b} = v$), this yields that uv is a square. Thus, Corollary 5.8.8 **(c)** is proven. □

Exercise 5.8.2. Let F be a finite field. Prove that the polynomial $x^4 + 1 \in F[x]$ is not irreducible.

[**Hint:** It suffices to consider the case $F = \mathbb{Z}/p$ for a prime p. In this case, assume further that $p \neq 2$, since the $p = 2$ case is easily done by hand. Use Corollary 5.8.8 **(c)** to show that at least one of the residue classes $\overline{-1}$, $\overline{2}$ and $\overline{-2}$ is a square in $\mathbb{Z}/p$. In each of these cases, factor $x^4 + 1$.]

5.8.5. When -1 is a QR

Let us now return to the computation of Legendre symbols. Thanks to Corollary 5.8.5, we have (for example) $\left(\frac{6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$ and $\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$ for any prime p. But how do we compute $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ and $\left(\frac{3}{p}\right)$?

We begin with $\left(\frac{-1}{p}\right)$, which is probably the easiest one:

Theorem 5.8.9. Let $p \neq 2$ be a prime. Then, -1 is a QR mod p (that is, $\overline{-1} \in \mathbb{Z}/p$ is a square) if and only if $p \equiv 1 \bmod 4$. In other words,

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4; \\ -1, & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

Proof. Since p is a prime satisfying $p \neq 2$, the number p is odd. Hence, $(p-1)/2 \in \mathbb{Z}$.

Theorem 5.8.4 yields the congruence

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} \bmod p.$$

Lemma 5.8.6 shows that this congruence must actually be an equality, since both of its sides are 0 or 1 or -1. In other words,

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}. \tag{115}$$

Now, p must satisfy $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$ (since p is odd). In the former case, $(-1)^{(p-1)/2}$ is 1; in the latter, -1. Hence, (115) can be rewritten as

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4; \\ -1, & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

□

Theorem 5.8.9 has some unexpected applications. For instance, it can be used to prove a strengthening of Euclid's famous result that there are infinitely many prime numbers:

Exercise 5.8.3. The **Fermat numbers** are the positive integers $F_0, F_1, F_2, \ldots$ defined by

$$F_n := 2^{2^n} + 1 \qquad \text{for each } n \in \mathbb{N}.$$

(a) Prove that $\gcd\left(F_i, F_j\right) = 1$ for all $i \neq j$.

(b) Prove that every prime p that divides some Fermat number F_n with $n \geq 1$ must satisfy $p \equiv 1 \bmod 4$.

(c) Conclude that there are infinitely many prime numbers p satisfying $p \equiv 1 \bmod 4$.

More generally, **Dirichlet's theorem on prime numbers in arithmetic progressions** says that whenever u and v are two coprime integers satisfying $u > 0$, then there are infinitely many prime numbers p satisfying $p \equiv v \bmod u$. However, this is far harder to prove; all known proofs require analysis (see, e.g., [Klazar10a, Chapter 1] and [Klazar10b, Chapter 2]).

5.8.6. Quadratic reciprocity

So we have simple formulas for $\left(\frac{-1}{p}\right)$ and $\left(\frac{5}{p}\right)$. What about $\left(\frac{a}{p}\right)$ for a general a ? We only need to know a formula for $\left(\frac{q}{p}\right)$ for each prime q (because,

as per Corollary 5.8.5 above, we can then get a general formula for $\left(\frac{a}{p}\right)$ by decomposing a into a product of primes and possibly -1, and multiplying). Here is one:

Theorem 5.8.10 (Quadratic Reciprocity Law)**.**

(a) Let $p \neq 2$ be a prime. Then,

$$\left(\frac{2}{p}\right) = (-1)^{\left(p^2-1\right)/8} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \bmod 8; \\ -1, & \text{if } p \equiv \pm 3 \bmod 8. \end{cases}$$

(b) Let p and q be two distinct primes distinct from 2. Then,

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right).$$

For example, if $p \neq 2$ is any prime distinct from 5, then Theorem 5.8.10 **(b)** (applied to $q = 5$) yields

$$\left(\frac{5}{p}\right) = \underbrace{(-1)^{(p-1)(5-1)/4}}_{\substack{=1 \\ \text{(since } 5-1=4 \text{ and thus} \\ (p-1)(5-1)/4 = p-1 \text{ is even)}}} \left(\frac{p}{5}\right) = \left(\frac{p}{5}\right)$$

$$= \begin{cases} 1, & \text{if } \overline{p} \in \mathbb{Z}/5 \text{ is a square;} \\ -1, & \text{if } \overline{p} \in \mathbb{Z}/5 \text{ is not a square} \end{cases} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \bmod 5; \\ -1, & \text{if } p \equiv \pm 2 \bmod 5 \end{cases}$$

(the last equality follows from the fact that the nonzero squares in $\mathbb{Z}/5$ are $\overline{1}$ and $\overline{-1}$); this recovers the claim of Theorem 5.7.3. So Theorem 5.7.3 was merely the tip of an iceberg.

Theorem 5.8.10 is known as the **law of quadratic reciprocity**[174], and is one of the most classical theorems in mathematics – discovered by Euler, proved by Gauss. By now, it has received over 250 proofs (see `https://www.mathi.uni-heidelberg.de/~flemmermeyer/qrg_proofs.html` for a list), and new proofs keep getting published. You'll get to prove its part **(a)** in the following exercise, inspired by the $q = 5$ case we proved above:

Exercise 5.8.4. Let p be an odd prime. Let ζ be a root of the polynomial $x^4 + 1 \in (\mathbb{Z}/p)[x]$ in a commutative $\mathbb{Z}/p$-algebra A. Thus, $\zeta^4 = -1$, so that ζ is a unit (with inverse $-\zeta^3$). Let $\tau \in A$ be defined by $\tau = \zeta + \zeta^{-1}$. Prove the following:

[174] Some authors refer only to Theorem 5.8.10 **(b)** as the law of quadratic reciprocity; they correspondingly call Theorem 5.8.10 **(a)** the "second supplementary law of quadratic reciprocity". (The name "first supplementary law" then refers to Theorem 5.8.9.)

(a) We have $\tau^2 = 2$. (Here, 2 stands for $2 \cdot 1_A \in A$.)

(b) We have $\tau^p = \left(\frac{2}{p}\right) \tau$, where $\left(\frac{2}{p}\right)$ means a Legendre symbol.

(c) If $p \equiv \pm 1 \bmod 8$ (that is, if p is congruent to 1 or to -1 modulo 8), then $\tau^p = \tau$.

(d) If $p \equiv \pm 3 \bmod 8$ (that is, if p is congruent to 3 or to -3 modulo 8), then $\tau^p = -\tau$.

(e) Prove Theorem 5.8.10 **(a)**.

[**Hint:** For part **(b)**, start out by writing $\tau^p = \left(\tau^2\right)^{(p-1)/2} \tau$.]

Hopefully, Exercise 5.8.4 sheds some light on the strange definition of τ.

The rest of this section will be devoted to proving Theorem 5.8.10 **(b)**. Before we embark on the actual proof, we shall show a few auxiliary results, which are themselves of some interest.

5.8.7. A sum of Legendre symbols

The first auxiliary result is a classical formula for a certain sum of Legendre symbols:

Proposition 5.8.11. Let $p \neq 2$ be a prime. Let $k \in \mathbb{Z}$. Then:

(a) If $p \mid k$, then $\sum_{i=0}^{p-1} \left(\frac{i(i-k)}{p}\right) = p - 1$.

(b) If $p \nmid k$, then $\sum_{i=0}^{p-1} \left(\frac{i(i-k)}{p}\right) = -1$.

Proof. We first observe that $\left(\frac{0(0-k)}{p}\right) = \left(\frac{0}{p}\right) = 0$ (since $p \mid 0$). In other words, the $i = 0$ addend of the sum $\sum_{i=0}^{p-1} \left(\frac{i(i-k)}{p}\right)$ is 0. Hence, we can remove this addend from the sum, and obtain

$$\sum_{i=0}^{p-1} \left(\frac{i(i-k)}{p}\right) = \sum_{i=1}^{p-1} \left(\frac{i(i-k)}{p}\right). \tag{116}$$

We also note that p is odd (since $p \neq 2$ is a prime), and thus $(p-1)/2 \in \mathbb{N}$.

(a) Assume that $p \mid k$. Then, $k \equiv 0 \bmod p$, so that $\overline{k} = \overline{0}$ in $\mathbb{Z}/p$.

Let $i \in \{1,2,\ldots,p-1\}$. Then, $p \nmid i$, so that $\overline{i} \neq 0$ in $\mathbb{Z}/p$. Hence, $\overline{i}^2 \neq 0$ in $\mathbb{Z}/p$ as well (since $\mathbb{Z}/p$ is an integral domain). However, in $\mathbb{Z}/p$, we have

$$\overline{i\,(i-k)} = \overline{i}\left(\overline{i} - \underbrace{\overline{k}}_{=\overline{0}}\right) = \overline{i}\left(\overline{i} - \overline{0}\right) = \overline{i}^2 \neq 0,$$

so that $i\,(i-k)$ is not divisible by p. Furthermore, the element $\overline{i\,(i-k)}$ of $\mathbb{Z}/p$ is a square (since $\overline{i\,(i-k)} = \overline{i}^2$), so that $i\,(i-k)$ is a QR mod p (since $i\,(i-k)$ is not divisible by p). Therefore, $\left(\dfrac{i\,(i-k)}{p}\right) = 1$.

Forget that we fixed i. We thus have proved the equality $\left(\dfrac{i\,(i-k)}{p}\right) = 1$ for each $i \in \{1,2,\ldots,p-1\}$. Summing this equality over all $i \in \{1,2,\ldots,p-1\}$, we obtain $\sum\limits_{i=1}^{p-1}\left(\dfrac{i\,(i-k)}{p}\right) = \sum\limits_{i=1}^{p-1} 1 = p-1$. Hence, (116) can be rewritten as $\sum\limits_{i=0}^{p-1}\left(\dfrac{i\,(i-k)}{p}\right) = p-1$. This proves Proposition 5.8.11 **(a)**.

(b) Assume that $p \nmid k$. We consider the polynomial

$$f := (x\,(x-k))^{(p-1)/2} - x^{p-1} \in \mathbb{Z}\,[x]$$

(this is well-defined, since $(p-1)/2 \in \mathbb{N}$). We claim that this polynomial f has degree $\leq p-2$. Indeed, f is the difference of the two polynomials $(x\,(x-k))^{(p-1)/2}$ and x^{p-1}, both of which have degree $p-1$ and leading coefficient 1 (this is obvious for x^{p-1}, and for $(x\,(x-k))^{(p-1)/2}$ it follows from Proposition 4.3.5 **(d)**[175]). When we subtract these two polynomials, the leading terms cancel out (since the leading coefficients are equal), and thus we are left with a polynomial of degree $\leq p-2$. In other words, the polynomial f has degree $\leq p-2$.

Hence, Corollary 4.3.21 yields $\sum\limits_{j=0}^{p-1} f(j) \equiv 0 \bmod p$. In other words,

$$\sum_{j=0}^{p-1}\left((j\,(j-k))^{(p-1)/2} - j^{p-1}\right) \equiv 0 \bmod p$$

[175] In more detail: An easy consequence of Proposition 4.3.5 **(d)** is that if g is a monic polynomial of degree i, then g^m is a monic polynomial of degree mi for each $m \in \mathbb{N}$. Applying this to $g = x\,(x-k)$ and $i = 2$ and $m = (p-1)/2$, we conclude that $(x\,(x-k))^{(p-1)/2}$ is a monic polynomial of degree $(p-1)/2 \cdot 2 = p-1$. In other words, $(x\,(x-k))^{(p-1)/2}$ is a polynomial with degree $p-1$ and leading coefficient 1.

(since the definition of f yields $f(j) = (j(j-k))^{(p-1)/2} - j^{p-1}$ for each $j \in \mathbb{Z}$). In other words,

$$\sum_{j=0}^{p-1} (j(j-k))^{(p-1)/2} - \sum_{j=0}^{p-1} j^{p-1} \equiv 0 \bmod p.$$

Hence,

$$\sum_{j=0}^{p-1} (j(j-k))^{(p-1)/2} \equiv \sum_{j=0}^{p-1} j^{p-1} = \underbrace{0^{p-1}}_{\substack{=0 \\ \text{(since } p-1>0\text{)}}} + \sum_{j=1}^{p-1} \underbrace{j^{p-1}}_{\substack{\equiv 1 \bmod p \\ \text{(by Corollary 2.6.5,} \\ \text{since } p \nmid j\text{)}}}$$

$$\equiv 0 + \sum_{j=1}^{p-1} 1 = p - 1 \equiv -1 \bmod p.$$

Now,

$$\sum_{i=0}^{p-1} \underbrace{\left(\frac{i(i-k)}{p}\right)}_{\substack{\equiv (i(i-k))^{(p-1)/2} \bmod p \\ \text{(by Theorem 5.8.4,} \\ \text{applied to } a = i(i-k)\text{)}}} \equiv \sum_{i=0}^{p-1} (i(i-k))^{(p-1)/2} = \sum_{j=0}^{p-1} (j(j-k))^{(p-1)/2}$$

$$\equiv -1 \bmod p. \tag{117}$$

This is very close to the thing we want to prove, but we are not quite there yet: We want to prove that the two sides of (117) are identical, not just congruent modulo p. Thus, we need an extra argument. Let $s := \sum_{i=0}^{p-1} \left(\frac{i(i-k)}{p}\right)$. This s is a sum of p Legendre symbols, each of which is either 0 or 1 or -1 (since any Legendre symbol is either 0 or 1 or -1). Hence, s is an integer between $-p$ and p (inclusive). However, we can show something slightly better: We can show that s is an integer between $-(p-2)$ and $p-2$.

In order to show this, we let ℓ be the remainder obtained when dividing k by p. Then, $\ell \in \{0, 1, \ldots, p-1\}$ and $\ell \neq 0$ (since $p \nmid k$) and $\ell \equiv k \bmod p$. Hence, $\ell - k$ is divisible by p, so that $\ell(\ell - k)$ is divisible by p. Thus, $\left(\frac{\ell(\ell-k)}{p}\right) = 0$ by Definition 5.8.2.

Now, the sum

$$s = \sum_{i=0}^{p-1} \left(\frac{i(i-k)}{p}\right) \tag{118}$$

has at least two addends that equal 0: namely, the $i = 0$ addend (which is $\left(\frac{0(0-k)}{p}\right) = 0$) and the $i = \ell$ addend (which is $\left(\frac{\ell(\ell-k)}{p}\right) = 0$). These are

two distinct addends (since $\ell \neq 0$). The remaining $p-2$ addends in the sum s are Legendre symbols, so each of them is either 0 or 1 or -1. Hence, the entire sum s is an integer between $-(p-2)$ and $p-2$ (inclusive).

We have now encircled s from all sides: On the one hand, we know that $s = \sum_{i=0}^{p-1} \left(\frac{i(i-k)}{p} \right) \equiv -1 \bmod p$ (by (117)), so that s is congruent to -1 modulo p. On the other hand, we know that s is an integer between $-(p-2)$ and $p-2$ (inclusive). However, the only integer between $-(p-2)$ and $p-2$ that is congruent to -1 modulo p is the integer -1 itself (since $p-1$ is too large, while $-p-1$ is too small). Thus, s must be -1. In other words, $\sum_{i=0}^{p-1} \left(\frac{i(i-k)}{p} \right)$ must be -1 (by (118)). This proves Proposition 5.8.11 **(b)**. □

The following exercise (a result of Jacobsthal from 1907, see [Jacobs07]) generalizes Proposition 5.8.11:

Exercise 5.8.5. Let $p \neq 2$ be a prime. Let $a, b \in \mathbb{Z}$. Prove that

$$\sum_{i=0}^{p-1} \left(\frac{i^2 + ai + b}{p} \right) = \begin{cases} p-1, & \text{if } a^2 \equiv 4b \bmod p; \\ -1, & \text{else.} \end{cases}$$

5.8.8. Gaussian sums

In our above proof of Theorem 5.7.3, we did some seemingly unmotivated things: We adjoined an element z satisfying $z^4 + z^3 + z^2 + z + 1 = 0$ to our field (which was $\mathbb{Z}/p$, but this is not important); then, we defined $\tau = z - z^2 - z^3 + z^4$; then, we showed (by computation) that $\tau^2 = \overline{5}$.

This element τ was not chosen at random; its definition can be rewritten using Legendre symbols as

$$\tau = \sum_{i=0}^{4} \left(\frac{i}{5} \right) z^i$$

(since $\sum_{i=0}^{4} \left(\frac{i}{5} \right) z^i = \underbrace{\left(\frac{0}{5} \right)}_{=0} z^0 + \underbrace{\left(\frac{1}{5} \right)}_{=1} z^1 + \underbrace{\left(\frac{2}{5} \right)}_{=-1} z^2 + \underbrace{\left(\frac{3}{5} \right)}_{=-1} z^3 + \underbrace{\left(\frac{4}{5} \right)}_{=1} z^4 = 0z^0 + 1z^1 + (-1)z^2 + (-1)z^3 + 1z^4 = z - z^2 - z^3 + z^4$). This suggests a generalization: Replacing 5 by an arbitrary prime $p \neq 2$, we can adjoin an element z satisfying $z^{p-1} + z^{p-2} + \cdots + z^0 = 0$ to our field (which, as we said, can be arbitrary), and define an element $\tau = \sum_{i=0}^{p-1} \left(\frac{i}{p} \right) z^i$. The square τ^2 of this element will then be $\overline{(-1)^{(p-1)/2} p}$ instead of $\overline{5}$. This was found by Gauss, and we shall prove this as part of the following theorem:

Theorem 5.8.12 (square of the Gaussian sum)**.** Let p be a prime. Let A be a commutative ring. Let $z \in A$ be an element satisfying

$$z^{p-1} + z^{p-2} + \cdots + z^0 = 0. \tag{119}$$

Then:

(a) We have $z^p = 1_A$.

(b) If $u, v \in \mathbb{N}$ satisfy $u \equiv v \bmod p$, then $z^u = z^v$.

(c) Assume that $p \neq 2$. Define an element $\tau \in A$ by

$$\tau = \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) z^i.$$

Then,

$$\tau^2 = (-1)^{(p-1)/2}\, p \cdot 1_A.$$

The τ defined in Theorem 5.8.12 **(c)** is known as a **Gaussian sum**. The best-known particular case of Theorem 5.8.12 is when $A = \mathbb{C}$ and $z = e^{2\pi i/p} = \cos\dfrac{2\pi}{p} + i\sin\dfrac{2\pi}{p}$; in this case, the claim of Theorem 5.8.12 **(c)** is saying that $\tau^2 = (-1)^{(p-1)/2}\, p$. This implies that $\tau = \pm\sqrt{(-1)^{(p-1)/2}\, p}$ in this case, and one can wonder whether the $\pm$ sign is a $+$ or a $-$. This question has been answered (the sign is always a $+$ sign), but the proof is tricky and would take us further afield than I'd like. You can find it in [Elman22, Theorem G.2]. To us, this question is not important, since it only concerns the case $A = \mathbb{C}$, whereas we will apply Theorem 5.8.12 to a different ring A.

Proof of Theorem 5.8.12. **(a)** Multiplying both sides of the equality (119) by z, we obtain $z \cdot \left(z^{p-1} + z^{p-2} + \cdots + z^0\right) = 0$. In other words,

$$z^p + z^{p-1} + \cdots + z^1 = 0.$$

Subtracting this equality from the original equality (119) (and cancelling all the addends that appear in both), we obtain $z^0 - z^p = 0$. In other words, $z^0 = z^p$. Hence, $z^p = z^0 = 1_A$. This proves Theorem 5.8.12 **(a)**.

(b) Let $u, v \in \mathbb{N}$ satisfy $u \equiv v \bmod p$. We must prove that $z^u = z^v$.

We WLOG assume that $u \geq v$ (otherwise, swap u with v). Thus, $u - v \in \mathbb{N}$. Since $u \equiv v \bmod p$, we also have $p \mid u - v$, so that $\dfrac{u-v}{p} \in \mathbb{Z}$ and therefore $\dfrac{u-v}{p} \in \mathbb{N}$ (since $u - v \in \mathbb{N}$). Let us denote this number $\dfrac{u-v}{p}$ by m. Thus,

$m = \dfrac{u-v}{p} \in \mathbb{N}$. Also, solving the equation $m = \dfrac{u-v}{p}$ for u, we find $u = mp + v$. Hence, $z^u = z^{mp+v} = \left(z^p\right)^m z^v$. However, Theorem 5.8.12 **(a)** yields $z^p = 1_A$. Thus, $\left(z^p\right)^m = 1_A^m = 1_A$ and therefore $z^u = \underbrace{\left(z^p\right)^m}_{=1_A} z^v = z^v$. Thus, Theorem 5.8.12 **(b)** is proved.

(c) From (119), we obtain

$$\begin{aligned} 0 &= z^{p-1} + z^{p-2} + \cdots + z^0 = \left(z^{p-1} + z^{p-2} + \cdots + z^1\right) + \underbrace{z^0}_{=1_A} \\ &= \left(z^{p-1} + z^{p-2} + \cdots + z^1\right) + 1_A. \end{aligned}$$

In other words,

$$z^{p-1} + z^{p-2} + \cdots + z^1 = -1_A. \tag{120}$$

We have $\tau = \sum\limits_{i=0}^{p-1} \left(\dfrac{i}{p}\right) z^i$ and $\tau = \sum\limits_{i=0}^{p-1} \left(\dfrac{i}{p}\right) z^i = \sum\limits_{j=0}^{p-1} \left(\dfrac{j}{p}\right) z^j$. Multiplying these two equalities, we obtain

$$\begin{aligned} \tau\tau &= \left(\sum_{i=0}^{p-1} \left(\frac{i}{p}\right) z^i\right) \left(\sum_{j=0}^{p-1} \left(\frac{j}{p}\right) z^j\right) = \sum_{i=0}^{p-1} \sum_{j=0}^{p-1} \left(\frac{i}{p}\right) z^i \left(\frac{j}{p}\right) z^j \\ &= \underbrace{\sum_{i=0}^{p-1} \sum_{j=0}^{p-1}}_{= \sum\limits_{(i,j) \in \{0,1,\ldots,p-1\}^2}} \left(\frac{i}{p}\right) \left(\frac{j}{p}\right) z^i z^j = \sum_{(i,j) \in \{0,1,\ldots,p-1\}^2} \left(\frac{i}{p}\right) \left(\frac{j}{p}\right) z^i z^j \\ &= \sum_{k=0}^{p-1} \sum_{\substack{(i,j) \in \{0,1,\ldots,p-1\}^2; \\ i+j \equiv k \bmod p}} \left(\frac{i}{p}\right) \left(\frac{j}{p}\right) \underbrace{z^i z^j}_{\substack{= z^{i+j} = z^k \\ \text{(by Theorem 5.8.12 \textbf{(b)},} \\ \text{since } i+j \equiv k \bmod p)}} \\ &\qquad \left(\begin{array}{c} \text{because for each } (i,j) \in \{0,1,\ldots,p-1\}^2, \text{ there exists a} \\ \text{unique } k \in \{0,1,\ldots,p-1\} \text{ that satisfies } i+j \equiv k \bmod p \\ \text{(namely, this } k \text{ is the remainder of } i+j \text{ upon division by } p) \end{array} \right) \\ &= \sum_{k=0}^{p-1} \sum_{\substack{(i,j) \in \{0,1,\ldots,p-1\}^2; \\ i+j \equiv k \bmod p}} \left(\frac{i}{p}\right) \left(\frac{j}{p}\right) z^k. \end{aligned} \tag{121}$$

Now, let $k \in \{0,1,\ldots,p-1\}$ be a number, and let $(i,j) \in \{0,1,\ldots,p-1\}^2$ be a pair satisfying $i + j \equiv k \bmod p$. Then, Corollary 5.8.5 yields

$$\left(\frac{ij}{p}\right) = \left(\frac{i}{p}\right) \left(\frac{j}{p}\right). \tag{122}$$

However, from $i+j \equiv k \bmod p$, we obtain $j \equiv k-i \bmod p$ and thus $ij \equiv i(k-i) = (-1)\,i(i-k) \bmod p$. Hence, $\left(\frac{ij}{p}\right) = \left(\frac{(-1)\,i(i-k)}{p}\right)$ (by (110), applied to $a = ij$ and $b = (-1)\,i(i-k)$). Comparing this with (122), we obtain

$$\left(\frac{i}{p}\right)\left(\frac{j}{p}\right) = \left(\frac{(-1)\,i(i-k)}{p}\right) = \underbrace{\left(\frac{-1}{p}\right)}_{\substack{=(-1)^{(p-1)/2} \\ \text{(by (115))}}} \left(\frac{i(i-k)}{p}\right)$$

$$\text{(by Corollary 5.8.5, applied to } a=-1 \text{ and } b=i(i-k)\text{)}$$

$$= (-1)^{(p-1)/2}\left(\frac{i(i-k)}{p}\right). \tag{123}$$

Forget that we fixed k and (i,j). We thus have proved (123) for each $k \in \{0,1,\ldots,p-1\}$ and each pair $(i,j) \in \{0,1,\ldots,p-1\}^2$ satisfying $i+j \equiv k \bmod p$. Therefore, (121) becomes

$$\begin{aligned}
\tau\tau &= \sum_{k=0}^{p-1} \sum_{\substack{(i,j)\in\{0,1,\ldots,p-1\}^2; \\ i+j\equiv k \bmod p}} \underbrace{\left(\frac{i}{p}\right)\left(\frac{j}{p}\right)}_{\substack{=(-1)^{(p-1)/2}\left(\frac{i(i-k)}{p}\right) \\ \text{(by (123))}}} z^k \\
&= (-1)^{(p-1)/2} \sum_{k=0}^{p-1} \underbrace{\sum_{\substack{(i,j)\in\{0,1,\ldots,p-1\}^2; \\ i+j\equiv k \bmod p}}}_{\substack{=\sum\limits_{i=0}^{p-1} \sum\limits_{\substack{j\in\{0,1,\ldots,p-1\}; \\ i+j\equiv k \bmod p}} \\ =\sum\limits_{i=0}^{p-1} \sum\limits_{\substack{j\in\{0,1,\ldots,p-1\}; \\ j\equiv k-i \bmod p}} \\ \text{(since the congruence } i+j\equiv k \bmod p \\ \text{is equivalent to } j\equiv k-i \bmod p\text{)}}} \left(\frac{i(i-k)}{p}\right) z^k \\
&= (-1)^{(p-1)/2} \sum_{k=0}^{p-1} \sum_{i=0}^{p-1} \sum_{\substack{j\in\{0,1,\ldots,p-1\}; \\ j\equiv k-i \bmod p}} \left(\frac{i(i-k)}{p}\right) z^k.
\end{aligned} \tag{124}$$

Now, fix two numbers $k, i \in \{0,1,\ldots,p-1\}$. Then, there is a unique number $j \in \{0,1,\ldots,p-1\}$ that satisfies $j \equiv k-i \bmod p$ (namely, the remainder of $k-i$ upon division by p). Hence, the sum $\sum\limits_{\substack{j\in\{0,1,\ldots,p-1\}; \\ j\equiv k-i \bmod p}} \left(\frac{i(i-k)}{p}\right)$ has exactly 1 addend, and therefore simplifies to $\left(\frac{i(i-k)}{p}\right)$.

Forget that we fixed k, i. We thus have shown that

$$\sum_{\substack{j \in \{0,1,\ldots,p-1\}; \\ j \equiv k-i \bmod p}} \left(\frac{i\left(i-k\right)}{p} \right) = \left(\frac{i\left(i-k\right)}{p} \right) \tag{125}$$

for each $k, i \in \{0, 1, \ldots, p-1\}$. Thus,

$$\begin{aligned}
&\sum_{k=0}^{p-1} \sum_{i=0}^{p-1} \underbrace{\sum_{\substack{j \in \{0,1,\ldots,p-1\}; \\ j \equiv k-i \bmod p}} \left(\frac{i\left(i-k\right)}{p} \right)}_{= \left(\frac{i\left(i-k\right)}{p} \right) \text{ (by (125))}} z^k \\
&= \sum_{k=0}^{p-1} \sum_{i=0}^{p-1} \left(\frac{i\left(i-k\right)}{p} \right) z^k \\
&= \underbrace{\sum_{i=0}^{p-1} \left(\frac{i\left(i-0\right)}{p} \right)}_{\substack{=p-1 \\ \text{(by Proposition 5.8.11 \textbf{(a)}, applied to } k=0)}} \underbrace{z^0}_{=1_A} + \sum_{k=1}^{p-1} \underbrace{\sum_{i=0}^{p-1} \left(\frac{i\left(i-k\right)}{p} \right)}_{\substack{=-1 \\ \text{(by Proposition 5.8.11 \textbf{(b)}, since } k \in \{1,2,\ldots,p-1\} \text{ entails } p \nmid k)}} z^k \\
&\qquad \left(\text{here, we have split off the addend for } k = 0 \text{ from the sum} \right) \\
&= \left(p-1\right) \cdot 1_A + \sum_{k=1}^{p-1} \left(-1\right) z^k \\
&= \left(p-1\right) \cdot 1_A - \underbrace{\sum_{k=1}^{p-1} z^k}_{\substack{= z^{p-1} + z^{p-2} + \cdots + z^1 = -1_A \\ \text{(by (120))}}} \\
&= \left(p-1\right) \cdot 1_A - \left(-1_A\right) = p \cdot 1_A.
\end{aligned}$$

Therefore, we can rewrite (124) as

$$\tau\tau = \left(-1\right)^{(p-1)/2} p \cdot 1_A.$$

In other words, $\tau^2 = \left(-1\right)^{(p-1)/2} p \cdot 1_A$. This proves Theorem 5.8.12 **(c)**. □

5.8.9. Proof of quadratic reciprocity for two odd primes

We are now ready to prove the Quadratic Reciprocity Law for two odd primes (i.e., part **(b)** of Theorem 5.8.10):

*Proof of Theorem 5.8.10 **(b)**.* Let F be the field $\mathbb{Z}/q$. (This is a field, since q is prime.) We have $q \nmid p$ (since p and q are two distinct primes); thus, the residue class $\overline{p}$ in $\mathbb{Z}/q$ is nonzero. Since $\mathbb{Z}/q$ is a field, this shows that $\overline{p}$ is a unit.

Now, we shall extend the field F to a ring by adjoining an element z that satisfies $z^{p-1} + z^{p-2} + \cdots + z^0 = 0$.

Indeed, the polynomial $x^{p-1} + x^{p-2} + \cdots + x^0 \in F[x]$ is a monic polynomial of degree $p-1$ over F, so that its leading coefficient is a unit. Thus, by Theorem 4.5.9 **(d)** (applied to $R = F$ and $b = x^{p-1} + x^{p-2} + \cdots + x^0$ and $m = p-1$), there exists a commutative ring that contains F as a subring and that contains a root of $x^{p-1} + x^{p-2} + \cdots + x^0$.

Let A be this ring, and let z be this root that it contains. Thus, $z \in A$ satisfies $z^{p-1} + z^{p-2} + \cdots + z^0 = 0$. (Note that we could use Theorem 5.3.7 **(b)** to obtain a field instead of this ring A, but we will have no need for this, so we have applied the less advanced Theorem 4.5.9 **(d)**.)

Note that A is a commutative $\mathbb{Z}/q$-algebra (since A is a commutative ring that contains $F = \mathbb{Z}/q$ as a subring).

Define an element $\tau \in A$ by

$$\tau = \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) z^i. \tag{126}$$

Then, Theorem 5.8.12 **(c)** yields[176]

$$\begin{aligned}
\tau^2 &= (-1)^{(p-1)/2} p \cdot \underbrace{1_A}_{\substack{=\overline{1} \\ (\text{in } \mathbb{Z}/q)}} = (-1)^{(p-1)/2} p \cdot \overline{1} \\
&= \overline{(-1)^{(p-1)/2} p} \\
&= \overline{(-1)^{(p-1)/2}} \cdot \overline{p}.
\end{aligned} \tag{127}$$

This shows that τ^2 is a unit of $\mathbb{Z}/q$ (since $\overline{(-1)^{(p-1)/2}}$ and $\overline{p}$ are units of $\mathbb{Z}/q$).

We shall now compute τ^{q-1}.

First, q is odd (since $q \neq 2$ is a prime), and thus $(q-1)/2 \in \mathbb{N}$. Taking the equality (127) to the $(q-1)/2$-th power, we obtain

$$\begin{aligned}
\left(\tau^2\right)^{(q-1)/2} &= \left(\overline{(-1)^{(p-1)/2} p}\right)^{(q-1)/2} = \overline{\left((-1)^{(p-1)/2} p\right)^{(q-1)/2}} \\
&= \overline{\left((-1)^{(p-1)/2}\right)^{(q-1)/2} p^{(q-1)/2}} = \overline{\left((-1)^{(p-1)/2}\right)^{(q-1)/2}} \cdot \overline{p^{(q-1)/2}}.
\end{aligned}$$

In view of $\left(\tau^2\right)^{(q-1)/2} = \tau^{q-1}$ and $\left((-1)^{(p-1)/2}\right)^{(q-1)/2} = (-1)^{(p-1)(q-1)/4}$, we can rewrite this as

$$\tau^{q-1} = \overline{(-1)^{(p-1)(q-1)/4}} \cdot \overline{p^{(q-1)/2}}. \tag{128}$$

[176] Here and in the rest of this proof, the notation $\overline{r}$ always means the residue class of an integer r in $\mathbb{Z}/q$.

However, Theorem 5.8.4 (applied to q and p instead of p and a) yields $\left(\frac{p}{q}\right) \equiv p^{(q-1)/2} \bmod q$. In other words, $\overline{\left(\frac{p}{q}\right)} = \overline{p^{(q-1)/2}}$ in $\mathbb{Z}/q$. Hence, we can rewrite (128) as

$$\begin{aligned} \tau^{q-1} &= \overline{(-1)^{(p-1)(q-1)/4}} \cdot \overline{\left(\frac{p}{q}\right)} \\ &= \overline{(-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right)}. \end{aligned} \tag{129}$$

On the other hand, define a map

$$\begin{aligned} \mathbf{f} : A &\to A, \\ a &\mapsto a^q. \end{aligned}$$

Then, Corollary 5.3.10 (applied to A and q instead of F and p) shows that $\mathbf{f}$ is a ring morphism (since A is a commutative $\mathbb{Z}/q$-algebra). Applying this map $\mathbf{f}$ to both sides of (126), we find

$$\begin{aligned} \mathbf{f}(\tau) &= \mathbf{f}\left(\sum_{i=0}^{p-1} \left(\frac{i}{p}\right) z^i\right) \\ &= \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \underbrace{\mathbf{f}\left(z^i\right)}_{\substack{=\left(z^i\right)^q \\ \text{(by the definition of } \mathbf{f}\text{)}}} \qquad \text{(since } \mathbf{f} \text{ is a ring morphism)} \\ &= \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) \underbrace{\left(z^i\right)^q}_{=z^{iq}} = \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) z^{iq}. \end{aligned}$$

Since $\mathbf{f}(\tau) = \tau^q$ (by the definition of $\mathbf{f}$), we can rewrite this as

$$\tau^q = \sum_{i=0}^{p-1} \left(\frac{i}{p}\right) z^{iq}. \tag{130}$$

We shall now rewrite τ in a different way. To this purpose, we consider the map

$$\begin{aligned} \{0, 1, \ldots, p-1\} &\to \{0, 1, \ldots, p-1\}, \\ i &\mapsto (iq) \,\%p, \end{aligned}$$

where $(iq) \,\%p$ denotes the remainder that iq leaves upon division by p. This

map is easily seen to be bijective[177]. Thus, we can substitute $(iq)\,\%p$ for i in the sum $\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)z^i$. We thus obtain

$$\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)z^i = \sum_{i=0}^{p-1} \underbrace{\left(\frac{(iq)\,\%p}{p}\right)}_{=\left(\frac{iq}{p}\right)} \underbrace{z^{(iq)\%p}}_{=z^{iq}}$$

(by (110), since $(iq)\%p \equiv iq \bmod p$; by Theorem 5.8.12 **(b)**, since $(iq)\%p \equiv iq \bmod p$)

$$= \sum_{i=0}^{p-1} \underbrace{\left(\frac{iq}{p}\right)}_{=\left(\frac{i}{p}\right)\left(\frac{q}{p}\right)} z^{iq} = \left(\frac{q}{p}\right)\cdot \underbrace{\sum_{i=0}^{p-1}\left(\frac{i}{p}\right)z^{iq}}_{=\tau^q} = \left(\frac{q}{p}\right)\cdot\tau^q.$$

(by Corollary 5.8.5; by (130))

In view of (126), we can rewrite this as

$$\tau = \left(\frac{q}{p}\right)\cdot\tau^q.$$

Multiplying both sides of this equality by τ, we obtain

$$\tau^2 = \left(\frac{q}{p}\right)\cdot \underbrace{\tau^{q+1}}_{=\tau^{q-1}\cdot\tau^2} = \left(\frac{q}{p}\right)\cdot\tau^{q-1}\cdot\tau^2$$

$$= \left(\frac{q}{p}\right)\cdot \overline{(-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)}\cdot\tau^2 \qquad \text{(by (129))}.$$

Since τ^2 is a unit of $\mathbb{Z}/q$, we can cancel τ^2 from both sides of this equality (by multiplying by its inverse). Thus, we obtain

$$\overline{1} = \left(\frac{q}{p}\right)\cdot\overline{(-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)} = \overline{\left(\frac{q}{p}\right)\cdot(-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)}$$

$$= \overline{(-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)}.$$

[177] *Proof.* It suffices to show that this map is injective (because an injective map between two finite sets of the same size is automatically bijective). So let us show this.

Let i_1, i_2 be two distinct elements of $\{0,1,\ldots,p-1\}$. We must prove that $(i_1q)\,\%p \neq (i_2q)\,\%p$.

Assume the contrary. Thus, $(i_1q)\,\%p = (i_2q)\,\%p$. Hence, $i_1q \equiv i_2q \bmod p$ (because two integers leave the same remainder upon division by p if and only if they are congruent modulo p). In other words, $p \mid i_1q - i_2q$. In other words, $p \mid (i_1 - i_2)\,q$. Since p is a prime, this entails that either $p \mid i_1 - i_2$ or $p \mid q$ (or both). Since $p \mid q$ is impossible (because p and q are two distinct primes), we thus conclude that $p \mid i_1 - i_2$. In other words, $i_1 \equiv i_2 \bmod p$. However, since $i_1, i_2 \in \{0,1,\ldots,p-1\}$, this entails $i_1 = i_2$, which contradicts the fact that i_1, i_2 are distinct. This contradiction shows that our assumption was false, qed.

In other words,

$$1 \equiv (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) \bmod q.$$

Thus, Lemma 5.8.6 (applied to q, 1 and $(-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right)$ instead of p, u and v) shows that

$$1 = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) \tag{131}$$

(because both 1 and $(-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) \left(\frac{q}{p}\right)$ are elements of $\{0, 1, -1\}$).

However, $p \nmid q$ (since p and q are two distinct primes), and thus $\left(\frac{q}{p}\right)$ is either 1 or -1. Hence, in either case, we have $\left(\frac{q}{p}\right)^2 = 1$. Now, multiplying both sides of the equality (131) by $\left(\frac{q}{p}\right)$, we obtain

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right) \underbrace{\left(\frac{q}{p}\right)^2}_{=1} = (-1)^{(p-1)(q-1)/4} \left(\frac{p}{q}\right).$$

This proves Theorem 5.8.10 **(b)**. □

See [Burton11, Chapter 9] or [Stein09, Chapter 4] (or almost any text on elementary number theory) for more about quadratic residues. A collection of proofs of Theorem 5.8.10 has also been published as a book ([Baumga15]); one of the most elementary proofs is presented in [KeeGui20, §3.12]. See also [Schroe09, particularly Chapter 16] for an application of quadratic residues to the acoustics of concert halls. Inside mathematics, there are many other applications:

Exercise 5.8.6. Let $p \neq 2$ be a prime. Prove the following:

(a) We have

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 8 \text{ or } p \equiv 3 \bmod 8; \\ -1, & \text{if } p \equiv -1 \bmod 8 \text{ or } p \equiv -3 \bmod 8. \end{cases}$$

(b) If $p \equiv 1 \bmod 8$ or $p \equiv 3 \bmod 8$, then p can be written in the form $x^2 + 2y^2$ for some $x, y \in \mathbb{Z}$.

[**Hint:** For part **(b)**, recall Exercise 2.13.1 and Section 2.16.]

Exercise 5.8.7. Let $p > 3$ be a prime. Prove the following:

(a) We have

$$\left(\frac{-3}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \bmod 3; \\ -1, & \text{if } p \equiv -1 \bmod 3. \end{cases}$$

(b) If $p \equiv 1 \bmod 3$, then p can be written in the form $u^2 - uv + v^2$ for some $u, v \in \mathbb{Z}$.

(c) If $p \equiv 1 \bmod 3$, then p can be written in the form $x^2 + 3y^2$ for some $x, y \in \mathbb{Z}$.

[**Hint:** For parts **(b)** and **(c)**, recall Exercise 2.13.3 and Section 2.16. This time, $\mathbb{Z}\left[\sqrt{-3}\right]$ is the wrong ring to be working in, since it is not Euclidean; but $\mathbb{Z}[\omega]$ acts its part well enough for part **(b)**. In order to obtain part **(c)**, use part **(b)** and then rewrite $u^2 - uv + v^2$ as $\left(\frac{u}{2} - v\right)^2 + 3\left(\frac{u}{2}\right)^2$ if u is even, or as $\left(\frac{v}{2} - u\right)^2 + 3\left(\frac{v}{2}\right)^2$ if v is even, or as $\left(\frac{u+v}{2}\right)^2 + 3\left(\frac{u-v}{2}\right)^2$ in the remaining case.]

Exercise 5.8.8. Let p be a prime such that $p \equiv 1 \bmod 8$ or $p \equiv 7 \bmod 8$. Prove that p can be written in the form $x^2 - 2y^2$ for some $x, y \in \mathbb{Z}$.

[**Hint:** Recall Exercise 2.13.2. Furthermore, observe that if $a^2 - 2b^2 = -p$, then $(a-2b)^2 - 2(a-b)^2 = p$.]

5.8.10. Jacobsthal's explicit formulas for $p = x^2 + y^2$

Legendre symbols are useful not only for studying squares in $\mathbb{Z}/p$. A surprising application was found by Jacobsthal in 1907 [Jacobs07, Seite 240]: Recall that Theorem 2.16.1 says that each prime p satisfying $p \equiv 1 \bmod 4$ can be written as a sum of two perfect squares. Jacobsthal used Legendre symbols to not only prove this theorem in a new way, but also to give "explicit" formulas for two perfect squares that sum to p. We are using scare quotes around the word "explicit", since using these formulas to compute the squares is much slower than searching for the squares by brute force (let alone than an actually efficient algorithm, such as the one given in [Stein09, §5.7]), but the formulas are fascinating in their own right.

Jacobsthal's theorem can be stated as follows:

Theorem 5.8.13 (Jacobsthal's formulas)**.** Let p be a prime such that $p \equiv 1 \bmod 4$. For any integer h, define

$$W(h) := \sum_{i=0}^{p-1} \left(\frac{i\left(i^2+h\right)}{p}\right) \in \mathbb{Z}. \tag{132}$$

Let m be a QNR mod p (that is, an integer such that $\overline{m} \in \mathbb{Z}/p$ is not a square). Let $a = W(1)$ and $b = W(m)$. Then:

(a) The integers a and b are even.

(b) We have $p = (a/2)^2 + (b/2)^2$.

Take a moment to appreciate this theorem as a miracle, before we somewhat dispel the mystery through the proof. First, an example:

- Let $p = 13$ (a prime that satisfies $p \equiv 1 \bmod 4$), and let $m = 5$ (a QNR mod p). Then, using the notation of Theorem 5.8.13, we have

$$\begin{aligned} a = W(1) &= \sum_{i=0}^{p-1} \left(\frac{i\left(i^2+1\right)}{p} \right) \\ &= \left(\frac{0\left(0^2+1\right)}{13} \right) + \left(\frac{1\left(1^2+1\right)}{13} \right) + \cdots + \left(\frac{12\left(12^2+1\right)}{13} \right) \\ &= 0 + (-1) + 1 + 1 + 1 + 0 + 1 + 1 + 0 + 1 + 1 + 1 + (-1) \\ &= 6 \end{aligned}$$

and

$$\begin{aligned} b = W(m) = W(5) &= \sum_{i=0}^{p-1} \left(\frac{i\left(i^2+5\right)}{p} \right) \\ &= \left(\frac{0\left(0^2+5\right)}{13} \right) + \left(\frac{1\left(1^2+5\right)}{13} \right) + \cdots + \left(\frac{12\left(12^2+5\right)}{13} \right) \\ &= 0 + (-1) + (-1) + 1 + (-1) + (-1) + 1 + 1 \\ &\qquad + (-1) + (-1) + 1 + (-1) + (-1) \\ &= -4, \end{aligned}$$

so that a and b are indeed even and we indeed have $p = (a/2)^2 + (b/2)^2$ (since $(a/2)^2 + (b/2)^2 = (6/2)^2 + (-4/2)^2 = 9 + 4 = 13 = p$).

The numbers $W(h)$ in Theorem 5.8.13 (and several similarly defined numbers) are known as **Jacobsthal sums**.

A sequence of lemmas will pave our way to the proof of Theorem 5.8.13. First, however, we introduce a simple piece of notation:

Definition 5.8.14. Let $p \neq 2$ be a prime. Let $u \in \mathbb{Z}/p$. Then, $K_p(u)$ shall denote the Legendre symbol $\left(\frac{a}{p} \right)$, where a is an integer satisfying $\overline{a} = u$. This Legendre symbol is well-defined, i.e., it depends only on u (not on a), because if a and b are two integers satisfying $\overline{a} = \overline{b}$, then $a \equiv b \bmod p$ and therefore $\left(\frac{a}{p} \right) = \left(\frac{b}{p} \right)$ (by (110)).

For example, $K_5(\overline{7}) = \left(\frac{7}{5} \right) = -1$ and $K_5(\overline{10}) = \left(\frac{10}{5} \right) = 0$.

We fix a prime $p \neq 2$ for the rest of this subsection (but we don't require that $p \equiv 1 \bmod 4$). From Definition 5.8.14, it follows that

$$K_p\left(\overline{a}\right) = \left(\frac{a}{p}\right) \qquad \text{for any } a \in \mathbb{Z}. \tag{133}$$

As a warm-up, we shall prove some facts about the $K_p\left(u\right)$, many of which are mere restatements of known properties of Legendre symbols using our new notation for them:

Lemma 5.8.15. Let $u \in \mathbb{Z}/p$. Then:

(a) If $u = 0$, then $K_p\left(u\right) = 0$.

(b) If $u \neq 0$ but u is a square, then $K_p\left(u\right) = 1$.

(c) If u is not a square, then $K_p\left(u\right) = -1$.

(d) If $u \neq 0$, then $K_p\left(u\right) \equiv 1 \bmod 2$.

(e) We always have $\left(K_p\left(u\right)\right)^3 = K_p\left(u\right)$.

(f) If $u \neq 0$, then $\left(K_p\left(u\right)\right)^2 = 1$.

Proof. Write the residue class u in the form $u = \overline{a}$ for some $a \in \mathbb{Z}$. Then, $K_p\left(u\right) = \left(\frac{a}{p}\right)$ (by Definition 5.8.14).

(a) We must prove that $K_p\left(0\right) = 0$. However, the zero of $\mathbb{Z}/p$ is the residue class $\overline{0}$. That is, $0 = \overline{0}$. Hence, $K_p\left(0\right) = K_p\left(\overline{0}\right) = \left(\frac{0}{p}\right)$ (by (133)), so that $K_p\left(0\right) = \left(\frac{0}{p}\right) = 0$ (by Definition 5.8.2, since $p \mid 0$). This proves Lemma 5.8.15 **(a)**.

(b) Assume that $u \neq 0$ and that u is a square. Then, $\overline{a} = u \neq 0$ in $\mathbb{Z}/p$, so that a is not divisible by p. Moreover, $\overline{a} = u$ is a square in $\mathbb{Z}/p$. Hence, a is a QR mod p (by the definition of a QR). Therefore, $\left(\frac{a}{p}\right) = 1$ (by the definition of the Legendre symbol). Now, $K_p\left(u\right) = \left(\frac{a}{p}\right) = 1$. This proves Lemma 5.8.15 **(b)**.

(c) Assume that u is not a square. Then, $\overline{a} = u \neq 0$ in $\mathbb{Z}/p$ (since 0 is a square but u is not), so that a is not divisible by p. Moreover, $\overline{a} = u$ is not a square in $\mathbb{Z}/p$. Hence, a is a QNR mod p (by the definition of a QNR). Therefore, $\left(\frac{a}{p}\right) = -1$ (by the definition of the Legendre symbol). Now, $K_p\left(u\right) = \left(\frac{a}{p}\right) = -1$. This proves Lemma 5.8.15 **(c)**.

(d) Assume that $u \neq 0$. Then, parts **(b)** and **(c)** of Lemma 5.8.15 show that $K_p\left(u\right)$ is either 1 or -1. In either case, $K_p\left(u\right)$ is odd, i.e., we have $K_p\left(u\right) \equiv 1 \bmod 2$. This proves Lemma 5.8.15 **(d)**.

(e) The number $K_p\left(u\right)$ is a Legendre symbol (by its definition) and thus belongs to the set $\{0, 1, -1\}$ (since any Legendre symbol belongs to this set). In other words, $K_p\left(u\right) \in \{0, 1, -1\}$.

However, each number $x \in \{0, 1, -1\}$ satisfies $x^3 = x$ (just check this for each of the values 0, 1 and -1). Applying this to $x = K_p(u)$, we obtain $\left(K_p(u)\right)^3 = K_p(u)$ (since $K_p(u) \in \{0, 1, -1\}$). This proves Lemma 5.8.15 **(e)**.

(f) Assume that $u \neq 0$. Then, parts **(b)** and **(c)** of Lemma 5.8.15 show that $K_p(u)$ is either 1 or -1. In either case, $\left(K_p(u)\right)^2 = 1$. This proves Lemma 5.8.15 **(f)**. □

Lemma 5.8.16. Let $u \in \mathbb{Z}/p$. Then,[178]

$$K_p(u) = \left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = u\right) - 1.$$

Proof. Write the residue class u as $u = \overline{a}$ for some integer a. We are in one of the following three cases:

Case 1: We have $u = 0$.

Case 2: We have $u \neq 0$, but u is a square in $\mathbb{Z}/p$.

Case 3: The element u is not a square in $\mathbb{Z}/p$.

Let us first consider Case 1. In this case, $u = 0$. Thus, Lemma 5.8.15 **(a)** yields $K_p(u) = 0$. On the other hand, $\mathbb{Z}/p$ is an integral domain. Thus, there is only one element $x \in \mathbb{Z}/p$ such that $x^2 = 0$ (namely, 0). Thus,

$$\left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = 0\right) = 1.$$

In other words,

$$\left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = u\right) = 1$$

(since $u = 0$). Hence,

$$\left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = u\right) - 1 = 0 = K_p(u)$$

(since $K_p(u) = 0$). Thus, Lemma 5.8.16 is proved in Case 1.

Let us now consider Case 2. In this case, we have $u \neq 0$, but u is a square in $\mathbb{Z}/p$. Hence, Lemma 5.8.15 **(b)** yields $K_p(u) = 1$.

We have $u = y^2$ for some $y \in \mathbb{Z}/p$ (since u is a square). Consider this y. Then, $y \neq 0$ (since $y^2 = u \neq 0$). Also, $\overline{2} \neq 0$ in $\mathbb{Z}/p$ (since $p \neq 2$ is a prime). Now, $2y = \underbrace{\left(2 \cdot 1_{\mathbb{Z}/p}\right)}_{=\overline{2}} y = \overline{2}y \neq 0$ (since $\overline{2} \neq 0$ and $y \neq 0$, and since $\mathbb{Z}/p$ is an integral domain). Subtracting y from this non-equation, we obtain $y \neq -y$.

Now,

$$\begin{aligned}
\left\{x \in \mathbb{Z}/p \mid x^2 = y^2\right\} &= \left\{x \in \mathbb{Z}/p \mid x^2 - y^2 = 0\right\} \\
&= \left\{x \in \mathbb{Z}/p \mid (x-y)(x+y) = 0\right\} \\
&\qquad \left(\text{since } x^2 - y^2 = (x-y)(x+y)\right) \\
&= \left\{x \in \mathbb{Z}/p \mid x - y = 0 \text{ or } x + y = 0\right\} \\
&\qquad (\text{since } \mathbb{Z}/p \text{ is an integral domain}) \\
&= \left\{x \in \mathbb{Z}/p \mid x = y \text{ or } x = -y\right\} \\
&= \{y, -y\}. \qquad (134)
\end{aligned}$$

[178] The symbol "#" means "number". For instance, $(\text{\# of odd integers } i \in \{0, 1, \ldots, 10\}) = 5$.

However, $u = y^2$, and thus

$$\begin{aligned}
&\left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = u\right) \\
&= \left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = y^2\right) \\
&= \left|\left\{x \in \mathbb{Z}/p \mid x^2 = y^2\right\}\right| = |\{y, -y\}| \qquad \text{(by (134))} \\
&= 2 \qquad (\text{since } y \neq -y),
\end{aligned}$$

so that

$$\left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = u\right) - 1 = 2 - 1 = 1 = K_p(u)$$

(since $K_p(u) = 1$). Thus, Lemma 5.8.16 is proved in Case 2.

Finally, let us consider Case 3. In this case, the element u is not a square in $\mathbb{Z}/p$. Thus, Lemma 5.8.15 **(c)** yields $K_p(u) = -1$. Also, there exist no elements $x \in \mathbb{Z}/p$ such that $x^2 = u$ (since u is not a square). Hence,

$$\left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = u\right) = 0,$$

so that

$$\left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = u\right) - 1 = 0 - 1 = -1 = K_p(u)$$

(since $K_p(u) = -1$). Thus, Lemma 5.8.16 is proved in Case 3.

We have now proved Lemma 5.8.16 in all three cases, so that Lemma 5.8.16 is really proved. □

Lemma 5.8.17. We have

$$\sum_{u \in \mathbb{Z}/p} K_p(u) = 0.$$

Proof. By Lemma 5.8.16, we have

$$\begin{aligned}
\sum_{u \in \mathbb{Z}/p} K_p(u) &= \sum_{u \in \mathbb{Z}/p} \left(\left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = u\right) - 1\right) \\
&= \underbrace{\sum_{u \in \mathbb{Z}/p} \left(\text{\# of elements } x \in \mathbb{Z}/p \text{ such that } x^2 = u\right)}_{\substack{= (\text{\# of all elements } x \in \mathbb{Z}/p) \\ (\text{since each } x \in \mathbb{Z}/p \text{ satisfies } x^2 = u \text{ for exactly one } u \in \mathbb{Z}/p)}} - \underbrace{\sum_{u \in \mathbb{Z}/p} 1}_{= |\mathbb{Z}/p|} \\
&= \underbrace{(\text{\# of all elements } x \in \mathbb{Z}/p)}_{= |\mathbb{Z}/p|} - |\mathbb{Z}/p| = |\mathbb{Z}/p| - |\mathbb{Z}/p| = 0.
\end{aligned}$$

This proves Lemma 5.8.17. □

Lemma 5.8.18. Let $u, v \in \mathbb{Z}/p$. Then, $K_p(uv) = K_p(u) \cdot K_p(v)$.

Proof. This is just a restatement of Corollary 5.8.5. In more detail:

Write the residue classes u and v in the forms $u = \overline{a}$ and $v = \overline{b}$ for some $a, b \in \mathbb{Z}$. Then, $uv = \overline{a} \cdot \overline{b} = \overline{ab}$. Hence,

$$\begin{aligned} K_p(uv) &= K_p\left(\overline{ab}\right) = \left(\frac{ab}{p}\right) \qquad \text{(by (133), applied to } ab \text{ instead of } a\text{)} \\ &= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \qquad \text{(by Corollary 5.8.5)}. \end{aligned}$$

Comparing this with

$$K_p\left(\underbrace{u}_{=\overline{a}}\right) K_p\left(\underbrace{v}_{=\overline{b}}\right) = \underbrace{K_p(\overline{a})}_{\substack{=\left(\frac{a}{p}\right) \\ \text{(by (133))}}} \underbrace{K_p\left(\overline{b}\right)}_{\substack{=\left(\frac{b}{p}\right) \\ \text{(by (133))}}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

we find $K_p(uv) = K_p(u) \cdot K_p(v)$. This proves Lemma 5.8.18. □

Lemma 5.8.19. Let $y \in \mathbb{Z}/p$ be nonzero. Then,

$$\sum_{\substack{x \in \mathbb{Z}/p; \\ x^2 = y^2}} K_p(xy) = 1 + (-1)^{(p-1)/2}.$$

Proof. Let $u = y^2$. Then, $u = y^2 = yy$ is nonzero (since y is nonzero, and since $\mathbb{Z}/p$ is an integral domain). Thus, as in the proof of Lemma 5.8.16 (specifically, in Case 2), we can see that $\left\{x \in \mathbb{Z}/p \mid x^2 = y^2\right\} = \{y, -y\}$ and $y \neq -y$. This shows that the sum $\sum_{\substack{x \in \mathbb{Z}/p; \\ x^2 = y^2}} K_p(xy)$ has only two addends, namely the addends for $x = y$ and for $x = -y$. Hence,

$$\begin{aligned} \sum_{\substack{x \in \mathbb{Z}/p; \\ x^2 = y^2}} K_p(xy) &= K_p\left(\underbrace{yy}_{=y^2}\right) + K_p\left(\underbrace{(-y)\,y}_{=(-1)y^2}\right) = K_p\left(y^2\right) + \underbrace{K_p\left((-1)\,y^2\right)}_{\substack{=K_p(-1)K_p\left(y^2\right) \\ \text{(by Lemma 5.8.18)}}} \\ &= K_p\left(y^2\right) + K_p(-1)\,K_p\left(y^2\right) = \left(1 + K_p(-1)\right) K_p\left(\underbrace{y^2}_{=u}\right) \\ &= \left(1 + K_p(-1)\right) K_p(u). \end{aligned} \tag{135}$$

However, u is a square (since $u = y^2$) and satisfies $u \neq 0$ (since u is nonzero). Thus, Lemma 5.8.15 **(b)** yields $K_p(u) = 1$. Moreover, in $\mathbb{Z}/p$, we have $-1 = \overline{-1}$, so that

$$\begin{aligned} K_p(-1) &= K_p\left(\overline{-1}\right) = \left(\frac{-1}{p}\right) \qquad \text{(by (133))} \\ &= \begin{cases} 1, & \text{if } p \equiv 1 \bmod 4; \\ -1, & \text{if } p \equiv 3 \bmod 4 \end{cases} \qquad \text{(by Theorem 5.8.9)} \\ &= (-1)^{(p-1)/2}. \end{aligned}$$

Thus, (135) becomes

$$\sum_{\substack{x\in\mathbb{Z}/p;\\ x^2=y^2}} K_p(xy) = \left(1+K_p(-1)\right)\underbrace{K_p(u)}_{=1} = 1+\underbrace{K_p(-1)}_{=(-1)^{(p-1)/2}} = 1+(-1)^{(p-1)/2}.$$

This proves Lemma 5.8.19. □

For each $d \in \mathbb{Z}/p$, we define an integer $W(d)$ by

$$W(d) = \sum_{u\in\mathbb{Z}/p} K_p\left(u\left(u^2+d\right)\right).$$

Thus, for each $h \in \mathbb{Z}$, we have

$$W\left(\overline{h}\right) = \sum_{u\in\mathbb{Z}/p} K_p\left(u\left(u^2+\overline{h}\right)\right) = \sum_{i=0}^{p-1} K_p\left(\underbrace{\overline{i}\left(\overline{i}^2+\overline{h}\right)}_{=\overline{i(i^2+h)}}\right)$$

$$\left(\begin{array}{c}\text{here, we have substituted } \overline{i} \text{ for } u \text{ in the sum,}\\ \text{since the map } \{0,1,\ldots,p-1\}\to\mathbb{Z}/p\\ \text{that sends each } i \text{ to } \overline{i} \text{ is a bijection}\end{array}\right)$$

$$= \sum_{i=0}^{p-1} \underbrace{K_p\left(\overline{i\left(i^2+h\right)}\right)}_{=\left(\frac{i\left(i^2+h\right)}{p}\right)} = \sum_{i=0}^{p-1}\left(\frac{i\left(i^2+h\right)}{p}\right). \tag{136}$$

(by (133))

The right hand side here is precisely what was called $W(h)$ in Theorem 5.8.13.

Now, we shall prove the following lemmas about these values $W(d)$:

Lemma 5.8.20. The residue class $\overline{0} \in \mathbb{Z}/p$ satisfies $W\left(\overline{0}\right) = 0$.

Proof. By definition of $W\left(\overline{0}\right)$, we have

$$W\left(\overline{0}\right) = \sum_{u\in\mathbb{Z}/p} K_p\left(u\underbrace{\left(u^2+\overline{0}\right)}_{=u^2}\right) = \sum_{u\in\mathbb{Z}/p} \underbrace{K_p\left(uu^2\right)}_{=K_p(u)\cdot K_p\left(u^2\right)} = \sum_{u\in\mathbb{Z}/p} K_p(u)\cdot \underbrace{K_p\left(u^2\right)}_{\substack{=K_p(uu)\\ =K_p(u)\cdot K_p(u)}}$$

(by Lemma 5.8.18) (by Lemma 5.8.18)

$$= \sum_{u\in\mathbb{Z}/p} \underbrace{K_p(u)\cdot K_p(u)\cdot K_p(u)}_{\substack{=\left(K_p(u)\right)^3\\ =K_p(u)}} = \sum_{u\in\mathbb{Z}/p} K_p(u) = 0$$

(by Lemma 5.8.15 **(e)**)

(by Lemma 5.8.17). This proves Lemma 5.8.20. □

Lemma 5.8.21. For any $d \in \mathbb{Z}/p$, the integer $W(d)$ is even.

Proof. We know that $p \neq 2$ is a prime; hence, p is odd. In other words, $p \equiv 1 \bmod 2$.

Let $d \in \mathbb{Z}/p$. The definition of $W(d)$ yields

$$\begin{aligned}
W(d) &= \sum_{u \in \mathbb{Z}/p} K_p\left(u\left(u^2+d\right)\right) \\
&= \sum_{\substack{u \in \mathbb{Z}/p; \\ u\left(u^2+d\right)=0}} \underbrace{K_p\left(u\left(u^2+d\right)\right)}_{\substack{=0 \\ \text{(by Lemma 5.8.15 \textbf{(a)}, applied to } u\left(u^2+d\right) \text{ instead of } u\text{)}}} + \sum_{\substack{u \in \mathbb{Z}/p; \\ u\left(u^2+d\right)\neq 0}} \underbrace{K_p\left(u\left(u^2+d\right)\right)}_{\substack{\equiv 1 \bmod 2 \\ \text{(by Lemma 5.8.15 \textbf{(d)}, applied to } u\left(u^2+d\right) \text{ instead of } u\text{)}}} \\
&\equiv \underbrace{\sum_{\substack{u \in \mathbb{Z}/p; \\ u\left(u^2+d\right)=0}} 0}_{=0} + \sum_{\substack{u \in \mathbb{Z}/p; \\ u\left(u^2+d\right)\neq 0}} 1 = \sum_{\substack{u \in \mathbb{Z}/p; \\ u\left(u^2+d\right)\neq 0}} 1 \\
&= \left|\left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right) \neq 0\right\}\right| \cdot 1 \\
&= \left|\left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right) \neq 0\right\}\right| \\
&= \underbrace{|\mathbb{Z}/p|}_{\substack{=p \\ \equiv 1 \bmod 2}} - \left|\left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right) = 0\right\}\right| \\
&\qquad \left(\begin{array}{c} \text{since the set } \left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right) \neq 0\right\} \text{ is the} \\ \text{complement of } \left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right) = 0\right\} \text{ within } \mathbb{Z}/p \end{array} \right) \\
&\equiv 1 - \left|\left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right) = 0\right\}\right| \bmod 2. \qquad (137)
\end{aligned}$$

We shall now prove that the number $\left|\left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right) = 0\right\}\right|$ is odd.

Indeed, assume the contrary. Thus, $\left|\left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right) = 0\right\}\right|$ is even. In other words, the number of all $u \in \mathbb{Z}/p$ satisfying $u\left(u^2+d\right) = 0$ is even. In other words, the number of roots of the polynomial $x\left(x^2+d\right) \in (\mathbb{Z}/p)[x]$ in $\mathbb{Z}/p$ is even.

The polynomial $x\left(x^2+d\right) \in (\mathbb{Z}/p)[x]$ has degree 3, and thus has ≤ 3 roots in $\mathbb{Z}/p$ (by Theorem 4.3.15, since $\mathbb{Z}/p$ is an integral domain). In other words, its number of roots is ≤ 3. Since we also know that this number is even, we thus conclude that this number is 0 or 2 (since the only even nonnegative integers ≤ 3 are 0 and 2). In other words, the polynomial $x\left(x^2+d\right) \in (\mathbb{Z}/p)[x]$ has either 0 or 2 roots in $\mathbb{Z}/p$. Since it cannot have 0 roots in $\mathbb{Z}/p$ (because 0 is clearly a root of this polynomial), we thus conclude that it has 2 roots in $\mathbb{Z}/p$. One of these 2 roots is 0 (since 0 is clearly a root of this polynomial); let r be the other root. Thus, $r \neq 0$ and $r\left(r^2+d\right) = 0$. Hence, $(-r)\left((-r)^2+d\right) = -\underbrace{r\left(r^2+d\right)}_{=0} = 0$. This shows that $-r$ is a root of the polynomial $x\left(x^2+d\right) \in (\mathbb{Z}/p)[x]$ in $\mathbb{Z}/p$. Since the only roots of this polynomial are 0 and r, we thus conclude that $-r$ must be either 0 or r. Since $-r$ cannot be 0 (because $r \neq 0$), we thus conclude that $-r = r$. Adding r to both sides of this equality, we find $0 = 2r = \underbrace{\left(2 \cdot 1_{\mathbb{Z}/p}\right)}_{=\overline{2}} r = \overline{2}r$. However, $\overline{2} \neq 0$ in $\mathbb{Z}/p$ (since $p \neq 2$ is a prime) and $r \neq 0$. Since $\mathbb{Z}/p$ is an integral domain, these entail that $\overline{2}r \neq 0$. This contradicts $0 = \overline{2}r$.

This contradiction shows that our assumption was wrong. Hence, we have shown that $\left|\left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right)=0\right\}\right|$ is odd. In other words,

$$\left|\left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right)=0\right\}\right| \equiv 1 \bmod 2.$$

Thus, (137) becomes

$$W(d) \equiv 1 - \underbrace{\left|\left\{u \in \mathbb{Z}/p \mid u\left(u^2+d\right)=0\right\}\right|}_{\equiv 1 \bmod 2} \equiv 1-1=0 \bmod 2.$$

In other words, $W(d)$ is even. This proves Lemma 5.8.21. □

Lemma 5.8.22. Let $d, c \in \mathbb{Z}/p$. Then, $W\left(c^2 d\right) = K_p(c)\, W(d)$.

Proof. We have $K_p\left(\overline{0}\right) = 0$ (by Lemma 5.8.15 **(a)**, applied to $u = \overline{0}$). Furthermore, $\overline{0}^2 d = \overline{0}$, and therefore

$$\begin{aligned} W\left(\overline{0}^2 d\right) &= W\left(\overline{0}\right) = 0 \qquad \text{(by Lemma 5.8.20)} \\ &= K_p\left(\overline{0}\right) W(d) \qquad \left(\text{since } \underbrace{K_p\left(\overline{0}\right)}_{=0} W(d) = 0\right). \end{aligned}$$

Thus, Lemma 5.8.22 is proved in the case when $c = \overline{0}$. For the rest of this proof, we thus WLOG assume that $c \neq \overline{0}$. Hence, c is a nonzero element of $\mathbb{Z}/p$, and thus is a unit (since $\mathbb{Z}/p$ is a field). Hence, the map

$$\begin{aligned} \mathbb{Z}/p &\to \mathbb{Z}/p, \\ u &\mapsto cu \end{aligned} \tag{138}$$

is a bijection. Furthermore, $c \neq \overline{0} = 0$ entails $c^2 \neq 0$ (since $\mathbb{Z}/p$ is an integral domain), and clearly c^2 is a square. Hence, Lemma 5.8.15 **(b)** (applied to $u = c^2$) shows that $K_p\left(c^2\right) = 1$.

Now, the definition of $W\left(c^2 d\right)$ yields

$$W\left(c^2 d\right) = \sum_{u \in \mathbb{Z}/p} K_p\left(u\left(u^2+c^2 d\right)\right) = \sum_{u \in \mathbb{Z}/p} K_p\left(\underbrace{(cu)\left((cu)^2+c^2 d\right)}_{=c^3 u\left(u^2+d\right)}\right)$$

$$\left(\begin{array}{c}\text{here, we have substituted } cu \text{ for } u \text{ in the sum,} \\ \text{since the map (138) is a bijection}\end{array}\right)$$

$$= \sum_{u \in \mathbb{Z}/p} \underbrace{K_p\left(c^3 u\left(u^2+d\right)\right)}_{\substack{=K_p\left(c^3\right) K_p\left(u\left(u^2+d\right)\right) \\ \text{(by Lemma 5.8.18)}}} = K_p\left(\underbrace{c^3}_{=cc^2}\right) \underbrace{\sum_{u \in \mathbb{Z}/p} K_p\left(u\left(u^2+d\right)\right)}_{\substack{=W(d) \\ \text{(by the definition of } W(d)\text{)}}}$$

$$= \underbrace{K_p\left(cc^2\right)}_{\substack{=K_p(c) K_p\left(c^2\right) \\ \text{(by Lemma 5.8.18)}}} W(d) = K_p(c) \underbrace{K_p\left(c^2\right)}_{=1} W(d) = K_p(c)\, W(d).$$

This proves Lemma 5.8.22. □

Lemma 5.8.23. Let $g \in \mathbb{Z}/p$ be an element of $\mathbb{Z}/p$ that is not a square. Let $d \in \mathbb{Z}/p$ be a further element. Then:

(a) If $d \in \mathbb{Z}/p$ is a nonzero square, then $(W(d))^2 = \left(W\left(\overline{1}\right)\right)^2$.

(b) If $d \in \mathbb{Z}/p$ is not a square, then $(W(d))^2 = (W(g))^2$.

Proof. **(a)** Assume that $d \in \mathbb{Z}/p$ is a nonzero square. Thus, $d = c^2$ for some $c \in \mathbb{Z}/p$. Consider this c. Then, $c \neq 0$ (since $c^2 = d \neq 0$). Thus, Lemma 5.8.15 **(f)** (applied to $u = c$) shows that $\left(K_p(c)\right)^2 = 1$. However, Lemma 5.8.22 (applied to $\overline{1}$ instead of d) yields $W\left(c^2 \cdot \overline{1}\right) = K_p(c) W\left(\overline{1}\right)$. In view of $c^2 \cdot \overline{1} = c^2 = d$, we can rewrite this as $W(d) = K_p(c) W\left(\overline{1}\right)$. Squaring this equality, we obtain

$$(W(d))^2 = \left(K_p(c) W\left(\overline{1}\right)\right)^2 = \underbrace{\left(K_p(c)\right)^2}_{=1} \left(W\left(\overline{1}\right)\right)^2 = \left(W\left(\overline{1}\right)\right)^2.$$

This proves Lemma 5.8.23 **(a)**.

(b) Assume that $d \in \mathbb{Z}/p$ is not a square. Thus, $d \neq 0$. Lemma 5.8.15 **(c)** yields $K_p(d) = -1$ (since d is not a square). Also, Lemma 5.8.15 **(c)** yields $K_p(g) = -1$ (since g is not a square).

We have $g \neq 0$ (since g is not a square). Hence, $\dfrac{d}{g} \in \mathbb{Z}/p$ is well-defined (since $\mathbb{Z}/p$ is a field). We have $d = \dfrac{d}{g} \cdot g$, so that

$$K_p(d) = K_p\left(\frac{d}{g} \cdot g\right) = K_p\left(\frac{d}{g}\right) \cdot K_p(g) \qquad \text{(by Lemma 5.8.18)}.$$

In view of $K_p(d) = -1$, this rewrites as $-1 = K_p\left(\dfrac{d}{g}\right) \cdot \underbrace{K_p(g)}_{=-1} = -K_p\left(\dfrac{d}{g}\right)$, so that $K_p\left(\dfrac{d}{g}\right) = 1$.

However, if $\dfrac{d}{g}$ was not a square, then Lemma 5.8.15 **(c)** would yield $K_p\left(\dfrac{d}{g}\right) = -1$, which would contradict $K_p\left(\dfrac{d}{g}\right) = 1$. Thus, $\dfrac{d}{g}$ must be a square. In other words, $\dfrac{d}{g} = c^2$ for some $c \in \mathbb{Z}/p$. Consider this c. Then, $c^2 g = d \neq 0$, so that $c \neq 0$. Thus, Lemma 5.8.15 **(f)** (applied to $u = c$) show that $\left(K_p(c)\right)^2 = 1$. However, Lemma 5.8.22 (applied to g instead of d) yields $W\left(c^2 g\right) = K_p(c) W(g)$. In view of $c^2 g = d$, we can rewrite this as $W(d) = K_p(c) W(g)$. Squaring this equality, we obtain

$$(W(d))^2 = \left(K_p(c) W(g)\right)^2 = \underbrace{\left(K_p(c)\right)^2}_{=1} (W(g))^2 = (W(g))^2.$$

This proves Lemma 5.8.23 **(b)**. □

Lemma 5.8.24. Let $g \in \mathbb{Z}/p$ be an element of $\mathbb{Z}/p$ that is not a square. Then,

$$\sum_{d \in \mathbb{Z}/p} \left(W\left(d\right)\right)^2 = \frac{p-1}{2}\left(\left(W\left(\overline{1}\right)\right)^2 + \left(W\left(g\right)\right)^2\right).$$

Proof. We have

$$\begin{aligned}
\sum_{d \in \mathbb{Z}/p} \left(W\left(d\right)\right)^2 &= \underbrace{\left(W\left(\overline{0}\right)\right)^2}_{\substack{=0 \\ \text{(since Lemma 5.8.20} \\ \text{yields } W\left(\overline{0}\right)=0\text{)}}} + \sum_{\substack{d \in \mathbb{Z}/p; \\ d \neq \overline{0}}} \left(W\left(d\right)\right)^2 = \sum_{\substack{d \in \mathbb{Z}/p; \\ d \neq \overline{0}}} \left(W\left(d\right)\right)^2 \\
&= \sum_{\substack{d \in \mathbb{Z}/p; \\ d \neq \overline{0}; \\ d \text{ is a square}}} \underbrace{\left(W\left(d\right)\right)^2}_{\substack{=\left(W\left(\overline{1}\right)\right)^2 \\ \text{(by Lemma 5.8.23 \textbf{(a)})}}} + \underbrace{\sum_{\substack{d \in \mathbb{Z}/p; \\ d \neq \overline{0}; \\ d \text{ is not a square}}}}_{\substack{= \sum\limits_{\substack{d \in \mathbb{Z}/p; \\ d \text{ is not a square} \\ \text{(since the condition ``}d \neq \overline{0}\text{'' follows from the} \\ \text{condition ``}d \text{ is not a square''}\text{)}}}} \underbrace{\left(W\left(d\right)\right)^2}_{\substack{=\left(W\left(g\right)\right)^2 \\ \text{(by Lemma 5.8.23 \textbf{(b)})}}} \\
&= \sum_{\substack{d \in \mathbb{Z}/p; \\ d \neq \overline{0}; \\ d \text{ is a square}}} \left(W\left(\overline{1}\right)\right)^2 + \sum_{\substack{d \in \mathbb{Z}/p; \\ d \text{ is not a square}}} \left(W\left(g\right)\right)^2 \\
&= \underbrace{\left|\left\{d \in \mathbb{Z}/p \mid d \neq \overline{0}, \text{ and } d \text{ is a square}\right\}\right|}_{\substack{=(\text{number of nonzero squares in } \mathbb{Z}/p) \\ =(p-1)/2 \\ \text{(by Proposition 5.8.3 \textbf{(a)})}}} \cdot \left(W\left(\overline{1}\right)\right)^2 \\
&\quad + \underbrace{\left|\left\{d \in \mathbb{Z}/p \mid d \text{ is not a square}\right\}\right|}_{\substack{=(\text{number of elements of } \mathbb{Z}/p \text{ that are not squares}) \\ =(p-1)/2 \\ \text{(by Proposition 5.8.3 \textbf{(c)})}}} \cdot \left(W\left(g\right)\right)^2 \\
&= \left(\left(p-1\right)/2\right) \cdot \left(W\left(\overline{1}\right)\right)^2 + \left(\left(p-1\right)/2\right) \cdot \left(W\left(g\right)\right)^2 \\
&= \frac{p-1}{2}\left(\left(W\left(\overline{1}\right)\right)^2 + \left(W\left(g\right)\right)^2\right).
\end{aligned}$$

This proves Lemma 5.8.24. □

Lemma 5.8.25. Let $x, y \in \mathbb{Z}/p$. Then,

$$\sum_{d \in \mathbb{Z}/p} K_p\left(\left(x^2+d\right)\left(y^2+d\right)\right) = -1 + \begin{cases} p, & \text{if } x^2 = y^2; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. Write the residue classes x and y as $x = \overline{a}$ and $y = \overline{b}$ for some $a, b \in \mathbb{Z}$. Let $k := b^2 - a^2 \in \mathbb{Z}$. Thus, in $\mathbb{Z}/p$, we have $\overline{k} = \overline{b^2 - a^2} = \overline{b}^2 - \overline{a}^2 = y^2 - x^2$ (since $\overline{a} = x$ and $\overline{b} = y$).

The map

$$\begin{aligned} \mathbb{Z}/p &\to \mathbb{Z}/p, \\ v &\mapsto v - y^2 \end{aligned}$$

is a bijection. Hence, we can substitute $v - y^2$ for d in the sum $\sum_{d \in \mathbb{Z}/p} K_p\left(\left(x^2+d\right)\left(y^2+d\right)\right)$. Thus, we find

$$\begin{aligned}
&\sum_{d \in \mathbb{Z}/p} K_p\left(\left(x^2+d\right)\left(y^2+d\right)\right) \\
&= \sum_{v \in \mathbb{Z}/p} K_p\left(\underbrace{\left(x^2+\left(v-y^2\right)\right)}_{=v-\left(y^2-x^2\right)} \underbrace{\left(y^2+\left(v-y^2\right)\right)}_{=v}\right) \\
&= \sum_{v \in \mathbb{Z}/p} K_p\left(\underbrace{\left(v-\left(y^2-x^2\right)\right) v}_{=v\left(v-\left(y^2-x^2\right)\right)}\right) = \sum_{v \in \mathbb{Z}/p} K_p\left(v\left(v-\underbrace{\left(y^2-x^2\right)}_{=\overline{k}}\right)\right) \\
&= \sum_{v \in \mathbb{Z}/p} K_p\left(v\left(v-\overline{k}\right)\right) = \sum_{i=0}^{p-1} K_p\left(\underbrace{\overline{i}\left(\overline{i}-\overline{k}\right)}_{=\overline{i(i-k)}}\right) \\
&\qquad \left(\begin{array}{c} \text{here, we have substituted } \overline{i} \text{ for } v \text{ in the sum,} \\ \text{since the map } \{0,1,\ldots,p-1\} \to \mathbb{Z}/p \text{ that} \\ \text{sends each } i \text{ to } \overline{i} \text{ is a bijection} \end{array}\right) \\
&= \sum_{i=0}^{p-1} \underbrace{K_p\left(\overline{i\left(i-k\right)}\right)}_{\substack{=\left(\dfrac{i(i-k)}{p}\right) \\ \text{(by (133))}}} = \sum_{i=0}^{p-1} \left(\frac{i\left(i-k\right)}{p}\right) \\
&= \begin{cases} p-1, & \text{if } p \mid k; \\ -1, & \text{if } p \nmid k \end{cases} \qquad \text{(by Proposition 5.8.11)} \\
&= \begin{cases} p-1, & \text{if } p \mid k; \\ -1, & \text{otherwise} \end{cases} \\
&= -1 + \begin{cases} p, & \text{if } p \mid k; \\ 0, & \text{otherwise.} \end{cases} \qquad (139)
\end{aligned}$$

However, the statement "$p \mid k$" is equivalent to "$x^2 = y^2$" (because we have the following chain of logical equivalences:

$$\begin{aligned}
(p \mid k) &\iff \left(\overline{k} = \overline{0} \text{ in } \mathbb{Z}/p\right) \\
&\iff \left(y^2 - x^2 = \overline{0} \text{ in } \mathbb{Z}/p\right) \qquad \left(\text{since } \overline{k} = y^2 - x^2\right) \\
&\iff \left(y^2 = x^2\right) \iff \left(x^2 = y^2\right)
\end{aligned}$$

). Thus, we can rewrite (139) as

$$\sum_{d\in\mathbb{Z}/p} K_p\left(\left(x^2+d\right)\left(y^2+d\right)\right) = -1 + \begin{cases} p, & \text{if } x^2 = y^2; \\ 0, & \text{otherwise.} \end{cases}$$

This proves Lemma 5.8.25. □

Lemma 5.8.26. We have

$$\sum_{d\in\mathbb{Z}/p} \left(W\left(d\right)\right)^2 = p\left(p-1\right)\left(1+\left(-1\right)^{(p-1)/2}\right).$$

Proof. For each $d \in \mathbb{Z}/p$, we have

$$\begin{aligned}
\left(W\left(d\right)\right)^2 &= \left(\sum_{u\in\mathbb{Z}/p} K_p\left(u\left(u^2+d\right)\right)\right)^2 \qquad \text{(by the definition of } W\left(d\right)\text{)} \\
&= \left(\sum_{u\in\mathbb{Z}/p} K_p\left(u\left(u^2+d\right)\right)\right)\left(\sum_{u\in\mathbb{Z}/p} K_p\left(u\left(u^2+d\right)\right)\right) \\
&= \left(\sum_{x\in\mathbb{Z}/p} K_p\left(x\left(x^2+d\right)\right)\right)\left(\sum_{y\in\mathbb{Z}/p} K_p\left(y\left(y^2+d\right)\right)\right) \\
&\qquad \text{(here, we have renamed both summation indices)} \\
&= \sum_{(x,y)\in(\mathbb{Z}/p)^2} \underbrace{K_p\left(x\left(x^2+d\right)\right)\cdot K_p\left(y\left(y^2+d\right)\right)}_{\substack{=K_p\left(x\left(x^2+d\right)\cdot y\left(y^2+d\right)\right) \\ \text{(by Lemma 5.8.18,} \\ \text{applied to } u=x\left(x^2+d\right) \text{ and } v=y\left(y^2+d\right)\text{)}}} \\
&= \sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p\left(\underbrace{x\left(x^2+d\right)\cdot y\left(y^2+d\right)}_{=(xy)\left(\left(x^2+d\right)\left(y^2+d\right)\right)}\right) \\
&= \sum_{(x,y)\in(\mathbb{Z}/p)^2} \underbrace{K_p\left(\left(xy\right)\left(\left(x^2+d\right)\left(y^2+d\right)\right)\right)}_{\substack{=K_p(xy)\cdot K_p\left(\left(x^2+d\right)\left(y^2+d\right)\right) \\ \text{(by Lemma 5.8.18)}}} \\
&= \sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p\left(xy\right)\cdot K_p\left(\left(x^2+d\right)\left(y^2+d\right)\right).
\end{aligned}$$

Summing this equality over all $d \in \mathbb{Z}/p$, we obtain

$$\begin{aligned}
\sum_{d\in\mathbb{Z}/p} \left(W\left(d\right)\right)^2 &= \sum_{d\in\mathbb{Z}/p} \sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p\left(xy\right) \cdot K_p\left(\left(x^2+d\right)\left(y^2+d\right)\right) \\
&= \sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p\left(xy\right) \underbrace{\sum_{d\in\mathbb{Z}/p} K_p\left(\left(x^2+d\right)\left(y^2+d\right)\right)}_{=-1+\begin{cases} p, & \text{if } x^2=y^2; \\ 0, & \text{otherwise} \end{cases}} \\
&\qquad \text{(by Lemma 5.8.25)} \\
&= \sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p\left(xy\right) \left(-1 + \begin{cases} p, & \text{if } x^2=y^2; \\ 0, & \text{otherwise} \end{cases}\right) \\
&= \sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p\left(xy\right)\left(-1\right) + \sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p\left(xy\right) \begin{cases} p, & \text{if } x^2=y^2; \\ 0, & \text{otherwise.} \end{cases}
\end{aligned}$$

Let us now simplify the two sums on the right hand side separately. First, we note that

$$\begin{aligned}
\sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p\left(xy\right)\left(-1\right) &= -\sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p\left(xy\right) \\
&= -\sum_{x\in\mathbb{Z}/p} \sum_{y\in\mathbb{Z}/p} \underbrace{K_p\left(xy\right)}_{=K_p(x)\cdot K_p(y)} \\
&\qquad \text{(by Lemma 5.8.18)} \\
&= -\sum_{x\in\mathbb{Z}/p} \sum_{y\in\mathbb{Z}/p} K_p\left(x\right)\cdot K_p\left(y\right) \\
&= -\sum_{x\in\mathbb{Z}/p} K_p\left(x\right) \underbrace{\sum_{y\in\mathbb{Z}/p} K_p\left(y\right)}_{=\sum_{u\in\mathbb{Z}/p} K_p(u)=0} \\
&\qquad \text{(by Lemma 5.8.17)} \\
&= -\underbrace{\sum_{x\in\mathbb{Z}/p} K_p\left(x\right) 0}_{=0} = 0.
\end{aligned}$$

The second sum is not much trickier by now. We have

$$\sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p(xy) \begin{cases} p, & \text{if } x^2 = y^2; \\ 0, & \text{otherwise} \end{cases}$$

$$= \sum_{\substack{(x,y)\in(\mathbb{Z}/p)^2; \\ x^2=y^2}} K_p(xy)\, p \qquad \left(\begin{array}{c} \text{since all the addends in this sum are } 0 \\ \text{except for those with } x^2 = y^2 \end{array} \right)$$

$$= \sum_{\substack{(x,y)\in(\mathbb{Z}/p)^2; \\ x^2=y^2; \\ y=0}} K_p\left(\underbrace{xy}_{\substack{=0 \\ (\text{since } y=0)}} \right) p + \sum_{\substack{(x,y)\in(\mathbb{Z}/p)^2; \\ x^2=y^2; \\ y\neq 0}} K_p(xy)\, p$$

$$= \sum_{\substack{(x,y)\in(\mathbb{Z}/p)^2; \\ x^2=y^2; \\ y=0}} \underbrace{K_p(0)}_{\substack{=0 \\ (\text{by Lemma 5.8.15 } \textbf{(a)})}} p + \sum_{\substack{(x,y)\in(\mathbb{Z}/p)^2; \\ x^2=y^2; \\ y\neq 0}} K_p(xy)\, p$$

$$= \underbrace{\sum_{\substack{(x,y)\in(\mathbb{Z}/p)^2; \\ x^2=y^2; \\ y=0}} 0p}_{=0} + \sum_{\substack{(x,y)\in(\mathbb{Z}/p)^2; \\ x^2=y^2; \\ y\neq 0}} K_p(xy)\, p$$

$$= \sum_{\substack{(x,y)\in(\mathbb{Z}/p)^2; \\ x^2=y^2; \\ y\neq 0}} K_p(xy)\, p = \sum_{\substack{y\in\mathbb{Z}/p; \\ y\neq 0}} \underbrace{\sum_{\substack{x\in\mathbb{Z}/p; \\ x^2=y^2}} K_p(xy)\, p}_{\substack{=1+(-1)^{(p-1)/2} \\ (\text{by Lemma 5.8.19})}}$$

$$= \sum_{\substack{y\in\mathbb{Z}/p; \\ y\neq 0}} \left(1 + (-1)^{(p-1)/2}\right) p = (p-1)\left(1 + (-1)^{(p-1)/2}\right) p$$

(since this sum has $p-1$ addends).

Now, we combine all we have found: We have

$$\sum_{d\in\mathbb{Z}/p} (W(d))^2 = \underbrace{\sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p(xy)\,(-1)}_{=0} + \underbrace{\sum_{(x,y)\in(\mathbb{Z}/p)^2} K_p(xy) \begin{cases} p, & \text{if } x^2 = y^2; \\ 0, & \text{otherwise} \end{cases}}_{=(p-1)\left(1+(-1)^{(p-1)/2}\right)p}$$

$$= (p-1)\left(1 + (-1)^{(p-1)/2}\right) p = p(p-1)\left(1 + (-1)^{(p-1)/2}\right).$$

This proves Lemma 5.8.26. □

Proof of Theorem 5.8.13. We have $4 \mid p-1$ (since $p \equiv 1 \bmod 4$), so that $(p-1)/2$ is even. Thus, $(-1)^{(p-1)/2} = 1$.

Comparing the equalities (132) and (136), we see that

$$W\left(\overline{h}\right) = W(h) \qquad \text{for each } h \in \mathbb{Z}.$$

Thus, in particular, $W\left(\overline{1}\right) = W\left(1\right) = a$ and $W\left(\overline{m}\right) = W\left(m\right) = b$. Moreover, $\overline{m} \in \mathbb{Z}/p$ is not a square (by the definition of m).

Lemma 5.8.26 yields

$$\sum_{d \in \mathbb{Z}/p} \left(W\left(d\right)\right)^2 = p\left(p-1\right)\left(1 + \underbrace{\left(-1\right)^{\left(p-1\right)/2}}_{=1}\right) = p\left(p-1\right)\left(1+1\right) = 2p\left(p-1\right).$$

Hence,

$$2p\left(p-1\right) = \sum_{d \in \mathbb{Z}/p} \left(W\left(d\right)\right)^2 = \frac{p-1}{2}\left(\left(W\left(\overline{1}\right)\right)^2 + \left(W\left(\overline{m}\right)\right)^2\right)$$

(by Lemma 5.8.24, applied to $g = \overline{m}$). Dividing both sides of this equality by $2\left(p-1\right)$, we obtain

$$p = \frac{1}{4}\left(\left(\underbrace{W\left(\overline{1}\right)}_{=a}\right)^2 + \left(\underbrace{W\left(\overline{m}\right)}_{=b}\right)^2\right) = \frac{1}{4}\left(a^2+b^2\right) = \left(a/2\right)^2 + \left(b/2\right)^2.$$

This proves Theorem 5.8.13 **(b)**.

(a) We have $a = W\left(\overline{1}\right)$, which is even (by Lemma 5.8.21). Also, we have $b = W\left(\overline{m}\right)$, which is even (by Lemma 5.8.21). Thus, Theorem 5.8.13 **(a)** is proven. □

Of course, Theorem 5.8.13 gives a new proof of Theorem 2.16.1 (because Theorem 5.8.13 **(a)** shows that $a/2$ and $b/2$ are integers, and Theorem 5.8.13 **(b)** shows that p is the sum of the squares of these two integers).

Some curious variants of Theorem 5.8.13 have been found recently by Chan, Long and Yang [ChLoYa11] and less recently by Whiteman [Whitem52]; I suspect that there is more to be discovered.

Exercise 5.8.9. Make the same assumptions and definitions as in Theorem 5.8.13.

(a) Prove that $a/2$ is odd, but $b/2$ is even.

(b) Now assume that $p \equiv 1 \bmod 8$. Prove that $b/2$ is divisible by 4, and thus we have $p = x^2 + 16y^2$ for $x = a/2$ and $y = b/8$.

Exercise 5.8.10. Make the same assumptions and definitions as in Theorem 5.8.13. Prove that

$$W\left(h\right) \equiv -h^{\left(p-1\right)/4}\binom{\left(p-1\right)/2}{\left(p-1\right)/4} \bmod p \qquad \text{for any } h \in \mathbb{Z}.$$

6. Polynomials II

We shall now resume the study of polynomials.

Convention 6.0.1. We fix a commutative ring R. This convention will remain in force for the entire chapter.

6.1. Multivariate polynomials again

Let us repeat Theorem 4.5.9 (in a slightly shortened version):

Theorem 6.1.1. Let $m \in \mathbb{N}$. Let $b \in R[x]$ be a polynomial of degree m such that its leading coefficient $[x^m] b$ is a unit. Then, each element of $R[x]/b$ can be uniquely written in the form

$$a_0\overline{x^0} + a_1\overline{x^1} + \cdots + a_{m-1}\overline{x^{m-1}} \qquad \text{with } a_0, a_1, \ldots, a_{m-1} \in R.$$

Equivalently, the m vectors $\overline{x^0}, \overline{x^1}, \ldots, \overline{x^{m-1}}$ form a basis of the R-module $R[x]/b$. Thus, this R-module $R[x]/b$ is free of rank $m = \deg b$. If $m > 0$, then the ring $R[x]/b$ contains "a copy of R".

Thus we understand quotients of univariate polynomials rings rather well when the leading coefficient is a unit. They are less predictable when it is not a unit. If R is a field, however, then the leading coefficient of a nonzero polynomial $b \in R[x]$ is always a unit, so we don't need to worry about this issue.

But can we do this with multivariate polynomials?

Consider, for example, the two-variable polynomial ring $R[x,y]$. How does $R[x,y]/b$ look like for a polynomial $b \in R[x,y]$? Keep in mind that the "idea" behind quotienting out b is that we are setting b to 0. So $R[x,y]/b$ is "the ring of polynomials in x and y subject to the assumption that $b(x,y) = 0$".

Let us first try to answer this question for some special polynomials b; we will then look for a pattern. There is a lot to be learned from the examples.

6.1.1. Example 1: $R[x,y]/y$

What is $R[x,y]/y$? We expect this to be isomorphic to $R[x]$, because setting y to 0 in a polynomial $f(x,y)$ should give $f(x,0) \in R[x]$.

This is indeed true, and the formal proof is essentially just a formalization of this informal argument:

Proposition 6.1.2. We have $R[x,y]/y \cong R[x]$ as R-algebras.

Proof. Define a map

$$\begin{aligned} \alpha : R[x,y]/y &\to R[x], \\ \overline{f} &\mapsto f(x,0). \end{aligned}$$

First, we need to check that this map α is well-defined. In other words, we need to check the following:

> *Claim 1:* If $f, g \in R[x,y]$ are two polynomials satisfying $\overline{f} = \overline{g}$ in $R[x,y]/y$, then $f(x,0) = g(x,0)$.

[*Proof of Claim 1:* Let $f, g \in R[x,y]$ be two polynomials satisfying $\overline{f} = \overline{g}$ in $R[x,y]/y$. Then, $\overline{f} = \overline{g}$ means that $f - g \in yR[x,y]$; in other words, $f - g = yp$ for some polynomial $p \in R[x,y]$. Consider this p. Now, evaluating both sides of the equality $f - g = yp$ at $(x,0)$ (that is, substituting 0 for y) yields $f(x,0) - g(x,0) = 0p(x,0) = 0$ and thus $f(x,0) = g(x,0)$. This proves Claim 1.]

Having proved Claim 1, we thus know that the map α is well-defined. It is straightforward to see that α is an R-algebra morphism (because the map $R[x,y] \to R[x]$, $f \mapsto f(x,0)$ is an R-algebra morphism[179]).

In the opposite direction, define a map

$$\begin{aligned} \beta : R[x] &\to R[x,y]/y, \\ g &\mapsto \overline{g[x]}. \end{aligned}$$

It is again clear that this is an R-algebra morphism.

Now, we shall show that the maps α and β are mutually inverse. To prove this, we need to check that $\alpha \circ \beta = \mathrm{id}$ and $\beta \circ \alpha = \mathrm{id}$. Checking $\alpha \circ \beta = \mathrm{id}$ is the easy part. The "hard part" is showing that $\beta \circ \alpha = \mathrm{id}$. There are two ways to do this:

[*First proof of $\beta \circ \alpha = \mathrm{id}$:* To show this, we need to prove that $(\beta \circ \alpha)\left(\overline{f}\right) = \overline{f}$ for each $f \in R[x,y]$. So let us fix an $f \in R[x,y]$. Then,

$$\begin{aligned} (\beta \circ \alpha)\left(\overline{f}\right) &= \beta\left(\alpha\left(\overline{f}\right)\right) \\ &= \beta(f(x,0)) && \left(\text{since } \alpha\left(\overline{f}\right) \text{ was defined to be } f(x,0)\right) \\ &= \overline{(f(x,0))[x]} && (\text{by the definition of } \beta) \\ &= \overline{f(x,0)} && (\text{since } (f(x,0))[x] = f(x,0)). \end{aligned}$$

Thus, it remains to show that $\overline{f(x,0)} = \overline{f}$ (because we want to show that $(\beta \circ \alpha)\left(\overline{f}\right) = \overline{f}$). In other words, it remains to show that $f - f(x,0) \in yR[x,y]$.

[179] This is a particular case of Theorem 4.2.11.

We do this directly: Write f in the form $f = \sum_{i,j \in \mathbb{N}} a_{i,j} x^i y^j$ (with $a_{i,j} \in R$). Then,

$$f(x,0) = \sum_{i,j \in \mathbb{N}} a_{i,j} x^i 0^j = \sum_{i \in \mathbb{N}} a_{i,j} x^i \underbrace{0^0}_{=1} + \sum_{\substack{i,j \in \mathbb{N}; \\ j>0}} a_{i,j} x^i \underbrace{0^j}_{\substack{=0 \\ (\text{since } j>0)}}$$

$$\left(\begin{array}{c} \text{here, we have split the sum into two parts:} \\ \text{one that contains all terms with } j = 0 \\ \text{and one that contains all terms with } j > 0 \end{array} \right)$$

$$= \sum_{i \in \mathbb{N}} a_{i,j} x^i = \sum_{\substack{i,j \in \mathbb{N}; \\ j=0}} a_{i,j} x^i y^j \qquad \left(\text{since } y^j = 1 \text{ for } j = 0 \right).$$

Subtracting this from $f = \sum_{i,j \in \mathbb{N}} a_{i,j} x^i y^j$, we find

$$f - f(x,0) = \sum_{i,j \in \mathbb{N}} a_{i,j} x^i y^j - \sum_{\substack{i,j \in \mathbb{N}; \\ j=0}} a_{i,j} x^i y^j = \sum_{\substack{i,j \in \mathbb{N}; \\ j>0}} a_{i,j} x^i \underbrace{y^j}_{\substack{=yy^{j-1} \\ (\text{we can do this} \\ \text{because } j>0)}}$$

$$= \sum_{\substack{i,j \in \mathbb{N}; \\ j>0}} a_{i,j} x^i y y^{j-1} = y \sum_{\substack{i,j \in \mathbb{N}; \\ j>0}} a_{i,j} x^i y^{j-1} \in yR[x,y],$$

as we wanted to prove. Thus, $\overline{f(x,0)} = \overline{f}$, so that $(\beta \circ \alpha)\left(\overline{f}\right) = \overline{f(x,0)} = \overline{f}$. This proves $\beta \circ \alpha = \mathrm{id}$.]

[*Second proof of $\beta \circ \alpha = \mathrm{id}$:* Here is a more "cultured" proof. We know that β and α are R-algebra morphisms, hence are R-linear maps. Thus, $\beta \circ \alpha$ and id are two R-linear maps from $R[x,y]/y$ to $R[x,y]/y$. Our goal is to prove that these two R-linear maps $\beta \circ \alpha$ and id are equal. As we have learned in Theorem 3.8.3, there is a shortcut for proving that two R-linear maps are equal: It suffices to pick a family of vectors that spans the domain (in our case, the R-module $R[x,y]/y$), and to show that the two maps agree on the vectors of this family. In our case, there is a rather natural choice of such a family: the family of monomials, or rather of their cosets. That is, we choose the family $\left(\overline{x^i y^j}\right)_{i,j \in \mathbb{N}}$. This family spans the R-module $R[x,y]/y$ (since the family $\left(x^i y^j\right)_{i,j \in \mathbb{N}}$ spans the R-module $R[x,y]$, and since the canonical projection onto $R[x,y]/y$ clearly preserves their spanning property). Thus, we only need to show that the two maps $\beta \circ \alpha$ and id agree on the vectors of this family – i.e., to show that

$$(\beta \circ \alpha)\left(\overline{x^i y^j}\right) = \mathrm{id}\left(\overline{x^i y^j}\right) \qquad \text{for any } i,j \in \mathbb{N}.$$

But this is straightforward: We fix $i,j \in \mathbb{N}$, and set out to show that $(\beta \circ \alpha)\left(\overline{x^i y^j}\right) = \mathrm{id}\left(\overline{x^i y^j}\right)$. If $j > 0$, then $\overline{x^i y^j} = 0$ (since $x^i y^j \in yR[x,y]$ in this case) and therefore

both $(\beta \circ \alpha)\left(\overline{x^i y^j}\right)$ and $\mathrm{id}\left(\overline{x^i y^j}\right)$ must be 0 in this case (since R-linear maps always send 0 to 0). If, on the other hand, $j = 0$, then $\overline{x^i y^j} = \overline{x^i y^0} = \overline{x^i}$ and therefore $\alpha\left(\overline{x^i y^j}\right) = \alpha\left(\overline{x^i}\right) = x^i$ (since substituting 0 for y does not change the monomial x^i) and thus $(\beta \circ \alpha)\left(\overline{x^i y^j}\right) = \beta\left(x^i\right) = \overline{x^i} = \overline{x^i y^j} = \mathrm{id}\left(\overline{x^i y^j}\right)$. Hence, in both cases, we have shown that $(\beta \circ \alpha)\left(\overline{x^i y^j}\right) = \mathrm{id}\left(\overline{x^i y^j}\right)$. This completes the proof of $\beta \circ \alpha = \mathrm{id}$.]

Either way, we have now shown that $\beta \circ \alpha = \mathrm{id}$. Combined with $\alpha \circ \beta = \mathrm{id}$, this yields that the two maps α and β are mutually inverse. Thus, α is an invertible R-algebra morphism, hence an R-algebra isomorphism. This proves Proposition 6.1.2. □

We can easily generalize this to multiple variables:

Proposition 6.1.3. For any $n > 0$, we have

$$R\left[x_1, x_2, \ldots, x_n\right] / x_n \cong R\left[x_1, x_2, \ldots, x_{n-1}\right] \text{ as } R\text{-algebras.}$$

Proof. Same idea as for Proposition 6.1.2, but requiring more subscripts to juggle. □

6.1.2. Example 2: $R[x,y] / \left(x^2 + y^2 - 1\right)$

How does $R[x,y] / \left(x^2 + y^2 - 1\right)$ look like?

This is a fairly useful R-algebra; it can be viewed as the algebra of polynomial functions on the unit circle. Indeed, any element $\overline{f} \in R[x,y] / \left(x^2 + y^2 - 1\right)$ can be "evaluated" at a point (a,b) on the unit circle (meaning, a pair of elements $a, b \in R$ with $a^2 + b^2 = 1$).

There are various interesting ring-theoretical questions to be asked about the quotient ring $R[x,y] / \left(x^2 + y^2 - 1\right)$; however, let us restrict ourselves to studying it as an R-module. As an R-module, is $R[x,y] / \left(x^2 + y^2 - 1\right)$ free? What is a basis? This boils down to asking whether (and how) we can divide polynomials with remainder by $x^2 + y^2 - 1$.

Here we will be helped by the following fact:

Proposition 6.1.4. We have

$$R[x,y] \cong (R[x])[y] \qquad \text{as } R\text{-algebras.}$$

More concretely, the map

$$\varphi : R[x,y] \to (R[x])[y],$$

$$\sum_{i,j \in \mathbb{N}} a_{i,j} x^i y^j \mapsto \sum_{j \in \mathbb{N}} \left(\sum_{i \in \mathbb{N}} a_{i,j} x^i \right) y^j \qquad (\text{where } a_{i,j} \in R)$$

is an R-algebra isomorphism.

Proof. First of all, you are excused for wondering what the deal is: Isn't the above map φ just the identity map, since $\sum_{j\in\mathbb{N}} \left(\sum_{i\in\mathbb{N}} a_{i,j} x^i \right) y^j$ is the same polynomial as $\sum_{i,j\in\mathbb{N}} a_{i,j} x^i y^j$ (just rewritten)?

Essentially yes, but there is a technical difference between the rings $R[x,y]$ and $(R[x])[y]$. The former is a polynomial ring in two indeterminates x, y over R, whereas the latter is a polynomial ring in one indeterminate y over the ring $R[x]$. Hence,

- the elements of $R[x,y]$ are polynomials in two variables x, y with coefficients in R, whereas
- the elements of $(R[x])[y]$ are polynomials in one variable y with coefficients in $R[x]$ (that is, their coefficients themselves are polynomials in one variable x over R).

Thus, even if a polynomial in $R[x,y]$ and a polynomial in $(R[x])[y]$ look exactly the same (such as, for example, the polynomials $2x^2y^3$ in both rings), they are technically different. (The polynomial $2x^2y^3$ in $R[x,y]$ has the monomial x^2y^3 appear in it with coefficient 2, whereas the polynomial $2x^2y^3$ in $(R[x])[y]$ has the monomial y^3 appear in it with coefficient $2x^2$.) The map φ thus sends each polynomial in $R[x,y]$ to the identically-looking polynomial in $(R[x])[y]$.

This being said, the claim we are proving is saying precisely that the difference between $R[x,y]$ and $(R[x])[y]$ is only a technicality; in essence the two rings are the same. The proof is rather straightforward. The simplest way is as follows: The map φ defined in the proposition is easily seen to be well-defined and an R-**module** isomorphism. Thus, it remains to prove that this map φ respects multiplication and respects the unity. It is clear enough that φ respects the unity (since the unities of both rings equal x^0y^0), so we only need to check that φ respects multiplication. According to Lemma 4.2.9, it suffices to prove this on a family of vectors that spans the R-module $R[x,y]$; in other words, we only need to find a family $(m_i)_{i\in I}$ of vectors in $R[x,y]$ that spans $R[x,y]$, and show that

$$\varphi(m_i m_j) = \varphi(m_i)\,\varphi(m_j) \qquad \text{for all } i,j \in I.$$

Fortunately, the family of monomials $\left(x^i y^j\right)_{(i,j)\in\mathbb{N}^2}$ is such a family of vectors (even better, it is a basis of the R-module $R[x,y]$); thus, we only need to prove that

$$\varphi\left(x^i y^u \cdot x^j y^v\right) = \varphi\left(x^i y^u\right) \cdot \varphi\left(x^j y^v\right) \qquad \text{for all } (i,u),(j,v) \in \mathbb{N}^2.$$

But this is easy (the left and right hand sides both equal $x^{i+j}y^{u+v} \in (R[x])[y]$). Thus, we conclude that φ respects multiplication; as we said above, this completes the proof of Proposition 6.1.4. □

Now, in view of Proposition 6.1.4, we have the R-algebra isomorphism

$$R[x,y] / \left(x^2+y^2-1\right) \cong (R[x])[y] / \left(x^2+y^2-1\right) \tag{140}$$

(since the isomorphism φ from Proposition 6.1.4 sends the polynomial $x^2+y^2-1 \in R[x,y]$ to the identically-looking polynomial $x^2+y^2-1 \in (R[x])[y]$).

The ring on the right hand side of (140) is a quotient ring of the **univariate** polynomial ring $(R[x])[y]$ modulo the **monic** polynomial $x^2+y^2-1 = y^2 + \underbrace{\left(x^2-1\right)}_{\text{constant term in } R[x]}$ in the variable y. Thus, Theorem 6.1.1 (applied to 2, $R[x]$, y and x^2+y^2-1 instead of m, R, x and b) shows that this quotient ring $(R[x])[y] / \left(x^2+y^2-1\right)$ has a basis $\left(\overline{y^0}, \overline{y^1}\right)$ as an $R[x]$-module. This means that any element of $(R[x])[y] / \left(x^2+y^2-1\right)$ can be uniquely written as

$$\alpha\overline{y^0} + \beta\overline{y^1} \qquad \text{for some } \alpha, \beta \in R[x].$$

Since elements of $R[x]$ themselves can be uniquely written as R-linear combinations of powers of x, we thus conclude that any element of $(R[x])[y] / \left(x^2+y^2-1\right)$ can be uniquely written as

$$\begin{aligned}
&\left(\alpha_0 x^0 + \alpha_1 x^1 + \alpha_2 x^2 + \cdots\right)\overline{y^0} + \left(\beta_0 x^0 + \beta_1 x^1 + \beta_2 x^2 + \cdots\right)\overline{y^1} \\
&= \overline{\left(\alpha_0 x^0 + \alpha_1 x^1 + \alpha_2 x^2 + \cdots\right) y^0 + \left(\beta_0 x^0 + \beta_1 x^1 + \beta_2 x^2 + \cdots\right) y^1} \\
&= \alpha_0\overline{x^0y^0} + \alpha_1\overline{x^1y^0} + \alpha_2\overline{x^2y^0} + \cdots + \beta_0\overline{x^0y^1} + \beta_1\overline{x^1y^1} + \beta_2\overline{x^2y^1} + \cdots
\end{aligned}$$

for some $\alpha_0, \alpha_1, \alpha_2, \ldots, \beta_0, \beta_1, \beta_2, \ldots \in R$ (with all but finitely many of these coefficients $\alpha_0, \alpha_1, \alpha_2, \ldots, \beta_0, \beta_1, \beta_2, \ldots$ being 0).

Thus, as an R-module, $(R[x])[y] / \left(x^2+y^2-1\right)$ has a basis

$$\left(\overline{x^0y^0}, \overline{x^1y^0}, \overline{x^2y^0}, \ldots, \overline{x^0y^1}, \overline{x^1y^1}, \overline{x^2y^1}, \ldots\right).$$

In view of the R-algebra isomorphism (140) (which sends each $\overline{x^iy^j}$ to $\overline{x^iy^j}$), we can thus conclude that, as an R-module, $R[x,y] / \left(x^2+y^2-1\right)$ has a basis

$$\left(\overline{x^0y^0}, \overline{x^1y^0}, \overline{x^2y^0}, \ldots, \overline{x^0y^1}, \overline{x^1y^1}, \overline{x^2y^1}, \ldots\right). \tag{141}$$

6.1.3. Indeterminates one at a time

We digress from our series of examples in order to make a few comments about Proposition 6.1.4. We first observe the following:

Proposition 6.1.5. The map $\varphi : R[x,y] \to (R[x])[y]$ from Proposition 6.1.4 is not just an R-algebra isomorphism, but also an $R[x]$-algebra isomorphism. Here, we view $R[x,y]$ as an $R[x]$-algebra via the ring morphism

$$\begin{aligned} R[x] &\to R[x,y], \\ f &\mapsto f[x]. \end{aligned}$$

Proof. LTTR. (It only needs to be shown that $\varphi(fg) = f\varphi(g)$ for any $f \in R[x]$ and $g \in R[x,y]$.) □

The order in which we list the variables doesn't matter much in a polynomial ring; thus, Proposition 6.1.4 has the following analogue (which is proved similarly):

Proposition 6.1.6. We have

$$R[x,y] \cong (R[y])[x] \qquad \text{as } R\text{-algebras.}$$

More concretely, the map

$$\begin{aligned} &\varphi : R[x,y] \to (R[y])[x], \\ &\sum_{i,j\in\mathbb{N}} a_{i,j}x^i y^j \mapsto \sum_{i\in\mathbb{N}} \left(\sum_{j\in\mathbb{N}} a_{i,j}y^j\right) x^i \qquad \left(\text{where } a_{i,j} \in R\right) \end{aligned}$$

is an R-algebra isomorphism.

Again, this isomorphism is an $R[y]$-algebra isomorphism (similarly to Proposition 6.1.5).

Proposition 6.1.4 can also be generalized to more than 2 variables:

Proposition 6.1.7. For any $n > 0$, we have

$$R[x_1, x_2, \ldots, x_n] \cong (R[x_1, x_2, \ldots, x_{n-1}])[x_n] \text{ as } R\text{-algebras.}$$

More concretely, the map

$$\begin{aligned} &\varphi : R[x_1, x_2, \ldots, x_n] \to (R[x_1, x_2, \ldots, x_{n-1}])[x_n], \\ &\sum_{(i_1,i_2,\ldots,i_n)\in\mathbb{N}^n} a_{i_1,i_2,\ldots,i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} \mapsto \sum_{j\in\mathbb{N}} \left(\sum_{(i_1,i_2,\ldots,i_{n-1})\in\mathbb{N}^{n-1}} a_{i_1,i_2,\ldots,i_{n-1},j} x_1^{i_1} x_2^{i_2} \cdots x_{n-1}^{i_{n-1}}\right) x_n^j \\ &\qquad\qquad \left(\text{where } a_{i_1,i_2,\ldots,i_n} \in R\right) \end{aligned}$$

is an R-algebra isomorphism.

Proof. Generalize the proof of Proposition 6.1.4 (same idea, more subscripts). □

As in Proposition 6.1.5, the map φ in Proposition 6.1.7 is not just an R-algebra isomorphism but also an $R[x_1, x_2, \ldots, x_{n-1}]$-algebra isomorphism.

6.1.4. More examples?

Having understood the R-modules $R[x,y]/y$ and $R[x,y]/\left(x^2+y^2-1\right)$, we move on to further examples.

How does $R[x,y]/(xy)$ look like? We cannot answer this using the methods used above, since the polynomial xy is neither monic in y when considered as a polynomial in $(R[x])[y]$ nor monic in x when considered as a polynomial in $(R[y])[x]$.

What about $R[x,y]/(xy(x-y))$? Can we divide $(x+y)^3$ by $xy(x-y)$ with remainder? What is the remainder? Should we replace x^2y by xy^2 or vice versa?

To make things more complicated (but also more useful), let's not forget that we can quotient a ring by an ideal, not just by a single element. Even if R is a field, the polynomial ring $R[x,y]$ is not a PID (unlike $R[x]$ for a field R), so not every ideal is principal.

The following shorthand will be useful:

Definition 6.1.8. Let S be a commutative ring. Let $a_1, a_2, \ldots, a_k$ be elements of S. Then, the ideal $a_1S + a_2S + \cdots + a_kS$ (this is the set of all S-linear combinations of $a_1, a_2, \ldots, a_k$) is called **the ideal generated by** $a_1, a_2, \ldots, a_k$. The quotient ring $S/(a_1S + a_2S + \cdots + a_kS)$ will be denoted by $S/(a_1, a_2, \ldots, a_k)$.

(Many authors actually write $(a_1, a_2, \ldots, a_k)$ for the ideal $a_1S + a_2S + \cdots + a_kS$, but this risks confusion since $(a_1, a_2, \ldots, a_k)$ also means the k-tuple.)

Informally, $S/(a_1, a_2, \ldots, a_k)$ is what is obtained from S if you set all of $a_1, a_2, \ldots, a_k$ to 0.

For an example, we can look at $R[x,y]/(x+y, x-y)$. This behaves differently depending on R:

- If $R = \mathbb{Q}$, then

$$R[x,y]/(x+y,x-y) = \mathbb{Q}[x,y]/(x+y,x-y) = \mathbb{Q}[x,y]/(x,y)$$

(since it is easy to see that the $\mathbb{Q}[x,y]$-linear combinations of $x+y$ and $x-y$ are precisely the $\mathbb{Q}[x,y]$-linear combinations of x and y), and thus

$$R[x,y]/(x+y,x-y) = \mathbb{Q}[x,y]/(x,y) \cong \mathbb{Q}.$$

- If $R = \mathbb{Z}/2$, then

$$\begin{aligned} R[x,y] / (x+y, x-y) &= (\mathbb{Z}/2)[x,y] / \left(\underbrace{x+y}_{\substack{=x-y \\ \text{(since we are in} \\ \text{characteristic 2)}}}, x-y \right) \\ &= (\mathbb{Z}/2)[x,y] / (x-y, x-y) \\ &= (\mathbb{Z}/2)[x,y] / (x-y) \cong (\mathbb{Z}/2)[x]. \end{aligned}$$

We can easily come up with more complicated examples:

- What is $R[x,y,z] / \left(x^2 - yz, y^2 - zx, z^2 - xy\right)$? What lies in the ideal $\left(x^2 - yz\right) R[x,y,z] + \left(y^2 - zx\right) R[x,y,z] + \left(z^2 - xy\right) R[x,y,z]$?
- What is $R[x,y,z] / \left(x^2 + xy, y^2 + yz, z^2 + zx\right)$? What lies in the ideal $\left(x^2 + xy\right) R[x,y,z] + \left(y^2 + yz\right) R[x,y,z] + \left(z^2 + zx\right) R[x,y,z]$? For example, I claim that z^4 lies in this ideal, but z^3 does not. How do I know? How can you tell?

In theory, you could imagine that there are ideals that do not even have a finite list of elements generating them. There are rings that have such ideals. For example, the polynomial ring $\mathbb{Z}[x_1, x_2, x_3, \ldots]$ in infinitely many variables has such ideals (see Exercise 6.1.1 below). But polynomial rings in finitely many variables over a field are not this bad. Indeed:

Theorem 6.1.9 (Hilbert's basis theorem)**.** Let F be a field. Let S be the polynomial ring $F[x_1, x_2, \ldots, x_n]$ for some $n \in \mathbb{N}$. Then, any ideal I of S is finitely generated (this means that there is a finite list $(a_1, a_2, \ldots, a_k)$ of elements of I such that $I = a_1 S + a_2 S + \cdots + a_k S$).

Proof. See [DumFoo04, §9.6, Corollary 22] or [Laurit09, Corollary 5.4.8] or (for a more general result) [Swanso17, Theorem 36.12]. □

Warning 6.1.10. If $n = 1$, then the ideal I in Theorem 6.1.9 is principal (since $F[x_1]$ is a PID), so you can get by with a length-1 list (i.e., with $k = 1$). However, if $n = 2$, then the list can be arbitrarily large. You cannot always find a length-2 list. For example, in the polynomial ring $F[x,y]$, the ideal generated by all monomials of degree p (that is, by $x^p, x^{p-1}y, x^{p-2}y^2, \ldots, y^p$) cannot be generated by p or fewer elements.

Exercise 6.1.1. Let S_∞ be the polynomial ring $\mathbb{Z}[x_1, x_2, x_3, \ldots]$ in infinitely many variables. Strictly speaking, we have never defined this ring, but you can easily produce its definition: It still is a monoid ring, but each monomial now has the form $x_1^{a_1} x_2^{a_2} x_3^{a_3} \cdots$ for some infinite sequence $(a_1, a_2, a_3, \ldots)$ of nonnegative integers with the property that only finitely many of the exponents a_k are nonzero. (Thus, there are infinitely many indeterminates, but each single monomial can only use finitely many of them. For instance, infinite monomials like $x_1 x_2 x_3 \cdots$ are not allowed. As a consequence, a polynomial in S_∞ must also use only a finite set of indeterminates.)

Let J be the set of all polynomials in S_∞ whose constant term (i.e., coefficient of the monomial $x_1^0 x_2^0 x_3^0 \cdots$) is 0.

(a) Show that J is an ideal of S_∞.

(b) Show that J is not an ideal generated by any finite list of elements of S_∞.

6.2. Degrees and the deg-lex order

Let us now attempt a more general approach.

Convention 6.2.1. From now on, for the rest of this chapter, we fix a commutative ring R and an $n \in \mathbb{N}$.

We let P denote the polynomial ring $R[x_1, x_2, \ldots, x_n]$.

As we recall, a **monomial** is an element of the free abelian monoid $C^{(n)}$ with n generators $x_1, x_2, \ldots, x_n$; it has the form $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ for some $(a_1, a_2, \ldots, a_n) \in \mathbb{N}^n$.

6.2.1. Degrees

Our first goal is to define the degree of a polynomial in n variables. We begin by defining the degree of a monomial:

Definition 6.2.2. The **degree** of a monomial $\mathfrak{m} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \in C^{(n)}$ is defined to be the number $a_1 + a_2 + \cdots + a_n \in \mathbb{N}$. It is denoted by $\deg \mathfrak{m}$.

For example, the monomial $x_1^5 x_2 x_4^2 = x_1^5 x_2^1 x_3^0 x_4^2$ has degree $5 + 1 + 0 + 2 = 8$.

Definition 6.2.3. A monomial $\mathfrak{m}$ is said to **appear** in a polynomial $f \in P$ if $[\mathfrak{m}] f \neq 0$. (Recall that $[\mathfrak{m}] f$ means the coefficient of $\mathfrak{m}$ in f.)

For example, the monomial $x^2 y$ appears in $(x + y)^3 \in R[x, y]$ (if $3 \neq 0$ in R), but the monomial xy does not.

Definition 6.2.4. The **degree** (or **total degree**) of a nonzero polynomial $f \in P$ is the largest degree of a monomial that appears in f.

For example:

- The polynomial $(x+y+1)^3 \in \mathbb{Q}[x,y]$ has degree 3.
- The polynomial $(x+y+1)^3 - (x+y)^3 \in \mathbb{Q}[x,y]$ has degree 2, since it equals $3x^2+3y^2+6xy+3x+3y+1$.
- The polynomial $\left(x+y+\overline{1}\right)^3 - (x+y)^3 \in (\mathbb{Z}/3)[x,y]$ has degree 0, since it equals $\overline{1}$.

Definition 6.2.4 generalizes our old definition of degree for nonzero univariate polynomials.

The following proposition generalizes a fact that we previously proved for univariate polynomials (parts **(a)** and **(c)** of Proposition 4.3.5):

Proposition 6.2.5 (Degree-of-a-product formula)**.** Let R be a commutative ring. Let $p, q \in P$ be nonzero.

(a) We have $\deg(pq) \leq \deg p + \deg q$.

(b) We have $\deg(pq) = \deg p + \deg q$ if R is an integral domain.

Part **(a)** of this proposition is pretty clear. (The reason is that $\deg(\mathfrak{mn}) = \deg \mathfrak{m} + \deg \mathfrak{n}$ for any monomials $\mathfrak{m}, \mathfrak{n}$.)

What about part **(b)**? We proved this for univariate polynomials using leading coefficients. What is a leading coefficient when several monomials can have the same degree? In order to define it, we need to break ties (i.e., establish an ordering on monomials of equal degrees) in a way that will be compatible with products[180]. To that aim, we shall introduce a total order on the set $C^{(n)}$ of all monomials.

6.2.2. The deg-lex order

Recall that a **total order** (or, to be more precise, a **strict total order**) on a set S is a binary relation $\prec$ on S that is

- **asymmetric** (meaning that no two elements a and b of S satisfy $a \prec b$ and $b \prec a$ at the same time);
- **transitive** (meaning that if $a, b, c \in S$ satisfy $a \prec b$ and $b \prec c$, then $a \prec c$);

[180] I will explain what this means later.

- **trichotomous** (meaning that for any two elements a and b of S, we have $a \prec b$ or $a = b$ or $b \prec a$).

Here are some examples of total orders:

- The relation $<$ on the set $\mathbb{N}$ or on the set $\mathbb{Z}$ or on the set $\mathbb{R}$ is a total order.
- So is the relation $>$ on each of these three sets.
- If S is a finite set, and if $(s_1, s_2, \ldots, s_k)$ is a list of all elements of S, with each element of S appearing exactly once in this list, then we can define a total order $\prec$ on S as follows: We declare that two elements $u, v \in S$ satisfy $u \prec v$ if and only if u appears prior to v in this list $(s_1, s_2, \ldots, s_k)$ (that is, if $u = s_i$ and $v = s_j$ for some $i < j$).
- On the other hand, the relation $\subseteq$ on the power set $\mathcal{P}(X)$ of a set X is not a total order unless $|X| \leq 1$. (Indeed, it is asymmetric and transitive, but not trichotomous, because if α and β are two distinct elements of X, then we have neither $\{\alpha\} \subseteq \{\beta\}$ nor $\{\alpha\} = \{\beta\}$ nor $\{\beta\} \subseteq \{\alpha\}$.)

If $\prec$ is a total order on a set S, then we view relations of the form $a \prec b$ as saying that a is in some sense smaller than b. We will use the notations $\preccurlyeq$, $\succ$ and $\succcurlyeq$ accordingly; this means that

- we write "$a \preccurlyeq b$" for "$a \prec b$ or $a = b$".
- we write "$a \succ b$" for "$b \prec a$".
- we write "$a \succcurlyeq b$" for "$a \succ b$ or $a = b$".

So we all know a total order on the set $\mathbb{R}$ of all real numbers. But what about other sets? For example, how can we find a total order on the set of words in the English language? A long time ago, creators of dictionaries and encyclopedias were faced with this very problem, because it would be hard to look a word up in a dictionary if there was no well-known total order in which the words appeared in the dictionary. The total order commonly used in dictionaries is known as the **lexicographic order** (or **dictionary order**): Words are ordered by their first letter (e.g., "ant" $\prec$ "bear"); ties are broken using the second letter ("ant" $\prec$ "armadillo"); remaining ties are broken using the third letter ("camel" $\prec$ "cat"); and so on; absent letters at the end are treated as being smaller than present letters (e.g., "ant" $\prec$ "anteater"). We use this as an inspiration for defining a total order on $C^{(n)}$, but we shall use the degree as the first level of comparison.

Definition 6.2.6. We define a total order $\prec$ (called the **degree-lexicographic order**, or – for short – the **deg-lex order**) on the set $C^{(n)}$ of all monomials as follows:

For two monomials $\mathfrak{m} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ and $\mathfrak{n} = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$, we declare that $\mathfrak{m} \prec \mathfrak{n}$ if and only if

- **either** $\deg \mathfrak{m} < \deg \mathfrak{n}$;
- **or** $\deg \mathfrak{m} = \deg \mathfrak{n}$ and the following holds: There is an $i \in \{1, 2, \ldots, n\}$ such that $a_i \neq b_i$, and the **smallest** such i satisfies $a_i < b_i$.

In words:

- If two monomials have different degrees, then we declare the monomial with smaller degree to be the smaller one.
- If they have equal degrees, then we look at the first variable that has different exponents in the two monomials, and we declare the monomial with the smaller exponent on this variable to be smaller.

For example:

- We have $x_1^2 \prec x_2 x_3^2$, since $\deg\left(x_1^2\right) = 2 < 3 = \deg\left(x_2 x_3^2\right)$.
- We have $x_1^5 x_2 x_3 x_4^2 \prec x_1^5 x_2 x_3^2 x_4$, since the two monomials have the same degree, and the first variable that has different exponents in these two monomials is x_3, and this variable appears with a smaller exponent in $x_1^5 x_2 x_3 x_4^2$ (namely, with exponent 1) than in $x_1^5 x_2 x_3^2 x_4$ (namely, with exponent 2).
- We have $x_1 x_3^2 \prec x_1 x_2 x_3$, since the first variable that has different exponents in these two monomials is x_2, and this variable appears with a smaller exponent in $x_1 x_3^2$ (namely, with exponent 0) than in $x_1 x_2 x_3$ (namely, with exponent 1).
- The reader may easily check that $x_3^3 \prec x_1 x_2 x_3^2 \prec x_1 x_2^2 x_3 \prec x_1^2 x_2 x_3 \prec x_3^5 \prec x_1^2 x_2^2 x_3^2 \prec x_1^6$.

You can intuitively think of the deg-lex order as follows: A monomial becomes larger (in this order) if you increase its degree, and also becomes larger if you replace an x_i factor by an x_j factor with $j < i$.

The deg-lex order has several good properties:

Proposition 6.2.7.

(a) The deg-lex order really is a total order on $C^{(n)}$.

(b) If $\mathfrak{m}, \mathfrak{n}, \mathfrak{p} \in C^{(n)}$ satisfy $\mathfrak{m} \prec \mathfrak{n}$, then $\mathfrak{mp} \prec \mathfrak{np}$.

(c) We have $1 \preccurlyeq \mathfrak{m}$ for any $\mathfrak{m} \in C^{(n)}$.

(d) Let $\mathfrak{m} \in C^{(n)}$ be any monomial. Then, there are only finitely many monomials $\mathfrak{p}$ such that $\mathfrak{p} \prec \mathfrak{m}$.

(e) There are no infinite decreasing chains $\mathfrak{m}_0 \succ \mathfrak{m}_1 \succ \mathfrak{m}_2 \succ \cdots$ of monomials.

(f) If T is a nonempty finite set of monomials, then T has a largest element with respect to $\prec$ (that is, an element $\mathfrak{t} \in T$ such that $\mathfrak{m} \preccurlyeq \mathfrak{t}$ for all $\mathfrak{m} \in T$).

(g) If T is a nonempty set of monomials, then T has a smallest element with respect to $\prec$ (that is, an element $\mathfrak{t} \in T$ such that $\mathfrak{m} \succcurlyeq \mathfrak{t}$ for all $\mathfrak{m} \in T$).

Note that we require T to be finite in Proposition 6.2.7 **(f)** but not in Proposition 6.2.7 **(g)**. This is similar to the situation for sets of nonnegative integers (viz., any nonempty set of nonnegative integers has a smallest element, but only finite nonempty sets of nonnegative integers have largest elements).

Hints to the proof of Proposition 6.2.7. **(a)**, **(b)**, **(c)**, **(d)** LTTR.
(e) This follows from **(d)**.
(f) This holds for any total order on any set.
(g) This is easily proved using **(d)** (or, less easily, using **(e)**). LTTR. □

(Proposition 6.2.7 **(b)** is what I meant when I said that the deg-lex order is "compatible with products".)

6.2.3. Leading coefficients, monomials and terms

Now, we can define leading coefficients of multivariate polynomials:

Definition 6.2.8. Let $f \in P$ be a nonzero polynomial.

(a) The **leading monomial** of f means the largest (with respect to $\prec$) monomial that appears in f. It is denoted by $\operatorname{LM} f$.

(b) The **leading coefficient** of f means the coefficient $[\operatorname{LM} f] f$. It is denoted by $\operatorname{LC} f$.

(c) The **leading term** of f means the product $\operatorname{LC} f \cdot \operatorname{LM} f$. It is denoted by $\operatorname{LT} f$.

For example, if $3 \neq 0$ in R, then

$$\operatorname{LM}\left(\left(x_1+x_2+1\right)^3-x_1^3\right) = x_1^2x_2;$$
$$\operatorname{LC}\left(\left(x_1+x_2+1\right)^3-x_1^3\right) = 3;$$
$$\operatorname{LT}\left(\left(x_1+x_2+1\right)^3-x_1^3\right) = 3x_1^2x_2.$$

Two simple consequences of this definition are:

Proposition 6.2.9. Let $f \in P$ be a nonzero polynomial. Then, $f - \operatorname{LT} f = 0$ or else $\operatorname{LM}\left(f - \operatorname{LT} f\right) \prec \operatorname{LM} f$.

Proof. By Definition 6.2.8, we have

$$f = \operatorname{LT} f + \left(\text{an } R\text{-linear combination of monomials } \mathfrak{m} \text{ with } \mathfrak{m} \prec \operatorname{LM} f\right).$$

Hence, $f - \operatorname{LT} f$ is an R-linear combination of monomials $\mathfrak{m}$ with $\mathfrak{m} \prec \operatorname{LM} f$. Therefore, $f - \operatorname{LT} f = 0$ or else $\operatorname{LM}\left(f - \operatorname{LT} f\right) \prec \operatorname{LM} f$. □

Proposition 6.2.10. Let $f, g \in P$ be nonzero polynomials such that $\operatorname{LC} f$ is not a zero divisor in R. Then,

$$\operatorname{LM}\left(fg\right) = \operatorname{LM} f \cdot \operatorname{LM} g \qquad \text{and} \qquad \operatorname{LC}\left(fg\right) = \operatorname{LC} f \cdot \operatorname{LC} g.$$

Proof. LTTR. (Use Proposition 6.2.7 **(b)**.) □

Now we can easily prove Proposition 6.2.5 **(b)**. (The details are LTTR.)
From Proposition 6.2.5 **(b)**, we obtain the following:

Corollary 6.2.11. If R is an integral domain, then the polynomial ring $P = R\left[x_1, x_2, \ldots, x_n\right]$ is an integral domain.

(Alternatively, this can also be proved by induction on n, using Proposition 6.1.7.)

6.3. Division with remainder and Gröbner bases

By defining leading monomials and leading coefficients, we have recovered one piece of the nice theory of univariate polynomials in the multivariate case. Can we do more? Can we define division with remainder?

6.3.1. The case of principal ideals

We **can** divide with remainder by a single polynomial[181]:

[181] Recall that $P = R\left[x_1, x_2, \ldots, x_n\right]$.

Theorem 6.3.1 (Division-with-remainder theorem for multivariate polynomials)**.** Let $b \in P$ be a nonzero polynomial whose leading coefficient $\operatorname{LC} b$ is a unit of R. Let $a \in P$ be any polynomial.

Then, there is a **unique** pair (q, r) of polynomials in P such that

$$a = qb + r \qquad \text{and} \qquad r \text{ is } \operatorname{LM} b\text{-reduced}.$$

Here, a polynomial $r \in P$ is said to be $\mathfrak{m}$**-reduced** (where $\mathfrak{m}$ is a monomial) if no monomial divisible by $\mathfrak{m}$ appears in r.

This generalizes the division-with-remainder theorem for univariate polynomials (Theorem 4.3.7 **(a)**); indeed, if $n = 1$, then the condition "r is $\operatorname{LM} b$-reduced" is equivalent to "$\deg r < \deg b$" (which is familiar from the case of univariate polynomials). The entries q and r of the pair (q, r) in Theorem 6.3.1 will be called the **quotient** and the **remainder** of the division of a by b.

Let us illustrate Theorem 6.3.1 on an example:

- Let $n = 2$ and $R = \mathbb{Z}$, and let us rename the indeterminates x_1, x_2 as x, y. Thus, $P = \mathbb{Z}[x, y]$. Let $b = xy(x - y) \in P$. Thus, $\operatorname{LM} b = x^2 y$ and $\operatorname{LC} b = 1$.

  Let $a = (x + y)^4$. We want to divide a by b with remainder. That is, we want to find the pair (q, r) in Theorem 6.3.1.

  Theorem 6.3.1 says that a can be written as a multiple of b plus some $\operatorname{LM} b$-reduced polynomial. In other words, it says that by subtracting an appropriate multiple of b from a, we can obtain an $\operatorname{LM} b$-reduced polynomial. How do we find the right multiple to subtract?

  In the univariate case, "$\operatorname{LM} b$-reduced" was simply saying that $\deg r < \deg b$, and we achieved this by repeatedly subtracting multiples of b from a in order to chip away at the leading term (reducing the degree by at least 1 in each step). We can do this similarly in the multivariate case: We simply check whether a is already $\operatorname{LM} b$-reduced. As long as it isn't, we find some monomial divisible by $\operatorname{LM} b$ that appears in a, and we clear it out by subtracting an appropriate multiple of b (so that this monomial no longer appears in a). More precisely, we clear out the highest such monomial that appears in a. We keep doing this until no such monomials remain (which means that a has become $\operatorname{LM} b$-reduced).

  Let us actually do this in our above example: We start with

  $$a = (x + y)^4 = x^4 + 4x^3 y + 6x^2 y^2 + 4xy^3 + y^4.$$

  Two monomials that are multiples of $\operatorname{LM} b = x^2 y$ appear on the right hand side: $x^3 y$ and $x^2 y^2$. The highest of them is $x^3 y$, so we clear it out

by subtracting an appropriate multiple of b. This appropriate multiple is $4xb$, since we want to clear out a $4x^3y$ term. So we get

$$\begin{aligned} a - 4xb &= \left(x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4\right) - 4x \cdot xy\,(x-y) \\ &= x^4 + 10x^2y^2 + 4xy^3 + y^4. \end{aligned}$$

Now we still have one monomial left that is a multiple of $\operatorname{LM} b = x^2y$, namely x^2y^2. We clear it out by subtracting $10yb$, and we end up with

$$\begin{aligned} a - 4xb - 10yb &= \left(x^4 + 10x^2y^2 + 4xy^3 + y^4\right) - 10y \cdot xy\,(x-y) \\ &= x^4 + 14xy^3 + y^4. \end{aligned}$$

The right hand side of this equality is $\operatorname{LM} b$-reduced, so it is the remainder we were looking for. That is, the r in our pair (q, r) is $x^4 + 14xy^3 + y^4$. The q in this pair we find by collecting the multiples of b that we have subtracted; thus, we get $q = 4x + 10y$ (since we have subtracted $4xb$ and $10yb$). Hence, our pair (q, r) is

$$(q, r) = \left(4x + 10y,\ x^4 + 14xy^3 + y^4\right).$$

This example was somewhat simplistic. In more complicated cases, it can happen that subtracting a multiple of b will create new monomials that are not $\operatorname{LM} b$-reduced. However, if we keep following our method, all those new monomials will eventually get removed as well.

Hints to the proof of Theorem 6.3.1. The existence of the pair (q, r) is proved by the same idea as in the example we just did. All we need to do is to explain why our procedure terminates (i.e., doesn't keep running forever). This is not hard: We observe that, as we keep subtracting appropriate multiples of b from a, the **highest** monomial that is a multiple of $\operatorname{LM} b$ and appears in a becomes smaller and smaller (because each subtraction clears out the highest such monomial, and can only introduce lower such monomials). Thus, if our procedure would run forever, then we would obtain an infinite decreasing chain $\mathfrak{m}_0 \succ \mathfrak{m}_1 \succ \mathfrak{m}_2 \succ \cdots$ of monomials; but this would contradict Proposition 6.2.7 **(e)**. Thus, the algorithm eventually terminates, and this proves the existence of (q, r).

To prove the uniqueness of (q, r), it suffices to show that no nonzero multiple of b is $\operatorname{LM} b$-reduced[182]. But this follows easily from Proposition 6.2.10. □

As a consequence of Theorem 6.3.1 (or, more precisely, of the algorithm for the construction of (q, r) that we demonstrated in the above example), we obtain

[182] Indeed, if (q_1, r_1) and (q_2, r_2) are two pairs (q, r) satisfying the claim of Theorem 6.3.1, then $r_1 - r_2 = (q_2 - q_1)\, b$ is a multiple of b that is $\operatorname{LM} b$-reduced (since r_1 and r_2 are $\operatorname{LM} b$-reduced).

an algorithmic way to tell whether a polynomial $a \in P$ is divisible by b or not (whenever $b \in P$ is a nonzero polynomial whose leading coefficient $\operatorname{LC} b$ is a unit of R). Namely, we compute the pair (q, r) from Theorem 6.3.1, and check whether $r = 0$. The uniqueness of this pair easily yields that $b \mid a$ if and only if $r = 0$.

Another consequence of Theorem 6.3.1 is the following corollary that explicitly constructs a basis of the R-module P/b:

Corollary 6.3.2. Let $b \in P$ be a nonzero polynomial whose leading coefficient $\operatorname{LC} b$ is a unit of R. Then, each element of P/b can be uniquely written in the form

$$\sum_{\substack{\mathfrak{m} \text{ is a monomial} \\ \text{not divisible by } \operatorname{LM} b}} a_{\mathfrak{m}} \overline{\mathfrak{m}} \qquad \text{with } a_{\mathfrak{m}} \in R$$

(where all but finitely many $\mathfrak{m}$ satisfy $a_{\mathfrak{m}} = 0$). Equivalently, the family $\left(\overline{\mathfrak{m}}\right)_{\mathfrak{m} \text{ is a monomial not divisible by } \operatorname{LM} b}$ is a basis of the R-module P/b. If b is not constant, then the ring P/b contains "a copy of R".

Corollary 6.3.2 generalizes Theorem 6.1.1 (and is proved in the same way, except that we use Theorem 6.3.1 instead of the univariate division-with-remainder theorem). Here are some examples:

- Let us take $P = R[x, y]$ and $b = y$ in Corollary 6.3.2. Then, $\operatorname{LM} b = y$, so that Corollary 6.3.2 yields that the family $\left(\overline{\mathfrak{m}}\right)_{\mathfrak{m} \text{ is a monomial not divisible by } y}$ is a basis of the R-module $P/b = R[x, y]/y$. Since the monomials not divisible by y are precisely the powers of x (that is, $x^0, x^1, x^2, \ldots$), we can rewrite this as follows: The family $\left(\overline{x^i}\right)_{i \in \mathbb{N}} = \left(\overline{x^0}, \overline{x^1}, \overline{x^2}, \ldots\right)$ is a basis of the R-module $P/b = R[x, y]/y$. This is in line with Proposition 6.1.2 (indeed, the isomorphism $R[x, y]/y \to R[x]$ sends this family to the standard basis $\left(x^0, x^1, x^2, \ldots\right)$ of $R[x]$).

- Let us take $P = R[x, y]$ and $b = x^2 + y^2 - 1$ in Corollary 6.3.2. Then, $\operatorname{LM} b = x^2$, so that Corollary 6.3.2 yields that the family $\left(\overline{\mathfrak{m}}\right)_{\mathfrak{m} \text{ is a monomial not divisible by } x^2}$ is a basis of the R-module $P/b = R[x, y] / \left(x^2 + y^2 - 1\right)$. Since the monomials not divisible by x^2 are precisely the monomials $x^i y^j$ with $i < 2$, we can rewrite this as follows: The family

  $$\left(\overline{x^i y^j}\right)_{(i,j) \in \mathbb{N}^2;\ i<2} = \left(\overline{x^0 y^0}, \overline{x^0 y^1}, \overline{x^0 y^2}, \ldots, \overline{x^1 y^0}, \overline{x^1 y^1}, \overline{x^1 y^2}, \ldots\right)$$

  is a basis of the R-module $P/b = R[x, y] / \left(x^2 + y^2 - 1\right)$. This is not the basis that we obtained back in (141), but rather is obtained from the latter by interchanging x and y. Of course, it is no surprise that interchanging x and y turns a basis into a basis; indeed, the variables x and y clearly play

symmetric roles in $R[x,y] / \left(x^2+y^2-1\right)$, so every basis that treats them unequally has a "mirror" version with x and y interchanged.

- Let us take $P = R[x,y]$ and $b = xy$ in Corollary 6.3.2. Then, $\operatorname{LM} b = xy$, so that Corollary 6.3.2 yields that the family $\left(\overline{\mathfrak{m}}\right)_{\mathfrak{m} \text{ is a monomial not divisible by } xy}$ is a basis of the R-module $P/b = R[x,y] / (xy)$. Since the monomials not divisible by xy are precisely the monomials $1, x^1, x^2, x^3, \ldots, y^1, y^2, y^3, \ldots$ (that is, the monomials that are powers of a single indeterminate), we can rewrite this as follows: The family

$$\left(\overline{1}, \overline{x^1}, \overline{x^2}, \overline{x^3}, \ldots, \overline{y^1}, \overline{y^2}, \overline{y^3}, \ldots\right)$$

is a basis of the R-module $P/b = R[x,y] / (xy)$. This can be obtained in more direct ways, too.

- Likewise, applying Corollary 6.3.2 to $P = R[x,y]$ and $b = xy(x-y)$ yields that the family

$$\begin{aligned}&\left(\overline{\mathfrak{m}}\right)_{\mathfrak{m} \text{ is a monomial not divisible by } x^2y} \\ &= \left(\overline{1}, \overline{x^1}, \overline{x^2}, \overline{x^3}, \ldots, \overline{y^1}, \overline{y^2}, \overline{y^3}, \ldots, \overline{xy^1}, \overline{xy^2}, \overline{xy^3}, \ldots\right)\end{aligned}$$

is a basis of the R-module $R[x,y] / (xy(x-y))$.

Exercise 6.3.1. Consider the setting of Theorem 6.3.1. Prove that the remainder of the division of a by b is the unique $\operatorname{LM} b$-reduced polynomial $p \in P$ that satisfies $a - p \in bP$.

Exercise 6.3.2. Let $R = \mathbb{Z}$, and let us rename the variables x_1, x_2, x_3, x_4 as x, y, z, w. Let n be a positive integer.

(a) Find the remainder of the division of $(x+y)^n$ by $xy(x-y)$.

(b) Find the remainder of the division of x^n by $(x-y)^2$.

(c) Find the remainder of the division of $(xz)^n$ by $(x-y)(z-w)$.

Exercise 6.3.3. Let R be any commutative ring. Let S be the ring $R[x,y] / \left(xy^2\right)$.

(a) Prove that the family

$$\begin{aligned}&\left(\overline{\mathfrak{m}}\right)_{\mathfrak{m} \text{ is a monomial not divisible by } xy^2} \\ &= \left(\overline{1}, \overline{x}, \overline{x^2}, \overline{x^3}, \ldots, \overline{y}, \overline{xy}, \overline{x^2y}, \overline{x^3y}, \ldots, \overline{y^2}, \overline{y^3}, \overline{y^4}, \ldots\right)\end{aligned}$$

is a basis of the R-module S.

(b) Prove that the maps

$$\begin{aligned} & S \to R\left[x\right], \\ & \overline{f} \mapsto f\left[x, 0\right] \qquad (\text{“substituting 0 for } y\text{”}) \end{aligned}$$

and

$$\begin{aligned} & S \to R\left[y\right], \\ & \overline{f} \mapsto f\left[0, y\right] \qquad (\text{“substituting 0 for } x\text{”}) \end{aligned}$$

are R-algebra morphisms.

(c) Assume that R is a field. Prove that the units of S are precisely the elements of the form $\overline{\lambda + xyf}$ for $f \in R\left[x, y\right]$ and $\lambda \in R^{\times}$.

Now, define two elements $a = \overline{x}$ and $b = \overline{x + xy}$ in this ring S.

(d) Prove that $aS = bS$.

(e) Prove that a is not associate to b in S if R is a field. (The notion of “associate” is defined in Definition 2.14.7.)

(f) Conclude that Proposition 2.14.9 becomes false if we don't require R to be an integral domain.

[**Hint:** For part **(c)**, use Exercise 2.5.9 (observing that $\overline{xy} \in S$ is nilpotent) and then show that an element of the form $\overline{f}$ for an xy-reduced polynomial f can only be a unit if f is constant (because otherwise, one of the two morphisms from part **(b)** would send this element to a non-constant univariate polynomial).

For part **(d)**, compute $\overline{x + xy} \cdot \overline{1 - y}$ in S.]

6.3.2. The case of arbitrary ideals

Now what if we want to know how P/I looks like for a non-principal ideal I, say $I = b_1P + b_2P + \cdots + b_kP$ for some $b_1, b_2, \ldots, b_k \in P$? Can we divide a polynomial by I with remainder? Can we check whether a polynomial belongs to I ? (Remember: If $I = bP$ is a principal ideal, then this means checking whether the polynomial is divisible by b. We have seen how to do this using Theorem 6.3.1.)

We can try to replicate the above “division with remainder” logic.

Example 6.3.3. Let $n = 2$, and let us write x, y for the indeterminates x_1, x_2. Let $R = \mathbb{Q}$ (just to be specific), and let $I = b_1P + b_2P$ with

$$\begin{aligned} b_1 &= xy + 1, \\ b_2 &= y + 1. \end{aligned}$$

Let $a \in P$ be any polynomial. We try to divide a by I with remainder. This means writing a in the form $a = i + r$ where $i \in I$ and r is a "remainder". Here, a "**remainder**" (modulo b_1 and b_2) means a polynomial that is both $\operatorname{LM} b_1$-reduced and $\operatorname{LM} b_2$-reduced, i.e., that contains neither multiples of $\operatorname{LM} b_1$ nor multiples of $\operatorname{LM} b_2$ among its monomials. We can achieve this by subtracting multiples of b_1 and multiples of b_2 from a until no such remain. In more detail: Whenever some monomial that is a multiple of $\operatorname{LM} b_1$ appears in our polynomial, we can subtract an appropriate multiple of b_1 from our polynomial to remove this monomial. (Namely, the multiple of b_1 that we choose is the one whose leading term would cancel the multiple of $\operatorname{LM} b_1$ we want to remove from our polynomial.) Similarly we get rid of multiples of $\operatorname{LM} b_2$. When no more monomials that are multiples of $\operatorname{LM} b_1$ or multiples of $\operatorname{LM} b_2$ remain in our polynomial, then we have found our "remainder".

We refer to this procedure as the **division-with-remainder algorithm**. Note that this is a nondeterministic algorithm, in the sense that you often have a choice of which step you make. For instance, if your polynomial contains a monomial that is a multiple of both $\operatorname{LM} b_1$ and $\operatorname{LM} b_2$ at the same time, do you remove it by subtracting a multiple of b_1 or by subtracting a multiple of b_2 ? Thus, the "remainder" at the end might fail to be unique.

Let us check this on a specific example. Let $a = xy - y \in P$. Here is one way to perform our division-with-remainder algorithm:

$$\begin{aligned} a = xy - y &\xrightarrow[\text{to get rid of the } xy \text{ monomial}]{\text{subtract } 1b_1} (xy - y) - (xy + 1) = -y - 1 \\ &\xrightarrow[\text{to get rid of the } y \text{ monomial}]{\text{subtract } -1b_2} (-y - 1) - (-1)(y + 1) = 0. \end{aligned}$$

Here is another way to do it:

$$\begin{aligned} a = xy - y &\xrightarrow[\text{to get rid of the } xy \text{ monomial}]{\text{subtract } xb_2} (xy - y) - x(y + 1) = -x - y \\ &\xrightarrow[\text{to get rid of the } y \text{ monomial}]{\text{subtract } -1b_2} (-x - y) - (-1)(y + 1) = -x - 1. \end{aligned}$$

Both results we have obtained are both $\operatorname{LM} b_1$-reduced and $\operatorname{LM} b_2$-reduced, so they qualify as "remainders" of a modulo b_1 and b_2. However, they are not equal! So the remainder is not unique this time (unlike in Theorem 6.3.1). In particular, the first remainder we obtained was 0, which showed that $a \in I$ (because this remainder was obtained from a by subtracting multiples of b_1 and b_2, and of course these multiples all belong to I); but the second remainder was not 0, thus allowing no such conclusion. So we don't have a sure way of telling whether a polynomial belongs to I or not; if we are unlucky, we get a nonzero remainder even for a polynomial that does belong to I.

This is bad! But it gets even worse:

Example 6.3.4. A simpler example: Let $n = 2$ and $I = b_1P + b_2P$ with

$$b_1 = xy + x,$$
$$b_2 = xy + y.$$

The polynomial $x - y$ lies in I (since $x - y = b_1 - b_2$), but it is both $\operatorname{LM} b_1$-reduced and $\operatorname{LM} b_2$-reduced, so we cannot see this from our division-with-remainder algorithm no matter what choices we make (because the algorithm does nothing: $x - y$ already is a "remainder"). We could, of course, subtract b_1 from $x - y$ (to obtain $(x - y) - (xy + x) = -y - xy$), but this would be a "step backwards", as it would increase the leading monomial (and even the degree) of our polynomial. The idea of the division-with-remainder algorithm is to reduce the polynomial step by step, always "walking downhill", rather than having to "cross a mountain" first (temporarily increasing the leading monomial).

Example 6.3.4 might give you an idea of what is standing in our way here: It is the fact that when we compute $b_1 - b_2$, the leading terms xy cancel. It means, in a sense, that our b_1 and b_2 are "unnecessarily convoluted"; we should perhaps fix this by replacing b_2 by the smaller polynomial $b_2 - b_1 = y - x$. This simplifies b_2 but does not change I (since $b_1P + b_2P = b_1P + (b_2 - b_1)\,P$ [183]). This is similar to one of the row-reduction steps involved in bringing a matrix to row echelon form.

What does it mean in general that a list $(b_1, b_2, \ldots, b_k)$ of polynomials is "unnecessarily convoluted"? The xy cancellation in $b_1 - b_2$ above was easy to see; what other cancellations can lurk in a list of polynomials?

Let me formalize this question. The following definition will be a bit long-winded but it is just giving names to the kind of observations you would have made when trying to discuss the above algorithm:

Definition 6.3.5. Let $\mathbf{b} = (b_1, b_2, \ldots, b_k)$ be a list of nonzero polynomials in P whose leading coefficients are units of R.

(a) Given two polynomials $c, d \in P$, we write $c \xrightarrow[\mathbf{b}]{} d$ (and say "c can be **reduced** to d in a **single step** using $\mathbf{b}$") if

- some monomial $\mathfrak{m}$ appearing in c is a multiple of $\operatorname{LM} b_i$ for some $i \in \{1, 2, \ldots, k\}$;
- we have
$$d = c - \frac{[\mathfrak{m}]\, c}{\operatorname{LC} b_i} \cdot \frac{\mathfrak{m}}{\operatorname{LM} b_i} \cdot b_i.$$

[183] This is a consequence of Exercise 2.11.5 (applied to b_2, $b_2 - b_1$ and b_1P instead of a, b and I).

(This equation essentially says that we obtain d from c by subtracting the appropriate multiple of b_i to get rid of the monomial $\mathfrak{m}$. The multiple is $\dfrac{[\mathfrak{m}]\, c}{\operatorname{LC} b_i} \cdot \dfrac{\mathfrak{m}}{\operatorname{LM} b_i} \cdot b_i$, since the $\dfrac{\mathfrak{m}}{\operatorname{LM} b_i}$ factor is needed to turn the leading monomial of b_i into $\mathfrak{m}$, whereas the $\dfrac{[\mathfrak{m}]\, c}{\operatorname{LC} b_i}$ factor serves to make the coefficient of this monomial the same as that in c. Note that the fraction $\dfrac{[\mathfrak{m}]\, c}{\operatorname{LC} b_i} \in R$ is well-defined since $\operatorname{LC} b_i$ is a unit, whereas the fraction $\dfrac{\mathfrak{m}}{\operatorname{LM} b_i} \in C^{(n)}$ is well-defined since $\mathfrak{m}$ is a multiple of $\operatorname{LM} b_i$.)

For instance, using the notations of Example 6.3.3 and setting $\mathbf{b} = (b_1, b_2)$, we have

$$xy - y \underset{\mathbf{b}}{\longrightarrow} -x - y,$$

because we obtain $-x - y$ from $xy - y$ by subtracting the multiple $1b_1$ of b_1 (which kills the xy monomial). Likewise, for the same $\mathbf{b}$, we have

$$5x^2y^3 \underset{\mathbf{b}}{\longrightarrow} -5xy^2,$$

because we obtain $-5xy^2$ from $5x^2y^3$ by subtracting the multiple $5xy^2b_1$ of b_1 (which kills the x^2y^3 monomial).

(b) Given two polynomials $c, d \in P$, we write $c \underset{\mathbf{b}}{\overset{*}{\longrightarrow}} d$ (and say "c can be **reduced** to d in **many steps** using $\mathbf{b}$") if there is a sequence $(c_0, c_1, \ldots, c_m)$ of polynomials in P such that $c_0 = c$ and $c_m = d$ and

$$c_i \underset{\mathbf{b}}{\longrightarrow} c_{i+1} \qquad \text{for each } i \in \{0, 1, \ldots, m-1\}.$$

Note that this sequence can be trivial (i.e., we can have $m = 0$), in which case of course we have $c = d$. Thus, $c \underset{\mathbf{b}}{\overset{*}{\longrightarrow}} c$ for any $c \in P$. (Like any true algebraists, we understand "many steps" to allow "zero steps".) We also can have $m = 1$; thus, $c \underset{\mathbf{b}}{\overset{*}{\longrightarrow}} d$ holds if $c \underset{\mathbf{b}}{\longrightarrow} d$. (That is, "many steps" allows "one step".)

As an example of a nontrivial many-steps reduction, we observe that using the notations of Example 6.3.3 and setting $\mathbf{b} = (b_1, b_2)$, we have

$$5x^2y^3 \underset{\mathbf{b}}{\longrightarrow} -5xy^2 \underset{\mathbf{b}}{\longrightarrow} 5y \underset{\mathbf{b}}{\longrightarrow} -5$$

and thus $5x^2y^3 \underset{\mathbf{b}}{\overset{*}{\longrightarrow}} -5$.

(c) We say that a polynomial $r \in P$ is **b-reduced** if it is $\operatorname{LM} b_i$-reduced for all $i \in \{1, 2, \ldots, k\}$. This is equivalent to saying that there exists no polynomial $s \in P$ with $r \underset{\mathbf{b}}{\longrightarrow} s$ (that is, "r cannot be reduced any further using $\mathbf{b}$").

(d) A **remainder** of a polynomial $a \in P$ modulo $\mathbf{b}$ means a $\mathbf{b}$-reduced polynomial $r \in P$ such that $a \underset{\mathbf{b}}{\overset{*}{\longrightarrow}} r$. Such a remainder always exists (this is not hard to show), but is not always unique (as we have seen in Example 6.3.3).

(e) We say that the list $\mathbf{b}$ is a **Gröbner basis** if any $a \in P$ has a **unique** remainder modulo $\mathbf{b}$.

(Don't take the word "basis" in "Gröbner basis" to heart. It is closer to "generating set" or "spanning set" than to any sort of "basis" in linear algebra. In particular, a Gröbner basis can be R-linearly dependent or even contain the same polynomial twice.)

So we have seen that not every list of nonzero polynomials is a Gröbner basis. This leads to the following two questions:

- Can we **tell** whether a list of nonzero polynomials is a Gröbner basis? (We cannot afford to check every $a \in P$ and every way of reducing it modulo $\mathbf{b}$.)
- If a list is not a Gröbner basis, can we at least **find** a Gröbner basis that generates the same ideal as the list?

If R is not a field, then the answers to these questions are "no" for reasons that should be familiar from the univariate case (non-unit leading coefficients).

When R is a field, Bruno Buchberger has answered both questions in the positive in the 1960s. The algorithms he found are one of the pillars of modern computer algebra. I will state the main results without proof, but you can find proofs in the literature (e.g., [DumFoo04, §9.6] or [deGraa20, Chapter 1]).

We will need the notion of an **S-polynomial**:

Definition 6.3.6. Let $f, g \in P$ be nonzero polynomials whose leading coefficients are units of R.

Let $\mathfrak{p} = x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n} = \operatorname{LM} f$ and $\mathfrak{q} = x_1^{q_1} x_2^{q_2} \cdots x_n^{q_n} = \operatorname{LM} g$ be their leading monomials, and let $\lambda = \operatorname{LC} f$ and $\mu = \operatorname{LC} g$ be their leading coefficients. So

$$f = \lambda \mathfrak{p} + (\text{smaller terms});$$
$$g = \mu \mathfrak{q} + (\text{smaller terms}).$$

Let

$$\mathfrak{m} = x_1^{\max\{p_1,q_1\}} x_2^{\max\{p_2,q_2\}} \cdots x_n^{\max\{p_n,q_n\}}.$$

(This is the lcm of $\mathfrak{p}$ and $\mathfrak{q}$ among the monomials; it is the smallest-degree monomial that is divisible by both $\mathfrak{p}$ and $\mathfrak{q}$.) Note that $\dfrac{\mathfrak{m}}{\mathfrak{p}}$ and $\dfrac{\mathfrak{m}}{\mathfrak{q}}$ are well-defined monomials (since $\mathfrak{p} \mid \mathfrak{m}$ and $\mathfrak{q} \mid \mathfrak{m}$).

The **S-polynomial** (short for **syzygy polynomial**) of f and g is defined to be the polynomial

$$S(f,g) := \frac{1}{\lambda} \cdot \frac{\mathfrak{m}}{\mathfrak{p}} \cdot f - \frac{1}{\mu} \cdot \frac{\mathfrak{m}}{\mathfrak{q}} \cdot g \in P.$$

Here is the intuition behind this: $S(f,g)$ is the simplest way to form a P-linear combination of f and g in which the leading terms of f and g cancel. Namely, in order to obtain such a P-linear combination, we must first rescale f and g so that their leading coefficients become equal (this can be achieved by scaling f by $\dfrac{1}{\lambda}$ and scaling g by $\dfrac{1}{\mu}$); then we must multiply them with appropriate monomials to make their leading monomials equal (this can be achieved by multiplying f by $\dfrac{\mathfrak{m}}{\mathfrak{p}}$ and multiplying g by $\dfrac{\mathfrak{m}}{\mathfrak{q}}$, so that both leading monomials become $\mathfrak{m}$). The resulting two polynomials have equal leading terms (namely, $\mathfrak{m}$), so their leading terms cancel out when we subtract them. The result of this subtraction is $S(f,g)$. To be more specific, when we multiplied f and g with appropriate monomials to make their leading monomials equal, we made sure to choose the latter monomials as low-degree as possible; this is why we took $\mathfrak{m}$ to be the lcm of $\mathfrak{p}$ and $\mathfrak{q}$ and not some other monomial divisible by $\mathfrak{p}$ and $\mathfrak{q}$ (such as the product $\mathfrak{pq}$).

Example 6.3.7. For $n = 2$ (and denoting x_1, x_2 by x, y as usual), we have

$$S\left(x^2y+1,\ xy^2+1\right) = y\left(x^2y+1\right) - x\left(xy^2+1\right) = y - x$$

and

$$S(xy+1,\ 2x) = 1(xy+1) - \frac{1}{2} \cdot y \cdot 2x = 1$$

and

$$\begin{aligned} S\left(x^2+2x+y,\ y^2+x+2y\right) &= y^2\left(x^2+2x+y\right) - x^2\left(y^2+x+2y\right) \\ &= -x^3 - 2x^2y + 2xy^2 + y^3. \end{aligned}$$

Note that the cancellation of the leading terms in the construction of $S(f,g)$ is precisely the sort of cancellation that prevented us from having a unique remainder in our above examples.

The following crucial theorem says that these cancellations are a canary in the mine: If they don't happen, then the list is a Gröbner basis.

Theorem 6.3.8 (Buchberger's criterion)**.** Let $\mathbf{b} = (b_1, b_2, \ldots, b_k)$ be a list of nonzero polynomials in P whose leading coefficients are units of R.

Then, $\mathbf{b}$ is a Gröbner basis if and only if every $i < j$ satisfy

$$S\left(b_i, b_j\right) \xrightarrow[\mathbf{b}]{*} 0.$$

The idea behind this theorem is that a list of polynomials (whose leading coefficients are units) is a Gröbner basis if and only if any S-polynomial of two polynomials in the list reduces to 0 modulo the list. Note that "reduces to 0 modulo the list" means that there is some way to get the remainder 0 when applying the division-with-remainder algorithm to this S-polynomial; we are not requiring that **every** way of applying the division-with-remainder algorithm to it will give 0. (But this will follow automatically if we have shown that $\mathbf{b}$ is a Gröbner basis.)

Example 6.3.9. Let $n = 2$, and write x, y for x_1, x_2. Let $I = b_1P + b_2P$, where

$$b_1 = xy + 1,$$
$$b_2 = y + 1.$$

We already know from Example 6.3.3 that (b_1, b_2) is not a Gröbner basis, but let us now see this using Buchberger's criterion:

$$S\left(b_1, b_2\right) = 1\left(xy + 1\right) - x\left(y + 1\right) = 1 - x.$$

This polynomial $1 - x$ is already $\mathbf{b}$-reduced (where $\mathbf{b} = (b_1, b_2)$), and it is not 0, so we **don't** have $S\left(b_1, b_2\right) \xrightarrow[\mathbf{b}]{*} 0$. Thus, Theorem 6.3.8 confirms again that our $\mathbf{b}$ is not a Gröbner basis.

Example 6.3.10. Let $n = 3$, and write x, y, z for x_1, x_2, x_3. Let $I = b_1P + b_2P + b_3P$, where

$$b_1 = x^2 - yz,$$
$$b_2 = y^2 - zx,$$
$$b_3 = z^2 - xy.$$

Is $\mathbf{b} := (b_1, b_2, b_3)$ a Gröbner basis? We check this using Buchberger's criterion. First, we rewrite b_1, b_2, b_3 in a way that their leading terms are up

front:

$$\begin{aligned} b_1 &= x^2 - yz, \\ b_2 &= -zx + y^2, \\ b_3 &= -xy + z^2. \end{aligned}$$

(It is generally advised to always write the terms of a polynomial in the deglex order, from highest to lowest, when performing division-with-remainder or computing S-polynomials. Otherwise, it is too easy to get confused about which terms are leading!)

Now, we compute remainders of $S\left(b_i, b_j\right)$ modulo $\mathbf{b}$ for all $i < j$:

- We have

$$\begin{aligned} S\left(b_1, b_2\right) &= S\left(x^2 - yz,\ -zx + y^2\right) \\ &= z\left(x^2 - yz\right) - (-x)\left(-zx + y^2\right) = xy^2 - yz^2 \\ &\xrightarrow[\mathbf{b}]{} \left(xy^2 - yz^2\right) - (-y)\left(-xy + z^2\right) \\ &\qquad \left(\begin{array}{c} \text{here, we subtracted } -yb_3 \\ \text{in order to remove the } xy^2 \text{ monomial} \end{array}\right) \\ &= 0, \end{aligned}$$

  so that $S\left(b_1, b_2\right) \xrightarrow[\mathbf{b}]{*} 0$.

- We have

$$\begin{aligned} S\left(b_1, b_3\right) &= S\left(x^2 - yz,\ -xy + z^2\right) \\ &= y\left(x^2 - yz\right) - (-x)\left(-xy + z^2\right) = xz^2 - y^2z \\ &\xrightarrow[\mathbf{b}]{} \left(xz^2 - y^2z\right) - (-z)\left(-zx + y^2\right) \\ &\qquad \left(\begin{array}{c} \text{here, we subtracted } -zb_2 \\ \text{in order to remove the } xz^2 \text{ monomial} \end{array}\right) \\ &= 0, \end{aligned}$$

  so that $S\left(b_1, b_3\right) \xrightarrow[\mathbf{b}]{*} 0$.

- We have

$$\begin{aligned} S\left(b_2, b_3\right) &= S\left(-zx + y^2,\ -xy + z^2\right) = y\left(-zx + y^2\right) - z\left(-xy + z^2\right) \\ &= y^3 - z^3 \text{ is } \mathbf{b}\text{-reduced and not } 0. \end{aligned}$$

  Thus, we **do not** have $S\left(b_2, b_3\right) \xrightarrow[\mathbf{b}]{*} 0$. This shows that $\left(b_1, b_2, b_3\right)$ is **not** a Gröbner basis.

(This example was a bit unusual in that our many-step reductions were actually one-step reductions. But it is certainly not unusual in that we have wasted a lot of work before getting the answer "no".)

Buchberger's criterion is proved (e.g.) in [DumFoo04, p. 324], in [Laurit09, Theorem 5.6.8] and in [deGraa20, proof of Theorem 1.1.33]. The "only if" part is obvious; the "if" part is interesting.

Gröbner bases help us better understand ideals of P:

Definition 6.3.11. Let I be an ideal of P. A **Gröbner basis of** I means a Gröbner basis $(b_1, b_2, \ldots, b_k)$ that generates I (that is, that satisfies $I = b_1P + b_2P + \cdots + b_kP$).

Corollary 6.3.12 (Macaulay's basis theorem)**.** Let $\mathbf{b} = (b_1, b_2, \ldots, b_k)$ be a list of nonzero polynomials in P whose leading coefficients are units of R. Assume that $\mathbf{b}$ is a Gröbner basis.

Let I be the ideal $b_1P + b_2P + \cdots + b_kP$ of P. Then, each element of P/I can be uniquely written in the form

$$\sum_{\substack{\mathfrak{m} \text{ is a } \mathbf{b}\text{-reduced} \\ \text{monomial}}} a_{\mathfrak{m}} \overline{\mathfrak{m}} \qquad \text{with } a_{\mathfrak{m}} \in R$$

(where all but finitely many $\mathfrak{m}$ satisfy $a_{\mathfrak{m}} = 0$). Equivalently, the family $\left(\overline{\mathfrak{m}}\right)_{\mathfrak{m} \text{ is a } \mathbf{b}\text{-reduced monomial}}$ is a basis of the R-module P/I. If none of the polynomials $b_1, b_2, \ldots, b_k$ is constant, then the ring P/b contains "a copy of R".

Proof. LTTR. □

To summarize: If we know a Gröbner basis of an ideal I of P, then we know a lot about I (in particular, we can tell when a polynomial belongs to I, and we can find a basis for P/I). But how do we find a Gröbner basis of an ideal? Is there always one?

Not for arbitrary R. But if R is a field, then yes:

Theorem 6.3.13 (Buchberger's theorem)**.** Let R be a field. Let I be an ideal of the polynomial ring $P = R[x_1, x_2, \ldots, x_n]$. Then, I has a Gröbner basis.

Moreover, if $b_1, b_2, \ldots, b_k$ are nonzero polynomials such that $I = b_1P + b_2P + \cdots + b_kP$, then we can construct a Gröbner basis of I by the following algorithm (**Buchberger's algorithm**):

- Initially, let $\mathbf{b}$ be the list $(b_1, b_2, \ldots, b_k)$.
- As long as there exist two entries of $\mathbf{b}$ whose S-polynomial has a nonzero remainder modulo $\mathbf{b}$, we append this remainder to the list. (It is enough to compute one remainder for each pair of entries of $\mathbf{b}$.)

- Once no such two entries exist any more, we are done: $\mathbf{b}$ is a Gröbner basis of I.

This algorithm always terminates after finitely many steps (i.e., we don't keep adding new entries to $\mathbf{b}$ forever).

We won't prove this (see, e.g., [deGraa20, Proposition 1.1.35] or [Laurit09, Theorem 5.7.2] for proofs), but we will give examples:

Example 6.3.14. Let $n = 3$, and write x, y, z for x_1, x_2, x_3. Let $I = b_1P + b_2P + b_3P$, where

$$b_1 = x^2 - yz,$$
$$b_2 = y^2 - zx,$$
$$b_3 = z^2 - xy.$$

We want to find a Gröbner basis of this ideal I.

As we have seen in Example 6.3.10, the list $\mathbf{b} := (b_1, b_2, b_3)$ is not a Gröbner basis, since $S(b_2, b_3) = y^3 - z^3$ does not have remainder 0 modulo $\mathbf{b}$. Its remainder is $y^3 - z^3$ itself. Thus, following Buchberger's algorithm, we append this remainder to the list. That is, we set $b_4 = y^3 - z^3$, and continue with the list (b_1, b_2, b_3, b_4). We call this list $\mathbf{b}$ again.

Since $\mathbf{b}$ has grown, we must now also check whether the new S-polynomials

$$S(b_1, b_4), \quad S(b_2, b_4), \quad S(b_3, b_4)$$

reduce to 0 modulo $\mathbf{b}$. Fortunately, they do. Thus, our new list $\mathbf{b} = (b_1, b_2, b_3, b_4)$ is a Gröbner basis of I.

Example 6.3.15. Let $n = 3$, and write x, y, z for x_1, x_2, x_3. Assume that $R = \mathbb{Q}$. Let $I = b_1P + b_2P + b_3P$, where

$$b_1 = x^2 + xy,$$
$$b_2 = y^2 + yz,$$
$$b_3 = z^2 + zx.$$

Then, again, it is not hard to see that (b_1, b_2, b_3) is not a Gröbner basis of I. Using Buchberger's algorithm, we can easily compute its Gröbner basis. For example, I has Gröbner basis

$$\left(x^2 + xy, \quad y^2 + yz, \quad xz + z^2, \quad yz^2 - z^3, \quad z^4\right).$$

(Note that the Gröbner basis of an ideal is not unique, so you might get a different one if you perform Buchberger's algorithm differently. When there

are several pairs $\left(b_i, b_j\right)$ whose S-polynomial does not reduce to 0, you have a choice of which of these pairs you handle first.)

This Gröbner basis reveals that $z^4 \in I$ but $z^3 \notin I$ (since z^3 is reduced modulo the above Gröbner basis). Just working from the original definition of I, this would be far from obvious!

You can do Gröbner basis computations with most computer algebra systems (e.g., SageMath, Mathematica, Singular, SymPy). For example, here is SageMath code for the Gröbner basis of the above ideal. Note that we took $R = \mathbb{Q}$ in this computation (the "`QQ`" means the field of rational numbers), but the same computation works over any field R (and, because our ideal is rather nice, even over any commutative ring R; this is not automatic).

Exercise 6.3.4. Let $n = 3$, and let us rename the indeterminates x_1, x_2, x_3 as x, y, z. Define two polynomials b_1 and b_2 in P by

$$b_1 = x^2 - y \qquad \text{and} \qquad b_2 = x^3 - z.$$

Let $I = b_1 P + b_2 P$. Find a Gröbner basis of I. (Feel free to assume that $R = \mathbb{Q}$ for simplicity.)

Exercise 6.3.5. Let $n = 3$, and write x, y, z for x_1, x_2, x_3. Let $I = b_1 P + b_2 P + b_3 P$, where

$$\begin{aligned} b_1 &= x + xyz, \\ b_2 &= y + xyz, \\ b_3 &= z + xyz. \end{aligned}$$

Find a Gröbner basis of I. (Feel free to assume that $R = \mathbb{Q}$ for simplicity.)

Exercise 6.3.6. Let $n = 3$, and write x, y, z for x_1, x_2, x_3. Let $I = b_1 P + b_2 P + b_3 P$, where

$$\begin{aligned} b_1 &= x^2 + yz, \\ b_2 &= y^2 + zx, \\ b_3 &= z^2 + xy. \end{aligned}$$

Find a Gröbner basis of I. (Feel free to assume that $R = \mathbb{Q}$ for simplicity.)

6.3.3. Monomial orders

We have so far been using the deg-lex order on the monomials. There are many other total orders that share most of its nice properties and are often more suited for specific problems.

Let me only mention the **lexicographic order**, which is defined just as the deg-lex order but without taking the degree into account. That is:

Definition 6.3.16. We define a total order $\prec$ (called the **lexicographic order**, or – for short – the **lex order**) on the set $C^{(n)}$ of all monomials as follows:

For two monomials $\mathfrak{m} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ and $\mathfrak{n} = x_1^{b_1} x_2^{b_2} \cdots x_n^{b_n}$, we declare that $\mathfrak{m} \prec \mathfrak{n}$ if and only if

- there is an $i \in \{1, 2, \ldots, n\}$ such that $a_i \neq b_i$, and the **smallest** such i satisfies $a_i < b_i$.

Several properties of the deg-lex order were collected in Proposition 6.2.7. All of those properties except for Proposition 6.2.7 **(d)** hold for the lex order as well. Proposition 6.2.7 **(d)** fails for the lex order (for $n > 1$), because x_1 is larger (with respect to the lex order) than **any** power of x_2 (and, of course, there are infinitely many powers of x_2). Proposition 6.2.7 **(e)** is still true for the lex order, but its proof is harder. However, the theory of Gröbner bases does not use Proposition 6.2.7 **(d)**, so it still can be done with the lex order. This yields new (in general, different) Gröbner bases.

Example 6.3.17. Let $n = 3$ and let $I = \left(x^2 - y\right) P + \left(y^2 - z\right) P + \left(z^2 - x\right) P$ (where we write x, y, z for x_1, x_2, x_3). Then, a Gröbner basis of I with respect to the deg-lex order is

$$\left(x^2 - y,\ \ y^2 - z,\ \ z^2 - x\right)$$

(this is precisely the list of generators that we started with). But this is not a Gröbner basis with respect to the lex order. Instead, a Gröbner basis of I with respect to the lex order is

$$\left(x - z^2,\ \ y - z^4,\ \ z^8 - z\right).$$

Example 6.3.18. Let $n = 3$ and let $I = \left(x^2 - y^3\right) P + \left(y^4 - z^2\right) P + \left(z^2 - x^5\right) P$ (where we write x, y, z for x_1, x_2, x_3). Then, a Gröbner basis of I with respect to the deg-lex order is

$$\begin{aligned}\Big(&z^6 - yz^2,\ \ x^3z^2 - yz^2,\ \ xy^2z^2 - z^2,\ \ xz^4 - y^2z^2,\\ &yz^4 - xz^2,\ \ x^4 - y^2z^2,\ \ x^2y - z^2,\ \ y^3 - x^2\Big).\end{aligned}$$

But a Gröbner basis of I with respect to the lex order is

$$\left(x^2 - y^3,\ \ xz^2 - z^8,\ \ y^4 - z^2,\ \ yz^2 - z^6,\ \ z^{16} - z^2\right).$$

In the SageMath computer algebra system, you can signal the use of the lex order (as opposed to the deg-lex order, which is used by default) by replacing "`PolynomialRing(QQ)`" by "`PolynomialRing(QQ, order="lex")`".

This last example illustrates one reason to vary the total order on monomials: Gröbner bases can be rather long, even if the ideal is easy to write down. The size of a Gröbner basis can be doubly exponential in the number of generators of I (see [MoSrSa24]). In real life, this worst-case scenario doesn't happen very often, but when it does, switching to a different monomial order will often ameliorate it. (Think of it as a way to re-roll the dice if you got an unlucky roll.)

Exercise 6.3.7. Let $n = 3$, and let us rename the indeterminates x_1, x_2, x_3 as x, y, z. Define two polynomials b_1 and b_2 in P by

$$b_1 = x^2 - yz \qquad \text{and} \qquad b_2 = x - y^2.$$

Let $I = b_1 P + b_2 P$.

(a) Find a Gröbner basis of I with respect to the deg-lex order.

(b) Find a Gröbner basis of I with respect to the lex order.

The following exercise generalizes Example 6.3.17 from $n = 3$ to arbitrary n:

Exercise 6.3.8. Let n be a positive integer. Define n polynomials $b_1, b_2, \ldots, b_n$ in P by setting

$$b_i = x_i^2 - x_{i+1} \qquad \text{for each } i \in \{1, 2, \ldots, n-1\} \qquad \text{and}$$
$$b_n = x_n^2 - x_1.$$

Let $I = b_1 P + b_2 P + \cdots + b_n P$.

(a) Find a Gröbner basis of I with respect to the deg-lex order. (This should go very quick!)

(b) Find a Gröbner basis of I with respect to the lex order.

[**Hint:** For part **(b)**, compute the answer for some small values of n and spot the pattern.]

6.4. Solving polynomial systems using Gröbner bases

Another occasion to use Gröbner bases (and the lex order in particular) is solving systems of polynomial equations. Polynomial equations are closely connected to ideals:

Definition 6.4.1. Let $b_1, b_2, \ldots, b_k$ be k polynomials in P, and let A be a commutative R-algebra. Then, a **root** (or, alternatively, a **common root**) of $(b_1, b_2, \ldots, b_k)$ in A means an n-tuple $(a_1, a_2, \ldots, a_n) \in A^n$ such that

$$b_i(a_1, a_2, \ldots, a_n) = 0 \qquad \text{for all } i \in \{1, 2, \ldots, k\}.$$

This definition generalizes the standard notion of a root of a polynomial to multiple variables and multiple polynomials.

Thus, solving systems of polynomial equations means finding roots of lists of polynomials. It turns out that the list of polynomials doesn't really matter; what does is the ideal it generates:

Proposition 6.4.2. Let $b_1, b_2, \ldots, b_k$ be k polynomials in P, and let A be a commutative R-algebra.

Then, the roots of $(b_1, b_2, \ldots, b_k)$ in A depend only on the ideal generated by $b_1, b_2, \ldots, b_k$, rather than on the polynomials $b_1, b_2, \ldots, b_k$ themselves.

More concretely: If $I = b_1P + b_2P + \cdots + b_kP$ is the ideal of P generated by $b_1, b_2, \ldots, b_k$, then the roots of $(b_1, b_2, \ldots, b_k)$ are precisely the n-tuples $(a_1, a_2, \ldots, a_n) \in A^n$ such that

$$f(a_1, a_2, \ldots, a_n) = 0 \qquad \text{for all } f \in I.$$

Proof. Easy, LTTR. (You have to prove that if $(a_1, a_2, \ldots, a_n) \in A^n$ is a root of $(b_1, b_2, \ldots, b_k)$, then $f(a_1, a_2, \ldots, a_n) = 0$ for all $f \in I$. But this is easy: Each $f \in I$ is a P-linear combination $c_1b_1 + c_2b_2 + \cdots + c_kb_k$ of $(b_1, b_2, \ldots, b_k)$, and therefore satisfies

$$\begin{aligned} & f(a_1, a_2, \ldots, a_n) \\ &= c_1(a_1, a_2, \ldots, a_n) \underbrace{b_1(a_1, a_2, \ldots, a_n)}_{=0} + c_2(a_1, a_2, \ldots, a_n) \underbrace{b_2(a_1, a_2, \ldots, a_n)}_{=0} \\ &\qquad + \cdots + c_k(a_1, a_2, \ldots, a_n) \underbrace{b_k(a_1, a_2, \ldots, a_n)}_{=0} \\ &= 0. \end{aligned}$$

The converse is even more obvious, since the polynomials $b_1, b_2, \ldots, b_k$ all belong to I.) □

Thus, if we want to find the roots of $(b_1, b_2, \ldots, b_k)$, we can replace $(b_1, b_2, \ldots, b_k)$ by any other tuple of polynomials that generates the same ideal of P. (This is just the polynomial analogue of the classical "addition" strategy for solving systems of linear equations.)

One of the most useful ways to do this is to replace $(b_1, b_2, \ldots, b_k)$ by a Gröbner basis of the ideal it generates – particularly, by a Gröbner basis with respect to the lex order. Let us see how this helps on an example:

Example 6.4.3. Recall Exercise 1.5.6:

Solve the following system of equations:

$$a^2 + b + c = 1,$$
$$b^2 + c + a = 1,$$
$$c^2 + a + b = 1$$

for three complex numbers a, b, c.

Let us formalize this in terms of polynomials and roots. We set $R = \mathbb{Q}$ and $n = 3$, and we write x, y, z for x_1, x_2, x_3. Thus, the exercise is asking for the roots of

$$\left(x^2 + y + z - 1,\ \ y^2 + z + x - 1,\ \ z^2 + x + y - 1\right)$$

in the $\mathbb{Q}$-algebra $\mathbb{C}$.

Let I be the ideal of $P = \mathbb{Q}[x, y, z]$ generated by the three polynomials $x^2 + y + z - 1$, $y^2 + z + x - 1$, $z^2 + x + y - 1$. Using a computer (or a lot of patience), we can easily find a Gröbner basis of I with respect to the lex order. We get

$$\left(x + y + z^2 - 1,\ \ y^2 - y - z^2 + z,\ \ yz^2 + \frac{1}{2}z^4 - \frac{1}{2}z^2,\ \ z^6 - 4z^4 + 4z^3 - z^2\right).$$

We observe that the last polynomial in this Gröbner basis only involves the variable z ! Thus, the c entry in each of the solutions (a, b, c) of our system must be a root of this polynomial $z^6 - 4z^4 + 4z^3 - z^2$. We can therefore find all possibilities for c by finding the roots of this polynomial (I am here assuming that you can solve univariate polynomials; we will learn a bit more about this in Section 6.5 perhaps). In our concrete case, we can easily do this:

$$z^6 - 4z^4 + 4z^3 - z^2 = z^2 (z - 1)^2 \left(z^2 + 2z - 1\right).$$

Thus, the options for c are $0, 1, \sqrt{2} - 1, \sqrt{2} + 1$.

Now let us find b. Either we use the symmetry of the original system to argue that the options for b must be the same as for c; or we use the second-to-last polynomial in our Gröbner basis (or the second one) to compute b now that c is known. At last, we get to a in a similar way.

In the end, we get finitely many options for (a, b, c). We need to check which of these options actually are solutions of the original system. This is a lot of work, but a computer can do it.

Of course, there are more elegant ways to solve the above exercise (otherwise, I would not have posed it). However, the way we just showed is generalizable. In general, if a system of polynomial equations over $\mathbb{C}$ has only finitely many solutions, then we can find them all in this way (provided that we have an algo-

rithm for finding all roots of a univariate polynomial).[184] Thus, using Gröbner bases with respect to the lex order, we can (often) reduce solving systems of polynomial equations in multiple variables to solving polynomial equations in a single variable. (See [Laurit09, §5.9] for more details on this.)

Some things don't look like systems of polynomial equations, but yet boil down to such systems. Here is an example:

Example 6.4.4. Recall Exercise 1.5.2:

Simplify $\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}$.

There are various ways of solving this using some creativity or lucky ideas. Let us try to be more methodical here. We set

$$a=\sqrt[3]{2+\sqrt{5}}, \qquad b=\sqrt[3]{2-\sqrt{5}}, \qquad c=\sqrt[3]{2+\sqrt{5}}+\sqrt[3]{2-\sqrt{5}}.$$

Thus, we want to find a simpler expression for c. A good first step would be to find a polynomial whose root c is (since we would then have a chance of finding c by root-finding techniques). We see that a, b, c satisfy the following system of equations:

$$\begin{aligned}\left(a^3-2\right)^2-5&=0,\\ \left(b^3-2\right)^2-5&=0,\\ a+b-c&=0.\end{aligned}$$

(Indeed, the first equation comes from "unraveling" $a=\sqrt[3]{2+\sqrt{5}}$, and likewise for the second; the third comes from the obvious fact that $c=a+b$.)

We try to solve this system using Gröbner bases. Thus, we consider the ideal

$$I:=\left(\left(x^3-2\right)^2-5\right)P+\left(\left(y^3-2\right)^2-5\right)P+(x+y-z)\,P$$

of the polynomial ring $P=\mathbb{Q}[x,y,z]$. Using SageMath, we can easily find a Gröbner basis of this ideal I with respect to the lex order. Its last entry is

[184] If a system of polynomial equations has infinitely many solutions, then this strategy usually will not work. For example, if we try to use it to solve the system

$$\begin{aligned}ab&=0,\\ bc&=0,\\ ca&=0,\end{aligned}$$

then we find the Gröbner basis (xy, yz, xz), which doesn't get us any closer to the solutions. Blame this on the problem, not on the Gröbner basis: The system has a more complicated combinatorial structure (its solution set is the union of the three axes in 3D space; there are infinitely many options for each of a, b, c).

a polynomial that involves only the variable z, so we can narrow down the options for c to the roots of this polynomial.

This looks nice in theory, but in practice you will realize that this last entry is

$$z^{21} - 40z^{18} + 218z^{15} - 72z^{12} - 9931z^9 - 5216z^6 + 19136z^3 - 4096.$$

Eek. With a good computer algebra system, you can factor this polynomial, but there will be some degree-4 factors irreducible over $\mathbb{Q}$. The polynomial has 5 real roots, so c must be one of them, but we need some harder work to find out which one. This is all not very convenient.

But our approach can be salvaged. We have been "throwing away" information about our a, b, c; no wonder that we got so many options for c. Indeed, the equation $\left(a^3 - 2\right)^2 - 5 = 0$ doesn't really mean $a = \sqrt[3]{2 + \sqrt{5}}$; it only means that a is **some** cube root of (2 plus **some** square root of 5). Here, we are using the word "root" in the wider sense, so a nonzero complex number has two square roots and three cube roots; thus, there are 6 possibilities in total for a. Likewise for b. Our system of equations above allows c to be a sum of any of the 6 possible a's with any of the 6 possible b's. Unsurprisingly, this leaves lots of different options for c.

Thus, we need to integrate a bit more information about the actual values of a, b into our system. Of course, we know that a is the **real** cube root of the **positive** square root of 5. But this is not the kind of information we can easily integrate into a system of equations.

However, we can observe that

$$\begin{aligned} ab &= \sqrt[3]{2 + \sqrt{5}} \cdot \sqrt[3]{2 - \sqrt{5}} = \sqrt[3]{\left(2 + \sqrt{5}\right) \cdot \left(2 - \sqrt{5}\right)} \\ &\qquad \left(\text{since } \sqrt[3]{u} \cdot \sqrt[3]{v} = \sqrt[3]{uv} \text{ for any } u, v \in \mathbb{R}\right) \\ &= \sqrt[3]{-1} = -1. \end{aligned}$$

Thus, we can extend our system to

$$\begin{aligned} \left(a^3 - 2\right)^2 - 5 &= 0, \\ \left(b^3 - 2\right)^2 - 5 &= 0, \\ a + b - c &= 0, \\ ab + 1 &= 0. \end{aligned}$$

This is a different system and has a smaller set of solutions than the previous one, but that's good news, since the solution we are looking for is one of its solutions.

Now, solving this new system using the Gröbner basis technique, we find that c is a root of the polynomial $z^3 + 3z - 4$ (since this polynomial is the last

entry of the Gröbner basis we find). But the roots of this polynomial are easy to find: The factorization

$$z^3 + 3z - 4 = (z-1) \underbrace{\left(z^2 + z + 4\right)}_{\text{always positive on } \mathbb{R}}$$

shows that its only real root is 1, so that c must be 1 (since c is real by definition). Thus our exercise is solved.

See [CoLiOs15] for more about solving systems of polynomial equations, and for further applications of Gröbner bases.

6.5. Factorization of polynomials

In Example 6.4.4, we used a computer to factor a polynomial. Let me say some words about the algorithms that are used for this (or, at least, about an algorithm that could theoretically be used for this, but is too slow in practice; actual computers use faster algorithms).

6.5.1. Factoring univariate polynomials

Let F be a field.

Recall that the ring $F[x]$ is a UFD; thus, each polynomial in $F[x]$ has an essentially unique factorization into irreducible polynomials. ("Essentially" means "up to order and up to associates". Keep in mind that the units of $F[x]$ are precisely the nonzero constant polynomials, so that two polynomials $f, g \in F[x]$ are associate if and only if there exists some $\lambda \in F \setminus \{0\}$ satisfying $g = \lambda f$.)

How do we find this factorization (into irreducible polynomials)?

When F is finite, we can just check all possibilities by brute force. Indeed, any factor in the factorization of a nonzero polynomial f must be a polynomial of degree $\leq \deg f$, and this leaves finitely many options for it when F is finite.

For general fields F, there is no algorithm that finds the factorization of every polynomial.[185] But what about well-known fields like $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$?

Over $\mathbb{R}$ and $\mathbb{C}$ you cannot "really" factor polynomials, because this is not a numerically stable problem. For example, the polynomial $x^2 - 2x + 1$ factors over $\mathbb{R}$ (as $(x-1)^2$), but $x^2 - 1.999x + 1$ does not (nontrivially at least). Approximate algorithms that work for sufficiently non-singular inputs exist, but this is more a question of numerical analysis than of algebra.

What about polynomials over $\mathbb{Q}$? There is an algorithm, whose main ingredient is the following fact:

[185] See `https://mathoverflow.net/a/350877/` for an outline of the proof.

Proposition 6.5.1 (Gauss's lemma in one of its forms)**.** Let $f \in \mathbb{Z}[x]$. If f is irreducible in $\mathbb{Z}[x]$, then f is irreducible in $\mathbb{Q}[x]$.

Proof. Assume the contrary. Thus, $f = gh$ for some nonconstant polynomials $g, h \in \mathbb{Q}[x]$ (since the units of $\mathbb{Q}[x]$ are precisely the nonzero constant polynomials). By multiplying the two polynomials g and h with the lowest common denominators of their coefficients, we obtain two nonconstant polynomials u and v in $\mathbb{Z}[x]$. These two polynomials u and v satisfy $uv = Ngh$ for some positive integer N (since u and v are positive integer multiples of g and h). Consider this N. We have $uv = N \underbrace{gh}_{=f} = Nf$, so that $Nf = uv$.

Thus, we have found two nonconstant polynomials $u, v \in \mathbb{Z}[x]$ and a positive integer N such that

$$Nf = uv. \tag{142}$$

We WLOG assume that N is **minimal** with the property such that such u, v exist. (In other words, among all triples (u, v, N) of two nonconstant polynomials $u, v \in \mathbb{Z}[x]$ and a positive integer N satisfying (142), we pick one in which N is minimal. This might not be the one that we obtained from g and h above.)

If $N = 1$, then (142) rewrites as $f = uv$, which contradicts the assumption that f is irreducible (since u and v are nonconstant and thus non-units). Hence, we cannot have $N = 1$. Thus, there exists a prime p that divides N. Consider such a p. Recall that $\mathbb{Z}/p$ is a field (since p is prime). Therefore, $\mathbb{Z}/p$ is an integral domain, so that the polynomial ring $(\mathbb{Z}/p)[x]$ is an integral domain as well (by Corollary 4.3.6).

We shall now show a way to turn any polynomial $s \in \mathbb{Z}[x]$ into a polynomial $\overline{s} \in (\mathbb{Z}/p)[x]$. It is as simple as you can imagine: We simply replace each coefficient by its residue class modulo p. In other words, if $s = s_0x^0 + s_1x^1 + \cdots + s_nx^n$ is a polynomial in $\mathbb{Z}[x]$ (with $s_i \in \mathbb{Z}$), then we define a polynomial $\overline{s} := \overline{s_0}x^0 + \overline{s_1}x^1 + \cdots + \overline{s_n}x^n \in (\mathbb{Z}/p)[x]$ (where $\overline{s_i}$ means the residue class of s_i modulo p). For example, if $p = 5$, then $\overline{2x^3 + 7} = \overline{2}x^3 + \overline{7} = \overline{2}x^3 + \overline{2}$. It is easy to see that the map

$$\begin{aligned} \mathbb{Z}[x] &\to (\mathbb{Z}/p)[x], \\ s &\mapsto \overline{s} \end{aligned}$$

is a ring morphism (since the rules for adding and multiplying polynomials are the same over $\mathbb{Z}$ and over $\mathbb{Z}/p$). Thus, $\overline{uv} = \overline{u} \cdot \overline{v}$.

Now, $f \in \mathbb{Z}[x]$; hence, all coefficients of the polynomial Nf are divisible by N, and thus also divisible by p (since p divides N). Thus, $\overline{Nf} = 0$ in $(\mathbb{Z}/p)[x]$. However, (142) entails $\overline{Nf} = \overline{uv} = \overline{u} \cdot \overline{v}$. Thus, $\overline{u} \cdot \overline{v} = \overline{Nf} = 0$. Since $(\mathbb{Z}/p)[x]$ is an integral domain, this shows that $\overline{u} = 0$ or $\overline{v} = 0$. We WLOG assume that $\overline{u} = 0$ (since otherwise, we can simply swap u with v).

Now, $\overline{u} = 0$ means that all coefficients of u are multiples of p. In other words, $\dfrac{1}{p}u \in \mathbb{Z}[x]$. Now, the equality (142) yields

$$\frac{N}{p}f = \left(\frac{1}{p}u\right)v.$$

Since $\dfrac{N}{p}$ is a positive integer (because p divides N) and since $\dfrac{1}{p}u \in \mathbb{Z}[x]$, this equality shows that $\left(\dfrac{1}{p}u, v, \dfrac{N}{p}\right)$ is a triple of two nonconstant polynomials $\dfrac{1}{p}u, v \in \mathbb{Z}[x]$ and a positive integer $\dfrac{N}{p}$ satisfying (142) (with u and N replaced by $\dfrac{1}{p}$ and $\dfrac{N}{p}$). But recall that among all such triples, we chose (u, v, N) to be one with minimal N. Thus, $N \leq \dfrac{N}{p}$. Therefore, $p \leq 1$ (since N is a positive integer). This contradicts the assumption that p is prime. This contradiction completes the proof. □

Let us now address two computational problems for polynomials with integer or rational coefficients.

> **Problem 1:** Let $f, g \in \mathbb{Z}[x]$ be two polynomials with $g \neq 0$. Check whether g divides f in $\mathbb{Z}[x]$.

Solution (sketched). The leading coefficient of g may or may not be a unit of $\mathbb{Z}$; however, it is always a unit of $\mathbb{Q}$. Thus, we can use division with remainder to check whether g divides f in the (larger) ring $\mathbb{Q}[x]$. If the answer is "no", then (a fortiori) g cannot divide f in $\mathbb{Z}[x]$ (since $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$). If the answer is "yes", then we compute the quotient $\dfrac{f}{g} \in \mathbb{Q}[x]$ and check whether it belongs to $\mathbb{Z}[x]$ (that is, whether its coefficients are integers). If yes, then the answer is "yes"; if no, then the answer is "no". Problem 1 is thus solved. □

> **Problem 2:** Let $f \in \mathbb{Z}[x]$ be a nonzero polynomial. Construct a list of all divisors of f in $\mathbb{Z}[x]$.

Solution (sketched). Let $n = \deg f$. Pick $n+1$ integers $a_0, a_1, \ldots, a_n$ that are **not** roots of f. (Such $n+1$ integers can always be found, since f is a nonzero polynomial of degree n and thus has at most n roots in the integral domain $\mathbb{Z}$. Thus, for example, among the $2n+1$ numbers $-n, -n+1, \ldots, n$, at least $n+1$ many are not roots of f.)

For each $i \in \{0, 1, \ldots, n\}$, let D_i be the set of all divisors of the integer $f[a_i]$ (recall that $f[a]$ is our notation for the evaluation of f at a; this is commonly denoted $f(a)$). This set D_i is finite (since $f[a_i] \neq 0$), and its elements can be

explicitly listed. Hence, the set $D_0 \times D_1 \times \cdots \times D_n$ is finite as well, and its elements can be explicitly listed.

Now, let g be a divisor of f in $\mathbb{Z}[x]$. Then, $g \in \mathbb{Z}[x]$, and there exists a further polynomial $h \in \mathbb{Z}[x]$ such that $f = gh$. Consider this h. From $f = gh$, we obtain $\deg f = \deg(gh) = \deg g + \underbrace{\deg h}_{\geq 0} \geq \deg g$, so that $\deg g \leq \deg f = n$. In other words, the polynomial g must have degree $\leq n$.

For each $i \in \{0, 1, \ldots, n\}$, we have

$$f[a_i] = g[a_i]\, h[a_i] \qquad (\text{since } f = gh)$$

and thus $g[a_i] \mid f[a_i]$, so that $g[a_i] \in D_i$. Hence,

$$(g[a_0],\ g[a_1],\ \ldots,\ g[a_n]) \in D_0 \times D_1 \times \cdots \times D_n.$$

Thus, for each divisor g of f in $\mathbb{Z}[x]$, we know that the $(n+1)$-tuple $(g[a_0],\ g[a_1],\ \ldots,\ g[a_n])$ belongs to the finite set $D_0 \times D_1 \times \cdots \times D_n$ (which does not depend on g and can be explicitly found). Hence, we have finitely many options for this $(n+1)$-tuple.

However, given the $(n+1)$-tuple $(g[a_0],\ g[a_1],\ \ldots,\ g[a_n])$, we can uniquely reconstruct the polynomial g. (Indeed, we know that g has degree $\leq n$, so that Corollary 4.3.27 (applied to g instead of f) yields $g = \sum_{j=0}^{n} g[a_j] \cdot \dfrac{\prod_{k \neq j} (x - a_k)}{\prod_{k \neq j} (a_j - a_k)}$. This is an explicit formula for g in terms of the $(n+1)$-tuple $(g[a_0],\ g[a_1],\ \ldots,\ g[a_n])$. Therefore, given the $(n+1)$-tuple $(g[a_0],\ g[a_1],\ \ldots,\ g[a_n])$ for a divisor g of f, we can uniquely reconstruct g.)

Thus, we have finitely many options for g (since we have finitely many options for this $(n+1)$-tuple). Usually, only few of these options will actually produce a polynomial $g \in \mathbb{Z}[x]$ that divides f (indeed, many of them will produce polynomials with non-integer coefficients; and even among the polynomials that do have integer coefficients, many will fail to divide f). However, we can check which of these options do produce a polynomial $g \in \mathbb{Z}[x]$ that divides f (our above solution to Problem 1 helps here). Thus, we end up with a list of all divisors of f in $\mathbb{Z}[x]$. This solves Problem 2. □

> **Problem 3:** Let $f \in \mathbb{Q}[x]$ be a nonzero polynomial. Find a factorization of f into a product of irreducible polynomials.

Solution sketch. WLOG assume that $f \in \mathbb{Z}[x]$ (otherwise, multiply f with the lowest common denominator of its coefficients). Furthermore, WLOG assume that the gcd of the coefficients of f is 1 (otherwise, divide f by this gcd). We find a list of all divisors of f in $\mathbb{Z}[x]$ (using the solution to Problem 2). If the only such divisors are ± 1 and $\pm f$, then f is irreducible in $\mathbb{Z}[x]$ and thus also irreducible in $\mathbb{Q}[x]$ (by Proposition 6.5.1), so we are done. Else, we find a divisor

g of f that is neither ± 1 nor $\pm f$, and thus we can decompose f as a product gh of two nonconstant polynomials $g, h \in \mathbb{Z}[x]$. In that case, we have reduced the problem to the same problem with the (lower-degree) polynomials g and h. Thus, recursively iterating the procedure, we end up with a factorization of f into a product of irreducible polynomials. □

Our solution to Problem 3 is a theoretical algorithm for factoring a polynomial in $\mathbb{Q}[x]$ into irreducible polynomials. The algorithm is too computationally intensive to be viable in practice, so computers use different methods (often using $\mathbb{Z}/p$ as a stand-in for $\mathbb{Z}$ and using the Chinese Remainder Theorem to "glue" the factorizations over different $\mathbb{Z}/p$'s together).

6.5.2. Factoring multivariate polynomials

Factoring multivariate polynomials over $\mathbb{Q}$ can be done similarly using multivariate Lagrange interpolation[186]. (The word "similarly" is doing some heavy duty here.) Alternatively, it can be reduced to the univariate case by the following trick: If $f \in \mathbb{Q}[x, y]$ is a polynomial of degree $< N$ (for some $N \in \mathbb{N}$), then the univariate polynomial $f\left(x, x^N\right)$ "carries all the information of f" (in the sense that no two different terms of f get merged when we substitute x^N for y). For example, if $f = x^2 + xy + y^2$ and $N = 5$, then

$$f\left(x, x^N\right) = f\left(x, x^5\right) = x^2 + xx^5 + \left(x^5\right)^2 = x^2 + x^6 + x^{10}.$$

Thus, in order to factor f, it suffices to factor $f\left(x, x^N\right)$ (a univariate polynomial), and then try to lift the factorization back by "substituting y for x^N". This trick is justified by the following exercise:

Exercise 6.5.1. Let R be a commutative ring. Let P be the polynomial ring $R[x, y]$. Fix $N \in \mathbb{N}$. Let P_N be the R-submodule

$$\{f \in P \mid f = 0 \text{ or } \deg f < N\}$$

of P. (This is an R-submodule, since it is the span of the family $\left(x^i y^j\right)_{(i,j) \in \mathbb{N}^2;\ i+j<N}$.)

(a) Consider the R-algebra morphism

$$S : P \to R[x],$$
$$f \mapsto f\left(x, x^N\right).$$

(This is the map that substitutes x^N for y in any polynomial $f \in P$. It is an R-algebra morphism, as we know from Theorem 4.2.11.)

Prove that the restriction of S to P_N is injective.

[186] See Exercise 4.3.29 for Lagrange interpolation in the case of 2 variables. The case of n variables is conceptually similar, though there are many more subscripts to deal with.

(b) Assume that R is a field. Let $f \in P_N$ be such that the polynomial $S(f) \in R[x]$ is irreducible. Show that $f \in P = R[x, y]$ is irreducible.

[**Remark:** The converse of part **(b)** does not hold. For example, if $R = \mathbb{Q}$ and $N = 2$, then the polynomial $f := 1 + 2x + y \in P$ is irreducible, but the polynomial $S(f) = 1 + 2x + x^2 = (1 + x)^2 \in R[x]$ is not.]

This trick (of substituting x^N for y) is easily generalized to polynomials in more than two variables. For example, a polynomial in 4 variables x, y, z, w can be transformed into a polynomial in 3 variables x, y, z by substituting z^N for w.

7. Modules over a PID (specifically, over $\mathbb{Z}$)

Modules over a field are rather well-behaved: they are all free, i.e., they have bases and thus are isomorphic to "direct sum powers" of the field.

Modules over an arbitrary ring can be rather wild.

Studying modules over a PID is a middle ground: they are not that wild, but still sufficiently frequent in "real life".

I will just give a taste of their theory. The only PID I will work with is $\mathbb{Z}$, and the only modules I will discuss are finite, but you will see some germs of more general arguments in my brief treatment of this rather special case.

7.1. Classifying finite abelian groups

7.1.1. The classification theorem

Classifying finite groups is notoriously hard. Even the so-called "simple" groups have a classification that spans a page (and takes a dozen of books to prove). The finite **abelian** groups, on the other hand, do have a rather manageable classification:

Theorem 7.1.1 (Classification of finite abelian groups)**.** Let G be a finite abelian group.

(a) Then, G is isomorphic to a direct product of finitely many finite cyclic groups.

In other words, there exist positive integers $n_1, n_2, \ldots, n_k$ such that

$$G \cong (\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_k).$$

(b) Moreover, we can choose these $n_1, n_2, \ldots, n_k$ in such a way that they are > 1 and satisfy

$$n_1 \mid n_2 \mid \cdots \mid n_k.$$

(c) Finally, if we choose them in such a way, then they are unique.

I will outline a proof of parts **(a)** and **(b)** of this theorem using modules over $\mathbb{Z}$. (There are other proofs, e.g., using group theory – see, e.g., [Elman22, Theorem 14.11].) A proof of Theorem 7.1.1 **(c)** is outlined in Exercise 7.1.3 below.

7.1.2. On modules and matrices

How do modules come into play here in the first place? Recall from Proposition 3.4.1 that abelian groups are $\mathbb{Z}$-modules[187]; thus, classifying finite abelian groups is the same as classifying finite $\mathbb{Z}$-modules.

One other thing that will be crucial is good old matrices. Recall from linear algebra that matrices over a field F correspond to linear maps between F-vector spaces. Likewise, matrices over an arbitrary commutative ring R correspond to linear maps between free R-modules. Specifically:

Convention 7.1.2. For any commutative ring R and any $n \in \mathbb{N}$, we identify the n-tuples $(a_1, a_2, \ldots, a_n) \in R^n$ with the column vectors $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \in R^{n \times 1}$. Thus, R^n becomes the R-module $R^{n \times 1}$ of column vectors of size n.

Proposition 7.1.3. Let R be a commutative ring.

(a) If $A \in R^{n \times m}$ is an $n \times m$-matrix over R, then the map

$$\begin{aligned} R^m &\to R^n, \\ v &\mapsto Av \end{aligned} \tag{143}$$

is an R-linear map.

(b) Moreover, any R-linear map from R^m to R^n has the form (143) for a unique $n \times m$-matrix $A \in R^{n \times m}$.

(c) Thus, there is a 1-to-1 correspondence between $n \times m$-matrices over R and linear maps from R^m to R^n.

Proof. As in linear algebra. (See [Grinbe19, Theorem 6.8.4] for part **(a)**, and see [Grinbe19, Proposition 6.8.5] for part **(b)**.) □

Definition 7.1.4. Let R be a commutative ring. Let $A \in R^{n \times m}$ be an $n \times m$-matrix over R.

(a) We set

$$\begin{aligned} \operatorname{Col} A &:= \{Av \mid v \in R^m\} \\ &= (\text{the image of the linear map (143)}) \\ &= (\text{the span of the columns of } A). \end{aligned}$$

[187] and we know from Proposition 3.5.2 that the group morphisms between these abelian groups are exactly the $\mathbb{Z}$-module morphisms

This is an R-submodule of R^n, and is called the **column space** of A. (This is all exactly as in linear algebra.)

(b) The **cokernel** of A is defined to be the quotient R-module $R^n / \operatorname{Col} A$.

Definition 7.1.5. Let R be a commutative ring. An R-module is said to be **finitely presented** if it is isomorphic to the cokernel of some matrix over R.

Remark 7.1.6. This latter definition might appear somewhat random. Here is some intuition for those who know a bit about groups, specifically about their presentations. An R-module is finitely presented if it can be "defined by finitely many generators and finitely many relations". For example, recall that the R-module R^4 can be viewed as the R-module consisting of all "formal" R-linear combinations $ax + by + cz + dw$ of four independent symbols x, y, z, w. Likewise, the R-module

$$R^4 / \operatorname{Col} A \qquad \text{for } A = \begin{pmatrix} 3 & 2 \\ 4 & 7 \\ -5 & 0 \\ -6 & -4 \end{pmatrix}$$

can be expressed as the R-module consisting of all "formal" R-linear combinations $ax + by + cz + dw$ but subject to the relations $3x + 4y = 5z + 6w$ and $2x + 7y = 4w$. Here, the "generators" x, y, z, w are the cosets $e_1 + \operatorname{Col} A$, $e_2 + \operatorname{Col} A$, $e_3 + \operatorname{Col} A$, $e_4 + \operatorname{Col} A$ of the four standard basis elements e_1, e_2, e_3, e_4 of R^4; they satisfy the relations $3x + 4y = 5z + 6w$ and $2x + 7y = 4w$ because we have factored out the submodule

$$\begin{aligned} \operatorname{Col} A &= \operatorname{span}\left(\begin{pmatrix} 3 \\ 4 \\ -5 \\ -6 \end{pmatrix}, \begin{pmatrix} 2 \\ 7 \\ 0 \\ -4 \end{pmatrix} \right) \\ &= \operatorname{span}\left(3e_1 + 4e_2 - 5e_3 - 6e_4, 2e_1 + 7e_2 - 4e_4\right). \end{aligned}$$

7.1.3. Every finite $\mathbb{Z}$-module is finitely presented

Our first step towards the classification theorem is the following:

Lemma 7.1.7. Let G be a finite $\mathbb{Z}$-module. ("Finite" means that the set G is finite.) Then, G is finitely presented.

Proof. The set G is finite and nonempty (since it contains 0); thus, its size $|G|$ is a positive integer. Let us denote this positive integer by n.

The abelian group $(G, +, 0)$ is finite; thus, Lagrange's theorem yields that $|G| \cdot a = 0$ for each $a \in G$. In other words,

$$na = 0 \qquad \text{for each } a \in G \tag{144}$$

(since $n = |G|$).

Let $(m_1, m_2, \ldots, m_n)$ be a list of all the n elements of G (each listed exactly once). Thus, $G = \{m_1, m_2, \ldots, m_n\}$.

Consider the free $\mathbb{Z}$-module $\mathbb{Z}^n$ with its standard basis $(e_1, e_2, \ldots, e_n)$. The map

$$\begin{aligned} f : \mathbb{Z}^n &\to G, \\ (r_1, r_2, \ldots, r_n) &\mapsto r_1 m_1 + r_2 m_2 + \cdots + r_n m_n \end{aligned}$$

is a $\mathbb{Z}$-module morphism (according to Theorem 3.7.9 **(a)**). Moreover, this map f satisfies $f(e_i) = m_i$ for each $i \in \{1, 2, \ldots, n\}$, and thus its image contains all of $m_1, m_2, \ldots, m_n$; thus, this map f is surjective (since $G = \{m_1, m_2, \ldots, m_n\}$). The First isomorphism theorem for modules (Theorem 3.6.8 **(f)**, applied to $M = \mathbb{Z}^n$ and $N = G$) yields

$$\mathbb{Z}^n / \operatorname{Ker} f \cong f(\mathbb{Z}^n) = G \qquad (\text{since } f \text{ is surjective}). \tag{145}$$

Now, we shall construct an $n \times k$-matrix (for some $k \in \mathbb{N}$) satisfying $\operatorname{Ker} f = \operatorname{Col} A$.

Indeed, we consider the following two kinds of vectors in $\mathbb{Z}^n$:

- The **n-stretched basis vectors** shall mean the n vectors $ne_1, ne_2, \ldots, ne_n$. These n vectors belong to $\operatorname{Ker} f$, since each $i \in \{1, 2, \ldots, n\}$ satisfies

$$\begin{aligned} f(ne_i) &= nm_i && (\text{by the definition of } f) \\ &= 0 && (\text{by (144), applied to } a = m_i) \end{aligned}$$

  and thus $ne_i \in \operatorname{Ker} f$.

- The **reduced kernel vectors** shall mean the vectors

$$(r_1, r_2, \ldots, r_n) \in \{0, 1, \ldots, n-1\}^n$$

  that belong to $\operatorname{Ker} f$. There are finitely many such vectors, since the set $\{0, 1, \ldots, n-1\}^n$ is finite.

We have just shown that all n-stretched basis vectors and all reduced kernel vectors belong to $\operatorname{Ker} f$. Hence, any $\mathbb{Z}$-linear combination of n-stretched basis vectors and reduced kernel vectors belongs to $\operatorname{Ker} f$ (because $\operatorname{Ker} f$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}^n$, and thus is closed under linear combination). Conversely, using division with remainder, it is not hard to see that any vector in $\operatorname{Ker} f$ is a

$\mathbb{Z}$-linear combination of n-stretched basis vectors and reduced kernel vectors[188]. Hence, $\operatorname{Ker} f$ is precisely the set of all $\mathbb{Z}$-linear combinations of n-stretched basis vectors and reduced kernel vectors. In other words, $\operatorname{Ker} f$ is the span of the vectors we just mentioned.

Now, let A be the matrix whose columns are precisely the n-stretched basis vectors and the reduced kernel vectors. (This is well-defined, since there are only finitely many of these vectors.) Then, $\operatorname{Col} A$ is the span of the vectors we just mentioned. But we have seen in the previous paragraph that $\operatorname{Ker} f$ is the span of these vectors. Comparing these two results, we conclude that $\operatorname{Ker} f = \operatorname{Col} A$. Hence, (145) rewrites as

$$\mathbb{Z}^n / \operatorname{Col} A \cong G.$$

In other words, G is isomorphic to the cokernel of A. Hence, G is finitely presented. This proves Lemma 7.1.7. □

7.1.4. Understanding cokernels of diagonal matrices

Recall that we still want to prove Theorem 7.1.1 **(a)**, which claims that every finite $\mathbb{Z}$-module G is isomorphic to a direct product of finitely many finite cyclic groups. Lemma 7.1.7 shows that G is finitely presented. How does this help us?

Well, G is finitely presented, i.e., isomorphic to the cokernel of a matrix. If this matrix happens to be diagonal, then we are basically done! Indeed, for

[188] *Proof.* Let $v = (v_1, v_2, \ldots, v_n)$ be a vector in $\operatorname{Ker} f$. We must show that v is a $\mathbb{Z}$-linear combination of n-stretched basis vectors and reduced kernel vectors.

For each $i \in \{1, 2, \ldots, n\}$, we write $v_i = q_i n + r_i$, where q_i and r_i are the quotient and the remainder obtained when dividing v_i by n. Then,

$$\begin{aligned} v = (v_1, v_2, \ldots, v_n) &= (q_1 n + r_1,\ \ q_2 n + r_2,\ \ \ldots,\ \ q_n n + r_n) \\ &= q_1 n e_1 + q_2 n e_2 + \cdots + q_n n e_n + (r_1, r_2, \ldots, r_n), \end{aligned}$$

so that

$$(r_1, r_2, \ldots, r_n) = v - (q_1 n e_1 + q_2 n e_2 + \cdots + q_n n e_n) \in \operatorname{Ker} f$$

(since the vector v as well as all the n vectors $ne_1, ne_2, \ldots, ne_n$ belong to $\operatorname{Ker} f$, and since $\operatorname{Ker} f$ is a $\mathbb{Z}$-submodule of $\mathbb{Z}^n$). Thus, $(r_1, r_2, \ldots, r_n)$ is a reduced kernel vector (since the definition of the r_i as remainders ensures that $r_i \in \{0, 1, \ldots, n-1\}$ for all i, and thus $(r_1, r_2, \ldots, r_n) \in \{0, 1, \ldots, n-1\}^n$). Thus, from

$$v = q_1 n e_1 + q_2 n e_2 + \cdots + q_n n e_n + (r_1, r_2, \ldots, r_n),$$

we conclude that v is a $\mathbb{Z}$-linear combination of n-stretched basis vectors and reduced kernel vectors. Qed.

example, here is how the cokernel of a diagonal 3×3-matrix looks like:

$$\begin{aligned}
&\mathbb{Z}^3 / \operatorname{Col} \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & c \end{pmatrix} \\
&= \mathbb{Z}^3 / \operatorname{span} \left(\begin{pmatrix} a \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ b \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ c \end{pmatrix} \right) \\
&= \mathbb{Z}^3 / \operatorname{span} \left(ae_1, be_2, ce_3 \right) \\
&\qquad\qquad \Big(\text{where } e_1, e_2, e_3 \text{ are the standard basis vectors of } \mathbb{Z}^3 \Big) \\
&\cong (\mathbb{Z}/a) \times (\mathbb{Z}/b) \times (\mathbb{Z}/c) \, .
\end{aligned}$$

(The "$\cong$" sign here is a nice exercise in understanding quotients of modules. Explicitly, it stems from the map

$$\begin{aligned}
\mathbb{Z}^3 / \operatorname{span} \left(ae_1, be_2, ce_3 \right) &\to (\mathbb{Z}/a) \times (\mathbb{Z}/b) \times (\mathbb{Z}/c) \, , \\
\overline{(u, v, w)} &\mapsto (\overline{u}, \overline{v}, \overline{w}) \, ,
\end{aligned}$$

which is easily seen to be a $\mathbb{Z}$-module isomorphism. The intuition is simply that when we take the quotient of the free $\mathbb{Z}$-module $\mathbb{Z}^3$ by its submodule $\operatorname{span} \left(ae_1, be_2, ce_3 \right)$, we end up identifying any two vectors (u, v, w) and (u', v', w') that satisfy $u \equiv u' \bmod a$ and $v \equiv v' \bmod b$ and $w \equiv w' \bmod c$; but this is tantamount to replacing the first entry of our vector by a residue class modulo a, the second by a residue class modulo b, and the third by a residue class modulo c.)

Usually, the matrix whose cokernel we need will be rectangular, not square; however, even for rectangular matrices there is a notion of being diagonal:

Definition 7.1.8. Let R be a ring. A rectangular matrix $A \in R^{n \times m}$ is said to be **diagonal** if its (i, j)-th entry is 0 whenever $i \neq j$.

This is a looser notion of "diagonal" than the one you learnt in linear algebra, since we are not requiring that $n = m$. For example, a diagonal 2×4-matrix looks like $\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \end{pmatrix}$, whereas a diagonal 4×2-matrix looks like $\begin{pmatrix} a & 0 \\ 0 & b \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$.

Proposition 7.1.9. Let $A \in \mathbb{Z}^{n \times m}$ be diagonal. Then, its cokernel $\mathbb{Z}^n / \operatorname{Col} A$ is isomorphic to a direct product of finitely many cyclic groups (which, however, are not necessarily finite).

Proof of Proposition 7.1.9 (sketched). We give a "proof by example", or rather a proof by two (hopefully representative) examples:

$$\mathbb{Z}^2 / \operatorname{Col} \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \end{pmatrix} = \mathbb{Z}^2 / \operatorname{span}(ae_1, be_2, 0, 0) = \mathbb{Z}^2 / \operatorname{span}(ae_1, be_2)$$
$$\cong (\mathbb{Z}/a) \times (\mathbb{Z}/b)$$

and

$$\mathbb{Z}^4 / \operatorname{Col} \begin{pmatrix} a & 0 \\ 0 & b \\ 0 & 0 \\ 0 & 0 \end{pmatrix} = \mathbb{Z}^4 / \operatorname{span}(ae_1, be_2) \cong (\mathbb{Z}/a) \times (\mathbb{Z}/b) \times \mathbb{Z} \times \mathbb{Z}.$$

□

7.1.5. The proof strategy

This suggests a somewhat daring strategy for proving parts **(a)** and **(b)** of Theorem 7.1.1:

1. Let G be a finite abelian group. Thus, G is a finite $\mathbb{Z}$-module.
2. By Lemma 7.1.7, the $\mathbb{Z}$-module G is finitely presented. In other words, there is a matrix $A \in \mathbb{Z}^{n \times m}$ (for some $m \in \mathbb{N}$) such that $G \cong \mathbb{Z}^n / \operatorname{Col} A$.
3. Tweaking this matrix A in a strategic way, we can make it diagonal without changing $\mathbb{Z}^n / \operatorname{Col} A$ too much (to be precise: $\mathbb{Z}^n / \operatorname{Col} A$ stays isomorphic to G).
4. Then, we use Proposition 7.1.9 to argue that $\mathbb{Z}^n / \operatorname{Col} A$ is isomorphic to a direct product of finitely many cyclic groups (which are not necessarily finite).
5. We notice that these cyclic groups must be finite, because their direct product is finite (after all, this direct product is isomorphic to G, which is finite).
6. Thus, $G \cong (\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_k)$ for some positive integers $n_1, n_2, \ldots, n_k$. (This proves Theorem 7.1.1 **(a)**.)
7. We WLOG assume that $n_1, n_2, \ldots, n_k$ are > 1, since any n_i that equals 1 only contributes a trivial factor $\mathbb{Z}/1$ to the direct product $(\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_k)$ (and of course such a factor can simply be removed from the product).
8. Finally, by fudging the $n_1, n_2, \ldots, n_k$ appropriately, we ensure that $n_1 \mid n_2 \mid \cdots \mid n_k$. (This proves Theorem 7.1.1 **(b)**.)

Steps 1, 2, 4, 5, 6, 7 should be rather clear by now. But Steps 3 and 8 sound rather ambitious. How can we turn an arbitrary matrix into a diagonal one? How can we pull $n_1 \mid n_2 \mid \cdots \mid n_k$ out of thin air?

7.1.6. Row and column operations and congruent matrices

To make Step 3 a reality, the tool of choice are **row operations** and **column operations**. These are a mild generalization of the row and column operations that you know from linear algebra. Here is one way to define them:

Definition 7.1.10.

(a) A square matrix $A \in \mathbb{Z}^{k \times k}$ is said to be **invertible** if it has an inverse matrix in $\mathbb{Z}^{k \times k}$ (that is, an inverse matrix with integer entries). In other words, it is said to be invertible if it is a unit of the matrix ring $\mathbb{Z}^{k \times k}$.

For example, $\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in \mathbb{Z}^{2 \times 2}$ is not invertible. It has an inverse in $\mathbb{Q}^{2 \times 2}$, but that doesn't count!

(b) A **row operation** means an operation transforming a matrix $A \in \mathbb{Z}^{n \times m}$ into BA, where $B \in \mathbb{Z}^{n \times n}$ is some invertible $n \times n$-matrix.

(c) A **column operation** means an operation transforming a matrix $A \in \mathbb{Z}^{n \times m}$ into AC, where $C \in \mathbb{Z}^{m \times m}$ is some invertible $m \times m$-matrix.

(d) Two matrices $A, A' \in \mathbb{Z}^{n \times m}$ are said to be **congruent** if there exist invertible matrices $B \in \mathbb{Z}^{n \times n}$ and $C \in \mathbb{Z}^{m \times m}$ such that $A' = BAC$. In other words, A, A' are said to be congruent if A can be transformed into A' using row and column operations.

You know all these notions in the case of a field; we are just adapting them to the case of $\mathbb{Z}$.

Remark 7.1.11.

(a) Any row operation can be undone by another row operation.

(b) Adding a multiple of a row to another row is a row operation.

(c) Swapping two rows is a row operation.

(d) Scaling a row by -1 is a row operation. (But scaling a row by 2 is not!)

(e) The analogues of all these statements for columns instead of rows hold.

Proof. Part **(a)** is obvious (since multiplying a matrix by an invertible matrix B can be undone by multiplying it by B^{-1}). The other parts are proved as in linear algebra. □

Proposition 7.1.12. If two matrices $A, A' \in \mathbb{Z}^{n\times m}$ are congruent, then their cokernels $\mathbb{Z}^n / \operatorname{Col} A$ and $\mathbb{Z}^n / \operatorname{Col} A'$ are isomorphic.

Proof. Let $A, A' \in \mathbb{Z}^{n\times m}$ be two matrices that are congruent. Thus, there exist invertible matrices $B \in \mathbb{Z}^{n\times n}$ and $C \in \mathbb{Z}^{m\times m}$ such that $A' = BAC$. Consider these B and C.

I claim that the map

$$f : \mathbb{Z}^n / \operatorname{Col} A \to \mathbb{Z}^n / \operatorname{Col} A', \quad \overline{v} \mapsto \overline{Bv}$$

is well-defined and is a $\mathbb{Z}$-module isomorphism.

First of all, let me prove that f is well-defined. Indeed, let $v, w \in \mathbb{Z}^n$ be such that $\overline{v} = \overline{w}$ in $\mathbb{Z}^n / \operatorname{Col} A$. We must prove that $\overline{Bv} = \overline{Bw}$ in $\mathbb{Z}^n / \operatorname{Col} A'$.

From $\overline{v} = \overline{w}$ in $\mathbb{Z}^n / \operatorname{Col} A$, we obtain $v - w \in \operatorname{Col} A$. In other words, $v - w = Au$ for some $u \in \mathbb{Z}^m$ (since $\operatorname{Col} A = \{Au \mid u \in \mathbb{Z}^m\}$). Consider this u. We have $C^{-1} \in \mathbb{Z}^{m\times m}$ (since C is invertible) and thus $C^{-1}u \in \mathbb{Z}^m$. Now,

$$Bv - Bw = B\underbrace{(v-w)}_{=Au} = \underbrace{BA}_{\substack{=A'C^{-1} \\ \text{(since } BAC=A'\text{)}}} u = A' \underbrace{C^{-1}u}_{\in\mathbb{Z}^m} \in \operatorname{Col} A'$$

(since $\operatorname{Col} A' = \{A'z \mid z \in \mathbb{Z}^m\}$). In other words, $\overline{Bv} = \overline{Bw}$ in $\mathbb{Z}^n / \operatorname{Col} A'$, which is precisely what we wanted to show.

Thus, we have shown that f is well-defined.

It is straightforward to see that f is a $\mathbb{Z}$-module morphism. Next, in order to show that f is invertible, I will construct an inverse.

Indeed, I claim that the map

$$g : \mathbb{Z}^n / \operatorname{Col} A' \to \mathbb{Z}^n / \operatorname{Col} A, \quad \overline{v} \mapsto \overline{B^{-1}v}$$

is well-defined and is inverse to f. The "well-defined" part of this claim is left to the reader (the proof is analogous to the proof that f is well-defined, since $A' = BAC$ entails $A = B^{-1}A'C^{-1}$). The "inverse to f" part is straightforward (we have $BB^{-1}v = v$ and $B^{-1}Bv = v$ for any v).

Now, f is invertible (since g is inverse to f), and thus is a $\mathbb{Z}$-module isomorphism (since f is a $\mathbb{Z}$-module morphism). Hence, the $\mathbb{Z}$-modules $\mathbb{Z}^n / \operatorname{Col} A$ and $\mathbb{Z}^n / \operatorname{Col} A'$ are isomorphic. This proves Proposition 7.1.12. □

7.1.7. The Smith normal form algorithm

The following theorem will be crucial for Step 3:

Theorem 7.1.13 (Smith normal form, weak version)**.** Each rectangular matrix $A \in \mathbb{Z}^{n \times m}$ is congruent to a diagonal matrix (i.e., can be transformed into a diagonal matrix via row and column operations).

This theorem, combined with Proposition 7.1.12, suffices to complete Step 3 of our plan. Thus, we need to prove Theorem 7.1.13. Here is a very rough outline of the proof:

Proof of Theorem 7.1.13 (sketched). Again, we give a "proof by example". We start with the matrix $\begin{pmatrix} 4 & 6 \\ 3 & 2 \\ 2 & 2 \end{pmatrix} \in \mathbb{Z}^{3 \times 2}$, and we try to transform it into a diagonal matrix by a sequence of row operations and column operations. Note that this is in some sense a subtler version of Gaussian elimination (subtler because we are not allowed to scale rows or columns by any numbers other than -1, and because we can only add $\mathbb{Z}$-multiples of rows/columns to other row/columns, rather than $\mathbb{Q}$-multiples). We shall use the "$\xrightarrow{\text{R}}$" arrow for "row operation"

and the "$\xrightarrow{\mathrm{C}}$" arrow for "column operation".

$$\begin{pmatrix} 4 & 6 \\ 3 & 2 \\ 2 & 2 \end{pmatrix} \xrightarrow{\mathrm{C}} \begin{pmatrix} 4 & 2 \\ 3 & -1 \\ 2 & 0 \end{pmatrix} \quad \text{(here we subtracted column 1 from column 2)}$$

$$\xrightarrow{\mathrm{C}} \begin{pmatrix} 0 & 2 \\ 5 & -1 \\ 2 & 0 \end{pmatrix} \quad \text{(here we subtracted } 2 \cdot \text{column 2 from column 1)}$$

$$\xrightarrow{\mathrm{C}} \begin{pmatrix} 2 & 0 \\ -1 & 5 \\ 0 & 2 \end{pmatrix} \quad \text{(here we swapped columns 1 and 2)}$$

$$\xrightarrow{\mathrm{R}} \begin{pmatrix} 2 & 0 \\ 1 & -5 \\ 0 & 2 \end{pmatrix} \quad \text{(here we scaled row 2 by } -1\text{)}$$

$$\xrightarrow{\mathrm{R}} \begin{pmatrix} 0 & 10 \\ 1 & -5 \\ 0 & 2 \end{pmatrix} \quad \text{(here we subtracted } 2 \cdot \text{row 2 from row 1)}$$

$$\xrightarrow{\mathrm{R}} \begin{pmatrix} 1 & -5 \\ 0 & 10 \\ 0 & 2 \end{pmatrix} \quad \text{(here we swapped rows 1 and 2)}$$

$$\xrightarrow{\mathrm{C}} \begin{pmatrix} 1 & 0 \\ 0 & 10 \\ 0 & 2 \end{pmatrix} \quad \text{(here we added } 5 \cdot \text{column 1 to column 2)}$$

$$\xrightarrow{\mathrm{R}} \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 0 & 2 \end{pmatrix} \quad \text{(here we subtracted } 5 \cdot \text{row 3 from row 2)}$$

$$\xrightarrow{\mathrm{R}} \begin{pmatrix} 1 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix} \quad \text{(here we swapped rows 2 and 3)},$$

and this is a diagonal matrix.

The general procedure is as follows (you can check that this is precisely what we have done in the example above):

- We first "clear out" the 1st row; this means turning it into $(g, 0, 0, \ldots, 0)$, where g is the gcd of its entries. This is achieved as follows: We first ensure that all entries in the 1st row are nonnegative by appropriate column operations (namely, whenever an entry is negative, we scale the respective column by -1). Then, as long as the 1st row contains at least two nonzero entries, we subtract the column that contains the smaller one (or, better, an appropriate multiple of this column) from the column that contains

the larger one[189]. Note that this is essentially the Euclidean algorithm (or, to be more precise, a variant thereof for multiple integers). Finally, when there is only one nonzero entry left in the 1st row, we move this entry into the position $(1,1)$ by another column operation (swapping its column with the first column).

- Then, we use the same method (but using row operations instead of column operations) to clear out the 1st column (i.e., to ensure that its only nonzero entry is the $(1,1)$-entry).

  Note that this might mess up the 1st row again (i.e., some entries of the 1st row that were previously 0 might become nonzero again); in this case, we again clear out the 1st row, then again clear out the 1st column, and so on, until neither the 1st row nor the 1st column contain any nonzero entries except for the $(1,1)$-entry.

  I claim that this loop cannot go on forever. To see why, you should note that each of the "clear out the 1st row" and "clear out the 1st column" subroutines causes the $(1,1)$-entry to be replaced by a gcd of several entries, one of which is the $(1,1)$-entry. Clearly, such a replacement cannot make the $(1,1)$-entry larger (at least in absolute value), since $|\gcd(a_1, a_2, \ldots, a_k)| \leq |a_1|$ for any integers $a_1, a_2, \ldots, a_k$ with a_1 nonzero[190]. Moreover, it will make this entry strictly smaller, unless the $(1,1)$-entry was the gcd of all the entries in its row/column to begin with. Let us refer to the latter case as the "degenerate case"; in this case, the $(1,1)$-entry does not change as we clear out the 1st row/column. Sooner or later, we will necessarily encounter this "degenerate case", since otherwise the $(1,1)$-entry would keep decreasing indefinitely (but a nonnegative integer cannot do that).

  What happens when we encounter the "degenerate case"? Let us say that we encounter it as we are clearing out the 1st row, after the 1st column has been already cleared out (this is always the case after the second time we apply our "clearing-out subroutine"). Say that the 1st row is $(a_1, a_2, \ldots, a_m)$ at the moment we start clearing it out, and becomes $(a_1, 0, 0, \ldots, 0)$ after we clear it out (the first entry is a_1 because we are in the "degenerate case"). This entails that $a_1 = \gcd(a_1, a_2, \ldots, a_n)$, so that all the entries $a_1, a_2, \ldots, a_n$ of the 1st row (before the "clearing out") must be multiples of a_1. This property is clearly preserved during the "clearing-

[189] If the two entries are equal, then we subtract the column that lies further left from the column that lies further right.

[190] There is one exception: If the $(1,1)$-entry was 0, then it can become larger during a "clearing-out" subroutine (for example, if the 1st row was $(0, 51)$, then its $(1,1)$-entry 0 will get replaced with $\gcd(0,\ 51) = 51$). But this can happen only once during our algorithm, because once the $(1,1)$-entry is nonzero, it will never become 0 again (since the gcd of multiple numbers cannot be 0 unless **all** these numbers were 0). Thus, this exception still cannot make our loop go on forever.

out" subroutine as we clear out the 1st row (since the gcd of its entries does not change, thus remains a_1 throughout it). As a consequence, we never have to change the 1st column during this subroutine (since the 1st column only has to change if its top entry is larger than another entry of the 1st row or if its top entry is ≤ 0, but neither of these can happen when all entries of the 1st row are multiples of the $(1,1)$-entry). So the 1st column does not change.

Thus, after clearing out the 1st row, we are left with a matrix whose 1st row is clear (i.e., contains no nonzero entries except for the $(1,1)$-entry) and whose 1st column is also clear (since it has not changed during the "clearing out the 1st row" subroutine, but was itself cleared just before it). In other words, we are left with a matrix whose 1st row and whose 1st column only contain a single nonzero entry (if any!), which is the $(1,1)$-entry.

At this point, we forget about the 1st row and the 1st column, and play the same game with the rest of the matrix. (So we are working recursively. Note that whatever operations we do with the rest of the matrix, the 1st row and the 1st column will be unaffected, because they are filled with 0s everywhere apart from the $(1,1)$-entry. Thus, we won't ever have to clear them up again.)

- At the end of the procedure, the matrix will be diagonal.

Thus, after a sequence of row operations and column operations, our matrix has become diagonal. This proves Theorem 7.1.13. □

This completes Step 3 of our plan.

7.1.8. A few words on arbitrary rings

Before I move on to Step 8, let me say a few words about generalizing Theorem 7.1.13 to other rings. In our proof of Theorem 7.1.13, we seemingly used the fact that the entries of our matrix are integers (since we argued that a nonnegative integer cannot keep decreasing indefinitely). However, the proof is easily adapted to any Euclidean domain instead of $\mathbb{Z}$ (we just need to argue that the Euclidean norm of the $(1,1)$-th entry decreases, instead of that entry itself). In truth, Theorem 7.1.13 holds even more generally, with $\mathbb{Z}$ replaced by a PID. This level of generality is a tad too advanced for us, but proofs of this version of Theorem 7.1.13 can be found in various algebra texts (e.g., in [ChaLoi21, Theorem (5.3.10)]). Note that the diagonal matrix in Theorem 7.1.13 is not unique.

Remark 7.1.14. When the base ring is a field, the Smith normal form (this is how the diagonal matrix in Theorem 7.1.13 is called) becomes the rank normal form (see, e.g., `https://math.stackexchange.com/questions/371497/`).

7.1.9. Solving systems of linear equations over $\mathbb{Z}$

Remark 7.1.15. Incidentally, Theorem 7.1.13 also helps solve systems of linear equations in integer unknowns (as in Exercise 1.5.3). To wit, if two matrices $A, A' \in \mathbb{Z}^{n\times m}$ are congruent, and if $B \in \mathbb{Z}^{n\times n}$ and $C \in \mathbb{Z}^{m\times m}$ are two invertible matrices satisfying $A' = BAC$, and if $v \in \mathbb{Z}^n$ is any vector, then there is a bijection

$$\begin{aligned} \{w \in \mathbb{Z}^m \mid Aw = v\} &\to \left\{y \in \mathbb{Z}^m \mid A'y = Bv\right\}, \\ w &\mapsto C^{-1}w \end{aligned}$$

(check this!). Thus, solving the equation $Aw = v$ for an unknown vector $w \in \mathbb{Z}^m$ is tantamount to solving the equation $A'y = Bv$ for an unknown vector $y \in \mathbb{Z}^m$. But Theorem 7.1.13 tells us that we can choose A' to be diagonal, and then the equation $A'y = Bv$ is rather easy to solve. Thus, we obtain an algorithm for solving a vector equation of the form $Aw = v$ for an unknown vector $w \in \mathbb{Z}^m$; that is, we obtain an algorithm for solving systems of linear equations in integer unknowns.

7.1.10. Step 8: streamlining direct products of $\mathbb{Z}/n$'s

Let us return to our multi-step plan for proving Theorem 7.1.1. Step 8 is fun. Let me first discuss it in the case when $k = 2$. In this case, I need to explain how a direct product of the form $(\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2)$ with two positive integers n_1 and n_2 can be rewritten (up to isomorphism) as a direct product of the form $(\mathbb{Z}/n_1') \times (\mathbb{Z}/n_2')$ with $n_1' \mid n_2'$. For simplicity, let me rename n_1 and n_2 as n and m; then I claim that n_1' and n_2' can be chosen to be $\gcd(n,m)$ and $\operatorname{lcm}(n,m)$, respectively (these clearly satisfy $n_1' \mid n_2'$, since $\gcd(n,m) \mid n \mid \operatorname{lcm}(n,m)$). In order to prove this claim, I need to show the following lemma:

Lemma 7.1.16. Let $n, m \in \mathbb{Z}$. Let $g = \gcd(n,m)$ and $\ell = \operatorname{lcm}(n,m)$.

(a) Then, the matrices

$$\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} g & 0 \\ 0 & \ell \end{pmatrix}$$

in $\mathbb{Z}^{2\times 2}$ are congruent.

(b) As a consequence,

$$(\mathbb{Z}/n) \times (\mathbb{Z}/m) \cong (\mathbb{Z}/g) \times (\mathbb{Z}/\ell)$$

as groups.

Proof. This is so enjoyable that you should probably try to prove this on your own! Read on at your own spoiler risk.

(a) We WLOG assume that $g \neq 0$ (since otherwise, we have $n = m = 0$, and thus the two matrices in question both equal the zero matrix).

Bezout's theorem shows that there exist integers x, y such that $g = xn + ym$ (since $g = \gcd(n, m)$). Consider these x, y. Moreover, there exists some $u \in \mathbb{Z}$ such that $n = gu$ (since $g \mid n$). Likewise, there exists some $v \in \mathbb{Z}$ such that $m = gv$ (since $g \mid m$). Consider these u and v.

Furthermore, it is known that $\gcd(n, m) \cdot \operatorname{lcm}(n, m) = |nm|$. In other words, $g\ell = |nm|$. Thus, $g\ell = \pm \underbrace{n}_{=gu} m = \pm gum$. Cancelling g from this equality, we find $\ell = \pm um$ (since $g \neq 0$). Thus, $um = \pm\ell$, so that $-um = -(\pm\ell) = \mp\ell$.

Now, we transform the matrix $\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}$ as follows (using the "$\xrightarrow{\text{R}}$" arrow for "row operation" and the "$\xrightarrow{\text{C}}$" arrow for "column operation"):

$$\begin{aligned}
\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix} &\xrightarrow{\text{C}} \begin{pmatrix} n & xn \\ 0 & m \end{pmatrix} && \text{(here we added } x \cdot \text{column 1 to column 2)} \\
&\xrightarrow{\text{R}} \begin{pmatrix} n & xn+ym \\ 0 & m \end{pmatrix} && \text{(here we added } y \cdot \text{row 2 to row 1)} \\
&= \begin{pmatrix} gu & g \\ 0 & m \end{pmatrix} && \text{(since } n = gu \text{ and } xn + ym = g\text{)} \\
&\xrightarrow{\text{C}} \begin{pmatrix} 0 & g \\ -um & m \end{pmatrix} && \text{(here we subtracted } u \cdot \text{column 2 from column 1)} \\
&= \begin{pmatrix} 0 & g \\ -um & gv \end{pmatrix} && \text{(since } m = gv\text{)} \\
&\xrightarrow{\text{R}} \begin{pmatrix} 0 & g \\ -um & 0 \end{pmatrix} && \text{(here we subtracted } v \cdot \text{row 1 from row 2)} \\
&\xrightarrow{\text{C}} \begin{pmatrix} g & 0 \\ 0 & -um \end{pmatrix} && \text{(here, we swapped column 1 with column 2)} \\
&= \begin{pmatrix} g & 0 \\ 0 & \mp\ell \end{pmatrix} && \text{(since } -um = \mp\ell\text{)}.
\end{aligned}$$

If the $\mp\ell$ here is a $+\ell$, then we have thus obtained the matrix $\begin{pmatrix} g & 0 \\ 0 & \ell \end{pmatrix}$, so

that we conclude that the two matrices $\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}$ and $\begin{pmatrix} g & 0 \\ 0 & \ell \end{pmatrix}$ are congruent, as we wanted to show. If it is a $-\ell$ instead, then we need one more column operation (viz., scaling the second column by -1) in order to get to the same result and therefore to the same conclusion. Thus, Lemma 7.1.16 **(a)** is proved.

(b) Lemma 7.1.16 **(a)** yields that the matrices

$$\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} g & 0 \\ 0 & \ell \end{pmatrix}$$

in $\mathbb{Z}^{2\times 2}$ are congruent. Hence, Proposition 7.1.12 yields that their cokernels

$$\mathbb{Z}^2/\operatorname{Col}\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix} \qquad \text{and} \qquad \mathbb{Z}^2/\operatorname{Col}\begin{pmatrix} g & 0 \\ 0 & \ell \end{pmatrix}$$

are isomorphic. In view of

$$\mathbb{Z}^2/\operatorname{Col}\begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix} = \mathbb{Z}^2/\operatorname{span}(ne_1, me_2) \cong (\mathbb{Z}/n)\times(\mathbb{Z}/m)$$

and

$$\mathbb{Z}^2/\operatorname{Col}\begin{pmatrix} g & 0 \\ 0 & \ell \end{pmatrix} = \mathbb{Z}^2/\operatorname{span}(ge_1, \ell e_2) \cong (\mathbb{Z}/g)\times(\mathbb{Z}/\ell),$$

this means that $(\mathbb{Z}/n)\times(\mathbb{Z}/m)$ and $(\mathbb{Z}/g)\times(\mathbb{Z}/\ell)$ are isomorphic (as $\mathbb{Z}$-modules, and thus as groups). This proves Lemma 7.1.16 **(b)**. □

Lemma 7.1.16 **(b)** is sufficient to complete Step 8 in the case when $k = 2$ (that is, when G is a direct product of two cyclic groups). In the general case, we can try to use Lemma 7.1.16 **(b)** multiple times; in fact, applying Lemma 7.1.16 **(b)** to any pair of consecutive factors $\mathbb{Z}/n_i$ and $\mathbb{Z}/n_{i+1}$ in the direct product $(\mathbb{Z}/n_1)\times(\mathbb{Z}/n_2)\times\cdots\times(\mathbb{Z}/n_k)$ will replace these two factors by $\mathbb{Z}/n_i'$ and $\mathbb{Z}/n_{i+1}'$ with $n_i' \mid n_{i+1}'$. For example, if $k = 3$, then we can thus construct the following chain of isomorphisms:

$$\begin{aligned}
&\underbrace{(\mathbb{Z}/n_1)\times(\mathbb{Z}/n_2)}_{\substack{\cong(\mathbb{Z}/n_1')\times(\mathbb{Z}/n_2') \\ \text{for } n_1'=\gcd(n_1,n_2) \text{ and } n_2'=\operatorname{lcm}(n_1,n_2) \\ \text{(by Lemma 7.1.16 \textbf{(b)})}}} \times(\mathbb{Z}/n_3) \\
&\cong (\mathbb{Z}/n_1')\times \underbrace{(\mathbb{Z}/n_2')\times(\mathbb{Z}/n_3)}_{\substack{\cong(\mathbb{Z}/n_2'')\times(\mathbb{Z}/n_3'') \\ \text{for } n_2''=\gcd(n_2',n_3) \text{ and } n_3''=\operatorname{lcm}(n_2',n_3) \\ \text{(by Lemma 7.1.16 \textbf{(b)})}}} \\
&\cong \underbrace{(\mathbb{Z}/n_1')\times(\mathbb{Z}/n_2'')}_{\substack{\cong(\mathbb{Z}/n_1''')\times(\mathbb{Z}/n_2''') \\ \text{for } n_1'''=\gcd(n_1',n_2'') \text{ and } n_2'''=\operatorname{lcm}(n_1',n_2'') \\ \text{(by Lemma 7.1.16 \textbf{(b)})}}} \times(\mathbb{Z}/n_3'') \\
&\cong (\mathbb{Z}/n_1''')\times(\mathbb{Z}/n_2''')\times(\mathbb{Z}/n_3'').
\end{aligned}$$

It takes some thought to confirm that the resulting numbers n_1''', n_2''', n_3'' really do satisfy $n_1''' \mid n_2''' \mid n_3''$. (Indeed, $n_1''' \mid n_2'''$ follows from the definitions of n_1''' and n_2''' as gcd and lcm of one and the same pair of integers. As for proving $n_2''' \mid n_3''$, you have to first argue that combining

$$n_1' = \gcd(n_1, n_2) \mid \operatorname{lcm}(n_1, n_2) = n_2' \mid \operatorname{lcm}(n_2', n_3) = n_3'' \qquad \text{and}$$
$$n_2'' = \gcd(n_2', n_3) \mid \operatorname{lcm}(n_2', n_3) = n_3''$$

leads to $\operatorname{lcm}(n_1', n_2'') \mid n_3''$, so that $n_2''' = \operatorname{lcm}(n_1', n_2'') \mid n_3''$.) It might not be obvious, but this generalizes to arbitrary k:

- First apply Lemma 7.1.16 **(b)** to the first two factors of the direct product, then to the second and third factors, then to the third and fourth factors, and so on, until you have reached the right end of the direct product. After this, the numbers $n_1, n_2, \ldots, n_{k-1}$ will all divide n_k.
- Then do the same, but stop just before the last factor (i.e., leave the last factor untouched). After this, the numbers $n_1, n_2, \ldots, n_{k-2}$ will all divide n_{k-1}, but the numbers $n_1, n_2, \ldots, n_{k-1}$ will still all divide n_k.
- Then do the same, but stop just before the second-to-last factor (i.e., leave the last two factors untouched). After this, the numbers $n_1, n_2, \ldots, n_{k-3}$ will all divide n_{k-2}, but the previously mentioned divisibilities will remain intact.
- And so on, until at the end there are no more factors left to apply Lemma 7.1.16 **(b)** to. At that point, you will have $n_1 \mid n_2 \mid \cdots \mid n_k$.

(Fun fact: There are many other ways to achieve $n_1 \mid n_2 \mid \cdots \mid n_k$ by a sequence of moves of the form "replace n_i and n_{i+1} by $\gcd(n_i, n_{i+1})$ and $\operatorname{lcm}(n_i, n_{i+1})$". Indeed, any sufficiently long sequence of such moves will eventually come to a halt – at least if we make sure to only apply such a move to pairs (n_i, n_{i+1}) that don't already satisfy $n_i \mid n_{i+1}$ – and the resulting numbers will satisfy $n_1 \mid n_2 \mid \cdots \mid n_k$. Moreover, the resulting numbers will not depend on the sequence of moves. Proving this all is Problem A3 on the Putnam contest 2008: problem statements and solutions. Our specific choreographed sequence above was merely the easiest one to analyze.)

Thus we have outlined a proof of parts **(a)** and **(b)** of Theorem 7.1.13.

Did Lemma 7.1.16 **(b)** remind you of the Chinese Remainder Theorem? There is indeed a connection, although it is not as obvious as one might expect:

Exercise 7.1.1. Let $n, m \in \mathbb{Z}$. Let $g = \gcd(n, m)$ and $\ell = \operatorname{lcm}(n, m)$.
Lemma 7.1.16 **(b)** shows that $(\mathbb{Z}/n) \times (\mathbb{Z}/m) \cong (\mathbb{Z}/g) \times (\mathbb{Z}/\ell)$ as groups.

(a) Prove that $(\mathbb{Z}/n) \times (\mathbb{Z}/m) \cong (\mathbb{Z}/g) \times (\mathbb{Z}/\ell)$ as rings as well.

(b) Use this to prove Theorem 2.12.6 again.

[**Hint:** Part **(a)** is easiest to solve using the prime factorizations of n and m. In particular, this yields a new proof of Lemma 7.1.16 **(b)**.]

Note that Exercise 7.1.1 cannot be generalized to the extent Theorem 2.12.6 was generalized to Theorem 2.12.4. In general, if I and J are two ideals of a commutative ring R, then the rings $(R/I) \times (R/J)$ and $(R/(I+J)) \times (R/(I \cap J))$ are usually not isomorphic. However, Exercise 7.1.1 **(a)** can be generalized slightly by replacing $\mathbb{Z}$ by an arbitrary PID.

7.1.11. Uniqueness of the SNF

The next two exercises contain a do-it-yourself proof of Theorem 7.1.13 **(c)** (see also [ChaLoi21, last claim of Corollary (5.4.4)] for a more general result).

Exercise 7.1.2. Let G be a $\mathbb{Z}$-module. Let $n_1, n_2, \ldots, n_k$ be k positive integers such that $G \cong (\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_k)$ and $n_1 \mid n_2 \mid \cdots \mid n_k$. Let p be a prime number, and let $i \in \mathbb{N}$. Prove that

$$\left| p^i G / p^{i+1} G \right| = p^{\left(\text{the number of all } j \in \{1,2,\ldots,k\} \text{ such that } p^{i+1} \mid n_j\right)}$$

(where we are regarding G as a $\mathbb{Z}$-module, so that $p^i G = \left\{ p^i g \mid g \in G \right\}$ and $p^{i+1} G = \left\{ p^{i+1} g \mid g \in G \right\}$).

Exercise 7.1.3. Prove Theorem 7.1.13 **(c)**.

[**Hint:** Assume that $G \cong (\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_k)$ and $n_1 \mid n_2 \mid \cdots \mid n_k$ and $n_1, n_2, \ldots, n_k > 1$. Prove that knowing the numbers

$$\left(\text{the number of all } j \in \{1,2,\ldots,k\} \text{ such that } p^{i+1} \mid n_j\right)$$

for all primes p and all $i \in \mathbb{N}$ uniquely characterizes $n_1, n_2, \ldots, n_k$. Now use Exercise 7.1.2.]

7.2. Application: Primitive roots

Theorem 7.1.1 has a curious (and actually rather useful) application to finite fields.

We begin with a fun observation:

The sequence of residue classes $\overline{1}, \overline{2}, \ldots, \overline{6}$ in $\mathbb{Z}/7$ is an arithmetic sequence (in the sense that there exists some "difference" $d \in \mathbb{Z}/7$ such that each entry of this sequence equals the preceding entry plus d).

I claim that you can permute this sequence so that it becomes a geometric sequence (in the sense that there exists some "quotient" $q \in \mathbb{Z}/7$ such that each entry of the permuted sequence equals the preceding entry times q) !

Namely, $\overline{1}, \overline{3}, \overline{2}, \overline{6}, \overline{4}, \overline{5}$ is a geometric sequence. Its "quotient" is $\overline{3}$, meaning that each entry equals the preceding entry times $\overline{3}$:

$$\overline{3} = \overline{1} \cdot \overline{3}, \qquad \overline{2} = \overline{3} \cdot \overline{3}, \qquad \overline{6} = \overline{2} \cdot \overline{3}, \qquad \ldots.$$

This can be generalized: For any prime p, we can arrange the residue classes $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ in a geometric sequence. Here is another way to put it:

Theorem 7.2.1 (Gauss)**.** Let p be a prime. Then, there exists some $g \in (\mathbb{Z}/p)^\times$ such that its $p-1$ powers $g^0, g^1, \ldots, g^{p-2}$ are distinct and satisfy

$$(\mathbb{Z}/p)^\times = \left\{g^0, g^1, \ldots, g^{p-2}\right\}.$$

Such a g is called a **primitive root** modulo p.

More generally:

Theorem 7.2.2. Let F be any finite field. Then, the group $F^\times = F \setminus \{0\}$ is cyclic.

Even more generally:

Theorem 7.2.3. Let F be any field. Let G be a **finite** subgroup of its group $F^\times = F \setminus \{0\}$ of units. Then, G is cyclic.

Proof of Theorem 7.2.3. The group G is finite and abelian. Thus, by Theorem 7.1.1 (parts **(a)** and **(b)**), we have

$$G \cong (\mathbb{Z}/n_1) \times (\mathbb{Z}/n_2) \times \cdots \times (\mathbb{Z}/n_k) \tag{146}$$

for some positive integers $n_1, n_2, \ldots, n_k > 1$ satisfying $n_1 \mid n_2 \mid \cdots \mid n_k$. Consider these $n_1, n_2, \ldots, n_k$.

Our goal is to show that $k \leq 1$ (because then, (146) will show that G is cyclic). In order to prove this, we assume the contrary. Thus, $k > 1$, so $k \geq 2$.

Now, G is not just a random abelian group. It has a peculiar property: Namely, for any positive integer d, the group G has no more than d elements g satisfying $g^d = 1$. (Indeed, all such elements g must be roots of the degree-d polynomial $x^d - 1 \in F[x]$, but we know that a degree-d polynomial over a field has no more than d roots.)

Applying this to $d = n_1$, we conclude that G has no more than n_1 elements g satisfying $g^{n_1} = 1$.

However, the $\mathbb{Z}/n_1$ factor on the right hand side of (146) contributes n_1 such elements (indeed, each element g of $\mathbb{Z}/n_1$ becomes 0 when multiplied by n_1, and thus – if we rewrite the group multiplicatively – satisfies $g^{n_1} = 1$), and the $\mathbb{Z}/n_2$ factor also contributes n_1 such elements (since $n_1 \mid n_2$, so that every of the n_1 multiples of $\overline{n_2/n_1}$ in $\mathbb{Z}/n_2$ is such an element). These two factors overlap only in the identity element. Thus, we have found at least $2n_1 - 1$ many elements $g \in G$ satisfying $g^{n_1} = 1$. But there are no more than n_1 such elements, as we have seen above. Thus, $2n_1 - 1 \leq n_1$, or, equivalently, $n_1 \leq 1$. This contradicts $n_1 > 1$. This contradiction shows that our assumption was wrong, and this completes the proof of Theorem 7.2.3. $\square$

Proof of Theorem 7.2.2. Apply Theorem 7.2.3 to $G = F^\times$. □

Proof of Theorem 7.2.1. Apply Theorem 7.2.2 to $F = \mathbb{Z}/p$. This yields that the group $(\mathbb{Z}/p)^\times$ is cyclic. In other words, there exists some $g \in (\mathbb{Z}/p)^\times$ such that its powers $g^0, g^1, \ldots, g^{\left|(\mathbb{Z}/p)^\times\right|-1}$ are distinct and satisfy

$$(\mathbb{Z}/p)^\times = \left\{g^0, g^1, \ldots, g^{\left|(\mathbb{Z}/p)^\times\right|-1}\right\}.$$

In view of $\left|(\mathbb{Z}/p)\right|^\times = p-1$, this rewrites as follows: There exists some $g \in (\mathbb{Z}/p)^\times$ such that its $p-1$ powers $g^0, g^1, \ldots, g^{p-2}$ are distinct and satisfy

$$(\mathbb{Z}/p)^\times = \left\{g^0, g^1, \ldots, g^{p-2}\right\}.$$

This proves Theorem 7.2.1. □

See Keith Conrad's note `https://kconrad.math.uconn.edu/blurbs/grouptheory/cyclicmodp.pdf` for various other proofs of Theorem 7.2.1.

Exercise 7.2.1. Let p be a prime. Prove that the group $(\mathbb{Z}/(2p))^\times$ is cyclic (even though $\mathbb{Z}/(2p)$ is not a field).

[**Hint:** There is a ring morphism $\pi : \mathbb{Z}/(2p) \to \mathbb{Z}/p$ that sends each $\overline{a}$ to $\overline{a}$. Like any ring morphism, this morphism sends units to units, and thus its restriction to $(\mathbb{Z}/(2p))^\times$ is a group morphism $(\mathbb{Z}/(2p))^\times \to (\mathbb{Z}/p)^\times$. Prove that the latter group morphism is an isomorphism whenever $p > 2$. Deal with the $p = 2$ case by hand. Alternatively, use the Chinese Remainder Theorem.]

Exercise 7.2.2.

(a) Prove that the group $(\mathbb{Z}/8)^\times$ is **not** cyclic.

(b) More generally: Let k be a positive integer. Prove that the group $\left(\mathbb{Z}/2^k\right)^\times$ is cyclic if and only if $k \leq 2$.

[**Hint:** For part **(b)**, if $k > 3$, find at least two distinct elements of $\left(\mathbb{Z}/2^k\right)^\times$ that have order 2.]

Exercise 7.2.3. Let $p \neq 2$ be a prime. Prove that the group $\left(\mathbb{Z}/p^2\right)^\times$ is cyclic (even though $\mathbb{Z}/p^2$ is not a field).

[**Hint:** This group has size $p^2 - p = p(p-1)$. Thus, it suffices to find an element of this group whose order is $p(p-1)$.

Pick $a \in \mathbb{Z}$ such that $\overline{a}$ is a generator of the cyclic group $(\mathbb{Z}/p)^\times$. Show first that $(a+p)^{p-1} \equiv a^{p-1} - pa^{p-2} \bmod p^2$. Conclude that at least one of the integers a^{p-1} and $(a+p)^{p-1}$ is not congruent to 1 modulo p^2. In other words, there exists a $b \in \{a, a+p\}$ such that $b^{p-1} \not\equiv 1 \bmod p^2$. Now, show that the corresponding element $\overline{b}$ of $\mathbb{Z}/p^2$ belongs to the group $\left(\mathbb{Z}/p^2\right)^\times$ and has order $p(p-1)$ in this group.]

Exercise 7.2.4. Let $p \neq 2$ be a prime. Let k be a positive integer. Prove that the group $\left(\mathbb{Z}/p^k\right)^\times$ is cyclic (even though $\mathbb{Z}/p^k$ is not a field).

[**Hint:** Induct on k. Exercise 7.2.3 yields that there exists an $a \in \mathbb{Z}$ such that $\overline{a}$ is a generator of the cyclic group $\left(\mathbb{Z}/p^2\right)^\times$. Consider such an a. Show that $a^{p-1} \equiv 1 \bmod p$ but $a^{p-1} \not\equiv 1 \bmod p^2$, and thus $a^{p-1} = 1 + pu$ for some integer u not divisible by p. Use this to show that $a^{p^{k-2}(p-1)} \not\equiv 1 \bmod p^k$. Also show that $a^{p^{k-1}u} \not\equiv 1 \bmod p^k$ for any proper divisor u of $p-1$. Use these non-congruences to conclude that $\overline{a} \in \mathbb{Z}/p^k$ has order $p^{k-1}(p-1)$ in the group $\left(\mathbb{Z}/p^k\right)^\times$, and therefore the latter group is cyclic.]

With all these exercises, we can finally characterize for which numbers n the group $(\mathbb{Z}/n)^\times$ is cyclic:

Exercise 7.2.5. Let n be a positive integer. Prove that the group $(\mathbb{Z}/n)^\times$ is cyclic if and only if

$$n \in \{1,2,4\} \cup \left\{p^k \mid p \neq 2 \text{ is a prime, and } k \text{ is a positive integer}\right\} \cup \left\{2p^k \mid p \neq 2 \text{ is a prime, and } k \text{ is a positive integer}\right\}.$$

[**Hint:** For the "if" direction: What is the connection between the groups $(\mathbb{Z}/m)^\times$ an $(\mathbb{Z}/(2m))^\times$ when m is odd?

For the "only if" direction: Argue that $(\mathbb{Z}/n)^\times$ has more than 2 elements of order 2 if n does not belong to the given set.]

References

[21s] Darij Grinberg, *An Introduction to Algebraic Combinatorics [Math 701, Spring 2021 lecture notes]*, 6 April 2024.
https://www.cip.ifi.lmu.de/~grinberg/t/21s/lecs.pdf

[21w] Darij Grinberg, *Math 533: Abstract Algebra I, Winter 2021*.
https://www.cip.ifi.lmu.de/~grinberg/t/21w/

[Aluffi16] Paolo Aluffi, *Algebra: Chapter 0*, Graduate Studies in Mathematics **104**, 2nd printing, AMS 2016.
See https://www.math.fsu.edu/~aluffi/ for errata.

[Aluffi21] Paolo Aluffi, *Algebra: Notes from the Underground*, Cambridge University Press 2021.
See https://www.math.fsu.edu/~aluffi/ for errata.

[Baumga15] Oswald Baumgart, *The Quadratic Reciprocity Law: A Collection of Classical Proofs*, Springer 2015.

[BeaBla19] John A. Beachy, William D. Blair, *Abstract Algebra*, 4th edition, Waveland Press 2019.

[Bosch18] Siegfried Bosch, *Algebra*, Springer 2018.

[Burton11] David M. Burton, *Elementary Number Theory*, 7th edition, McGraw-Hill 2011.

[ChaLoi21] Antoine Chambert-Loir, *(Mostly) Commutative Algebra*, 27 January 2021.
https://webusers.imj-prg.fr/~antoine.chambert-loir/publications/teach/sv-commalg.pdf

[ChLoYa11] Heng Huat Chan, Ling Long and YiFan Yang, *A Cubic Analogue of the Jacobsthal Identity*, The American Mathematical Monthly **118**, No. 4 (April 2011), pp. 316–326.

[CoLiOs15] David A. Cox, John Little, Donal O'Shea, *Ideals, Varieties, and Algorithms*, Undergraduate Texts in Mathematics, 4th edition, Springer 2015.
https://dx.doi.org/10.1007/978-3-319-16721-3

[Cox12] David A. Cox, *Galois Theory*, 2nd edition, Wiley 2012.

[Cox22] David A. Cox, *Primes of the form $x^2 + ny^2$*, AMS Chelsea Publishing **387**, 3rd edition, AMS 2022.

[deGraa20] Willem de Graaf, *Computational Algebra*, 5 August 2021.
https://degraaf.maths.unitn.it/algnotes/compalg.pdf

[DumFoo04] David S. Dummit, Richard M. Foote, *Abstract Algebra*, 3rd edition, Wiley 2004.
See `https://site.uvm.edu/rfoote/files/2022/06/errata_3rd_edition.pdf` for errata.

[Edward22] Harold M. Edwards, *Essays in Constructive Mathematics*, 2nd edition, Springer 2022.

[Elman22] Richard Elman, *Lectures on Abstract Algebra*, 21 September 2024.
`https://www.math.ucla.edu/~rse/algebra_book.pdf`

[Ford22] Timothy J. Ford, *Abstract Algebra*, 14 August 2024.
`https://tim4datfau.github.io/Timothy-Ford-at-FAU/preprints/Algebra_Book.pdf`

[Friedm19] Robert Friedman, *Factorization in Integral Domains I*, 27 March 2019.
`https://web.archive.org/web/20221130230143/https://www.math.columbia.edu/~rf/factorization1.pdf`

[Gallia21] Joseph A. Gallian, *Contemporary Abstract Algebra*, 10th edition, CRC Press 2021.

[Goodma16] Frederick M. Goodman, *Algebra: Abstract and Concrete*, edition 2.6, 12 October 2016.
`https://homepage.divms.uiowa.edu/~goodman/algebrabook.dir/algebrabook.html`

[Grinbe15] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 15 September 2022, arXiv:2008.09862v3.

[Grinbe19] Darij Grinberg, *Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)*, 29 June 2019.
`http://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf`

[Grinbe20] Darij Grinberg, *Regular elements of a ring, monic polynomials and "lcm-coprimality"*, 22 May 2021.
`https://www.cip.ifi.lmu.de/~grinberg/algebra/regpol.pdf`

[Grinbe21] Darij Grinberg, *Notes on mathematical problem solving*, 23 December 2024.
`http://www.cip.ifi.lmu.de/~grinberg/t/20f/mps.pdf`

[Haensc16] Anna Haensch, *Quaternions and the four-square theorem*, 2016.
`https://web.archive.org/web/20230112025709/https://www.mathcs.duq.edu/~haensch/411Materials/Quaternions.pdf`

[Jacobs07] Ernst Jacobsthal, *Über die Darstellung der Primzahlen der Form* $4n+1$ *als Summe zweier Quadrate*, J. Reine Angew. Math. **132** (1907), pp. 238–245.
Correction in J. Reine Angew. Math. **132** (1907), pp. 246.

[JacobsXX] Nathan Jacobson, *Lectures in Abstract Algebra, volume I: Basic Concepts; volume II: Linear Algebra; volume III: Theory of Fields and Galois Theory*, Springer 1951–1964.

[KeeGui20] Patrick Keef, David Guichard, *An Introduction to Higher Mathematics*, 13 May 2023.

[Klazar10a] Martin Klazar, *Analytic and combinatorial number theory I*, lecture notes 2010.
`https://kam.mff.cuni.cz/~klazar/ln_antcI.pdf`

[Klazar10b] Martin Klazar, *Analytic and combinatorial number theory II*, lecture notes 2010.
`https://kam.mff.cuni.cz/~klazar/ln_antcII.pdf`

[Knapp16] Anthony W. Knapp, *Basic Algebra*, Digital 2nd edition 2016.
`http://www.math.stonybrook.edu/~aknapp/download.html`

[LaNaSc16] Isaiah Lankham, Bruno Nachtergaele, Anne Schilling, *Linear Algebra As an Introduction to Abstract Mathematics*, 2016.
`https://www.math.ucdavis.edu/~anne/linear_algebra/mat67_course_notes.pdf`

[Laurit09] Niels Lauritzen, *Concrete Abstract Algebra*, Cambridge University Press 2009.

[Leeb20] Bernhard Leeb, *Some multilinear algebra*, 25 January 2020.
`https://www.math.lmu.de/~leeb/lehre/texte/ana3/ana3_multilinalg.pdf`

[Lehman19] James Larry Lehman, *Quadratic Number Theory*, Dolciani Mathematical Expositions **52**, MAA Press 2019.

[Leinst24] Tom Leinster, *Galois Theory*, arXiv:2408.07499v1.
See `https://www.maths.ed.ac.uk/~tl/galois/` for videos and extra materials.

[LidNie00] Rudolf Lidl, Harald Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, 2nd edition 1997.

[Lorsch20a] Oliver Lorscheid, *Algebra 1*, Lecture notes, IMPA, 25 June 2020.
`https://web.archive.org/web/20230810012748/https://oliver.impa.br/notes/algebra1.pdf`

[Lorsch20b] Oliver Lorscheid, *Galois theory*, Lecture notes, IMPA, 26 August 2020.
https://web.archive.org/web/20230307002620/https://oliver.impa.br/notes/galoistheory.pdf

[McNult16] George F. McNulty, *Algebra for First Year Graduate Students*, 10 January 2017.
https://people.math.sc.edu/mcnulty/algebrafirst.pdf

[Mileti20] Joseph R. Mileti, *Abstract Algebra*, 10 April 2023.
https://mileti.math.grinnell.edu/m321s23/AbstractAlgebra.pdf

[MoSrSa24] Archana S Morye, Sreenanda S B, Prakash Saivasan, *Reduced Grobner Basis With Double Exponential Cardinality*, arXiv:2411.17602v2.

[MulMum07] Gary L. Mullen, Carl Mummert, *Finite Fields and Applications*, Student Mathematical Library **41**, AMS 2007.

[Nica22] Bogdan Nica, *On an identity of Sylvester*, arXiv:2212.13624v2.

[Philip23] Peter Philip, *Linear Algebra I*, 22 April 2024, AMS Open Math Notes OMN:202109.111304.
https://www.ams.org/open-math-notes/omn-view-listing?listingId=111304

[Poonen18] Bjorn Poonen, *Why all rings should have a 1*, 15 June 2018.
https://math.mit.edu/~poonen/papers/ring.pdf

[Richma88] Fred Richman, *Nontrivial Uses of Trivial Rings*, Proceedings of the American Mathematical Society **103**, No. 4. (Aug., 1988), pp. 1012–1014.

[Rosen02] Michael Rosen, *Number Theory in Function Fields*, Springer 2002.

[Rotman3e] Joseph J. Rotman, *Advanced Modern Algebra: Third Edition, Part 1 and Part 2*, Graduate Studies in Mathematics **165** and **180**, AMS 2015 and 2017.

[Schroe09] Manfred Schroeder, *Number Theory in Science and Communication*, 5th edition 2009.

[Schwar14] Rich Schwartz, *Math 153: The Four Square Theorem*, April 12, 2014.
https://www.math.brown.edu/reschwar/M153/lagrange.pdf

[Sharif22] Romyar Sharifi, *Abstract Algebra*, 16 March 2024.
https://www.math.ucla.edu/~sharifi/algebra.pdf

[Shifri96] Theodore Shifrin, *Abstract Algebra: A Geometric Approach*, Prentice-Hall 1996.

[Siksek19] Samir Siksek, *MA3D5 Galois Theory*, 2019.
`https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/gt/whole.pdf`

[Siksek20] Samir Siksek, *Introduction to Abstract Algebra*, 2020.
`http://homepages.warwick.ac.uk/~maseap/teaching/aa/aanotes.pdf`

[Siksek21] Samir Siksek, *MA377 Rings and Modules*, 2021.
`https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/rm/rmversion9.pdf`

[Stein09] William Stein, *Elementary Number Theory: Primes, Congruences, and Secrets*, Springer 2009.

[Steinb06] Mark Steinberger, *Algebra*, 31 August 2006.
`https://math.hawaii.edu/~tom/algebra.pdf`

[Stewar15] Ian Stewart, *Galois theory*, 4th edition, CRC Press 2015.
`http://matematicaeducativa.com/foro/download/file.php?id=1647`

[Swanso17] Irena Swanson, *Abstract Algebra*, 13 December 2016.
`https://www.math.purdue.edu/~iswanso/abstractalgebra.pdf`

[Treil21] Serge Treil, *Linear Algebra Done Wrong*, 1 October 2024.
`https://sites.google.com/a/brown.edu/sergei-treil-homepage/linear-algebra-done-wrong`

[vanDal05] Birgit van Dalen, *Lenstra's wonderlijke kaartspel: Een generalisatie van de Chinese Reststelling voor niet-commutatieve ringen*, bachelor thesis, 9 May 2005.
`https://www.universiteitleiden.nl/binaries/content/assets/science/mi/scripties/dalenbachelor.pdf`

[vanDal06] Birgit van Dalen, *Card games with ideals*, Nieuw Archief voor Wiskunde **5/7** (2006), pp. 52–56.

[Vorobi02] Nicolai N. Vorobiev, *Fibonacci Numbers*, Translated from the Russian by Mircea Martin, Springer 2002 (translation of the 6th Russian edition).

[Waerde91] B. L. van der Waerden, *Algebra: Volume I and Volume II*, based in part on lectures by E. Artin and E. Noether, 7th edition (volume I) and 5th edition (volume II), Springer 1991.

[Warner90] Seth Warner, *Modern Algebra: two volumes bound as one*, Dover 1990.

[Whitem52] Albert Leon Whiteman, *Cyclotomy and Jacobsthal Sums*, American Journal of Mathematics **74**, No. 1 (Jan., 1952), pp. 89–99.

[ZarSam86] Oscar Zariski, Pierre Samuel, *Commutative Algebra, Volume 1*, 3rd printing, Springer 1986.

[Zhang07] Ying Zhang, *Representing Primes as $x^2 + 5y^2$: An Inductive Proof that Euler Missed*, arXiv:math/0606547v2.