Introduction to Modern Algebra (UMN Spring 2019 Math 4281 notes)

Darij Grinberg

Tuesday 6th April, 2021 at 14:37.
Status: finished up to Section 4.2.4.

Contents

Note

This is the version without proofs. See `https://www.cip.ifi.lmu.de/~grinberg/t/19s/notes.pdf` for the complete version.

1. Introduction

This file contains notes for the Math 4281 class ("Introduction to Modern Algebra") I have taught at the University of Minnesota in Spring 2019. Occasionally, it also includes material that did not appear in the lectures.

The website of the class is `https://www.cip.ifi.lmu.de/~grinberg/t/19s/index.html` ; you will find homework sets and midterms there.

1.1. Status

The first few chapters of these notes are finished. The rest are at various degrees of completion (mostly readable, but sometimes not completely polished).

1.2. Literature

Many books have been written about abstract algebra. I have only a passing familiarity with most of them. Some of the "bibles" of the subject (bulky texts covering lots of material) are Dummit/Foote [DumFoo04], Knapp [Knapp16a] and [Knapp16b] (both freely available), van der Waerden [Waerde91a] and [Waerde91b] (one of the oldest texts on modern algebra, thus rather dated, but still as readable as ever).

Of course, any book longer than 200 pages likely goes further than our course will (unless it is full of details or solved exercises or printed in really large letters, like this one will be once it is finished). Thus, let me recommend some more introductory sources. Siksek's lecture notes [Siksek15] are a readable introduction that is a lot more amusing than I had ever expected an algebra text to be. Goodman's free book [Goodma16] combines introductory material with geometric motivation and applications, such as the classification of regular polyhedra and 2-dimensional crystals. In a sense, it is a great complement to our ungeometric course. Pinter's [Pinter10] often gets used in classes like ours. Armstrong's notes [Armstr18] cover a significant part of what we do. Childs's [Childs00] comes the closest to what we are setting out to do here, that is, give an example-grounded introduction to basic abstract algebra.

Keith Conrad's blurbs [Conrad*] are not a book, as they only cover selected topics. But at pretty much every topic they cover, they are one of the best sources (clear, full of examples, and often going fairly deep). We shall follow one of them particularly closely: the one on Gaussian integers [ConradG].

We will use some basic linear algebra, all of which can be found in Hefferon's book [Heffer17] (but we won't need all of this book). As far as determinants are concerned, we will briefly build up their theory; we refer to [Strick13, Section 12 & Appendix B] for proofs (and to [Grinbe15, Chapter 6] for a really detailed and formal treatment).

This course will begin (after some motivating questions) with a survey of elementary number theory. This is in itself a deep subject (despite the name) with a

long history (perhaps as old as mathematics), and of course we will just scratch the surface. Books like [NiZuMo91], [Burton10] and [UspHea39] cover a lot more than we can do. The Gallier/Quaintance survey [GalQua17] covers a good amount of basics and more.

We assume that the reader is familiar with the commonplaces of mathematical argumentation, such as induction (including strong induction), "WLOG" arguments, proof by contradiction, summation signs ($\sum$) and polynomials (a vague notion of polynomials will suffice; we will give a precise definition when it becomes necessary). If not, several texts can be helpful in achieving such familiarity: e.g., [LeLeMe18, particularly Chapters 1–5], [Hammac18], [Day16].

I thank the students of the Math 4281 class for discovering and reporting errors in previous versions of these notes. Some of the discussion of variants of Gaussian integers (and the occasional correction) is due to Keith Conrad; the discussion of Gaussian integers itself owes much to his [ConradG].

These notes include some excerpts from [Grinbe16] and slightly rewritten sections of [Grinbe15].

1.3. The plan

The material I am going to cover is mostly standard. However, the order in which I will go through it is somewhat unusual: I will spend a lot of time studying the basic examples before defining abstract notions such as "group", "monoid", "ring" and "field". This way, once I come to these notions, you'll already have many examples to work with. (Don't be fooled by the word "example": We will prove a lot about them, much of which is neither straightforward nor easy.)

First, I will show some motivating questions that are easy to state yet require abstract algebra to answer. We will hopefully see their answers by the end of this class. (Some of them can also be answered elementarily, without using abstract algebra, but such answers usually take more work and are harder to find.)

1.4. Motivation: $n = x^2 + y^2$

A *perfect square* means the square of an integer. Thus, the perfect squares are

$$0^2 = 0, \qquad 1^2 = 1, \qquad 2^2 = 4, \qquad 3^2 = 9, \qquad 4^2 = 16, \qquad \ldots.$$

Here is an old problem (first solved by Pierre de Fermat in 1640, but apparently already studied by Diophantus in the 3rd Century):

Question 1.4.1. What integers can be written as sums of two perfect squares?

For example, 5 can be written in this way, since $5 = 2^2 + 1^2$.

So can 4, since $4 = 2^2 + 0^2$. (Keep in mind that 0 is a perfect square.)

However, 7 cannot be written in this way. In fact, if we had $7 = a^2 + b^2$ for two integers a and b, then a^2 and b^2 would have to be ≤ 7 (since a^2 and b^2 are always

≥ 0, no matter what sign a and b have); but the only perfect squares that are ≤ 7 are $0, 1, 4$, and there is no way to write 7 as a sum of two of these perfect squares (just check all the possibilities).

For a similar but simpler reason, no negative number can be written as a sum of two perfect squares.

We can of course approach Question 1.4.1 using a computer: It is easy to check, for a given integer n, whether n is a sum of two perfect squares. (Just check all possibilities for a and b for the validity of the equation $n = a^2 + b^2$. You only need to try a and b belonging to $\left\{0, 1, \ldots, \left\lfloor \sqrt{n} \right\rfloor\right\}$, where $\lfloor y \rfloor$ (for a real number y) denotes the largest integer that is less or equal than y (also known as "y rounded down").) If you do this, you will see that among the first 101 nonnegative integers, the ones that can be written as sums of two perfect squares are precisely

$$0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29,$$
$$32, 34, 36, 37, 40, 41, 45, 49, 50, 52, 53, 58, 61, 64,$$
$$65, 68, 72, 73, 74, 80, 81, 82, 85, 89, 90, 97, 98, 100.$$

Having this data, you can look up the sequence in the Online Encyclopedia of Integer Sequences (short OEIS), and see that the sequence of these integers is known as OEIS Sequence A001481. In the "Comments" field, you can read a lot of what is known about it (albeit in telegraphic style).

For example, one of the comments says "Closed under multiplication". This is short for "if you multiply two entries of the sequence, then the product will again be an entry of the sequence". In other words, if you multiply two integers that are sums of two perfect squares, then you get another sum of two perfect squares. Why is this so?

It turns out that there is a "simple" reason for this: the identity

$$\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ad + bc)^2 + (ac - bd)^2, \tag{1}$$

which holds for arbitrary reals a, b, c, d (and thus, in particular, for integers). This is known as the Brahmagupta-Fibonacci identity, and of course can easily be proven by expanding both sides. But how would you come up with such an identity?

If you stare at the above sequence long enough, you may also discover another pattern: An integer of the form $4k + 3$ with integer k (that is, an integer that is larger by 3 than a multiple of 4) can never be written as a sum of two perfect squares. (Thus, $3, 7, 11, 15, 19, 23, \ldots$ cannot be written in this way.) This does not account for all integers that cannot be written in this way, but it does provide some clues to the answer that we will later see. In order to prove this observation, we shall need basic modular arithmetic (or at least division with remainder); we will see this proof very soon (see Exercise 2.7.2 **(c)**).

We will resolve Question 1.4.1 using the theory of Gaussian integers in Chapter 4. For a survey of different approaches to Question 1.4.1 (including a full answer using finite fields), see [AigZie18, Chapter 4].

Further questions can be asked. One of them is: Given an integer n, how many ways are there to represent n as a sum of two perfect squares? This is actually several questions masquerading as one, since it is not so clear what a "way" is. Do $5 = 1^2 + 2^2$ and $5 = 2^2 + 1^2$ count as two different ways? What about $5 = 1^2 + 2^2$ versus $5 = (-1)^2 + 2^2$ (here, the perfect squares are the same, but do we really want to count the squares or rather the numbers we are squaring?).

Let me formalize the question as follows:

Question 1.4.2. Let n be an integer.

(a) How many pairs $(a, b) \in \mathbb{N}^2$ are there that satisfy $n = a^2 + b^2$? Here, and in the following, $\mathbb{N}$ denotes the set $\{0, 1, 2, \ldots\}$ of all nonnegative integers.

(b) How many pairs $(a, b) \in \mathbb{Z}^2$ are there that satisfy $n = a^2 + b^2$? Here, and in the following, $\mathbb{Z}$ denotes the set $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$ of all integers.

(c) How do these counts change if we count **unordered** pairs instead (i.e., count (a, b) and (b, a) as one only)?

Note that when I say "pair", I always mean "ordered pair" by default, unless I explicitly say "unordered pair".

Again, a little bit of programming easily yields answers to all three parts of this question for small values of n, and the resulting data can be plugged into the OEIS and yields lots of information.

Note that sums of squares have a geometric meaning (going back to Pythagoras): Two real numbers a and b satisfy $a^2 + b^2 = n$ (for a given integer $n \geq 0$) if and only if the point with Cartesian coordinates (a, b) lies on the circle with center 0 and radius $\sqrt{n}$. This will actually prove a valuable insight that will lead us to the answers to the above questions.

Just as a teaser: There are formulas for all three parts of Question 1.4.2, in terms of divisors of n of the forms $4k + 1$ and $4k + 3$. We will see these formulas after we have properly understood the concept of Gaussian integers.

1.5. Motivation: Algebraic numbers

A real number z is said to be *algebraic* if there exists a nonzero polynomial P with rational coefficients such that $P(z) = 0$. In other words, a real number z is algebraic if and only if it is a root of a nonzero polynomial with rational coefficients.

(If you know the complex numbers, you can replace "real" by "complex" in this definition; but we shall only see real numbers in this little motivational section.)

Here are a few examples:

- Each rational number a is algebraic (being a root of the nonzero polynomial $x - a$ with rational coefficients).
- The number $\sqrt{2}$ is algebraic (being a root of the nonzero polynomial $x^2 - 2$).
- The number $\sqrt[3]{5}$ is algebraic (being a root of $x^3 - 5$).

- All the roots of the polynomial $f(x) := \frac{3}{2}x^4 + 17x^3 - 12x + \frac{9}{4}$ (whatever they are) are algebraic.
  Speaking of these roots, what are they? Using a computer, one can show that this polynomial $f(x)$ has 4 real roots $(-11.269\ldots, -0.960\ldots, 0.198\ldots, 0.697\ldots)$, which can be written as complicated expressions with radicals (i.e., $\sqrt[k]{}$ signs), though complex numbers appear in these expressions (despite the roots being real!). All this does not matter to the fact that they are algebraic $\ddot{\smile}$

- All the roots of the polynomial $g(x) := x^7 - x^5 + 1$ are algebraic.
  This polynomial has only one real root. This root cannot be written as an expression with radicals (as can be proven using Galois theory – indeed, the discovery of this theory greatly motivated the development of abstract algebra). Nevertheless, it is algebraic, by definition. (The same holds for the remaining 6 complex roots of g – we are working with real numbers here only for the sake of familiarity.)

- The most famous number that is not algebraic is π. This is a famous result of Lindemann, but it belongs to analysis, not to algebra, because π is not defined algebraically in the first place (it is defined as the length of a curve or as an area of a curved region – but either of these definitions boils down to a limit of a sequence).

- The second most famous number that is not algebraic is Euler's number e (the basis of the natural logarithm). Again, analysis is needed to define e, and thus also to prove its non-algebraicity.

Numbers that are not algebraic are called *transcendental*. We shall not study them much, since most of them do not come from algebra. Instead, we shall try our hands at the following question:

Question 1.5.1. **(a)** Is the sum of two (or, more generally, finitely many) algebraic numbers always algebraic?
(b) What if we replace "sum" by "difference" or "product"?

Let me motivate why this is a natural question to ask. The sum of two integers is still an integer; the sum of two rational numbers is still a rational number. These facts are fundamental; without them we could hardly work with integers and rational numbers. If a similar fact would not hold for algebraic numbers, it would mean that the algebraic numbers are not a good "number system" to work in; on a practical level, it would mean that (e.g.) if we defined a function on the set of all algebraic numbers, then we could not plug a sum of algebraic numbers into it.

1.6. Motivation: Shamir's Secret Sharing Scheme

1.6.1. The problem

Adi Shamir is one of the founders of modern mathematical cryptography (famous in particular for the RSA cryptosystem, which we will discuss in Subsection 3.8.1).

Shamir's Secret Sharing Scheme is a way in which a secret $\mathbf{a}$ (a piece of data – e.g., nuclear launch codes) can be distributed among n people in such a way that

- any k of them can (if they come together) reconstruct it uniquely, but
- any $k-1$ of them (if they come together) cannot gain **any** insight about it (i.e., not only cannot they reconstruct it, but they cannot even tell that some values are more likely than others to be $\mathbf{a}$).

Here n and k are fixed positive integers.

Understanding this scheme completely will require some abstract algebra, but we can already start thinking about the problem and get reasonably far.

So we have n people $1, 2, \ldots, n$, a positive integer $k \in \{1, 2, \ldots, n\}$ and a secret piece of data $\mathbf{a}$. We assume that this data $\mathbf{a}$ is encoded as a *bitstring* – i.e., a finite sequence of bits. A *bit* is an element of the set $\{0, 1\}$. Thus, examples of bitstrings are $(0, 1, 1, 0)$ and $(1, 0)$ and $(1, 1, 0, 1, 0, 0, 0)$ as well as the empty sequence $()$. When writing bitstring, we shall usually omit both the commas and the parentheses; thus, e.g., the bitstring $(1, 1, 0, 1, 0, 0, 0)$ will become 1101000. Make sure you don't mistake it for a number. Our goal is to give each of the n people $1, 2, \ldots, n$ some bitstring in such a way that:

- *Requirement 1:* Any k of the n people can (if they come together) reconstruct $\mathbf{a}$ uniquely.
- *Requirement 2:* Any $k-1$ of the n people are unable to gain any insight about $\mathbf{a}$ (even if they collaborate).

We denote the bitstrings given to the people $1, 2, \ldots, n$ by $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_n$, respectively.

We assume that the length of our secret bitstring $\mathbf{a}$ is known in advance to all parties; i.e., it is not a secret. Thus, when we say "$k-1$ persons cannot gain any insight about $\mathbf{a}$", we do not mean that they don't know the length; and when we say "some values are more likely than others to be $\mathbf{a}$", we only mean values that fit this length.

1.6.2. The $k = 1$ case

One simple special case of our problem is when $k = 1$. In this case, it suffices to give each of the n people the full secret $\mathbf{a}$ (that is, we set $\mathbf{a}_i = \mathbf{a}$ for all i). Then, Requirement 1 is satisfied (since any 1 of the n people already knows $\mathbf{a}$), while Requirement 2 is satisfied as well (0 people know nothing).

1.6.3. The $k = n$ case: what doesn't work

Let us now consider the case when $k = n$. This case will not help us solve the general problem, but it will show some ideas that we will encounter again and again in abstract algebra.

We want to ensure that all n people needed to reconstruct the secret $\mathbf{a}$, while any $n-1$ of them will be completely clueless.

It sounds reasonable to split $\mathbf{a}$ into n parts, and give each person one of these parts[1] (i.e., we let $\mathbf{a}_i$ be the i-th part of $\mathbf{a}$ for each $i \in \{1, 2, \ldots, n\}$). This method satisfies Requirement 1 (indeed, all n people together can reconstruct $\mathbf{a}$ simply by fusing the n parts back together), but fails Requirement 2 (indeed, any $n-1$ people know $n-1$ parts of the secret $\mathbf{a}$, which is a far from being clueless about $\mathbf{a}$). So this method doesn't work. It is not that easy.

1.6.4. The XOR operations

One way to solve the $k = n$ case is using the XOR operation.

Let us first define some basic language. A *binary operation* on a set S is (informally speaking) a function that takes two elements of S and assigns a new element of S to them. More formally:

Definition 1.6.1. A *binary operation* on a set S is a map f from $S \times S$ to S. When f is a binary operation on S and a and b are two elements of S, we shall write afb for the value $f(a, b)$.

Example 1.6.2. Addition, subtraction and multiplication of integers are three binary operations on the set $\mathbb{Q}$ (the set of all rational numbers). For example, addition is the map from $\mathbb{Q} \times \mathbb{Q}$ to $\mathbb{Q}$ that sends each pair $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ to $a + b$.

Division is not a binary operation on the set $\mathbb{Q}$. Indeed, if it was, then it would send the pair $(1, 0)$ to some integer called $1/0$; but there is no such integer.

There are myriad more complicated binary operations around waiting for someone to name them. For example, you could define a binary operation $\odot$ on the set $\mathbb{Q}$ by $a \odot b = \dfrac{a-b}{1+a^2+b^2}$. Indeed, you can do this because $1 + a^2 + b^2$ is always nonzero when $a, b \in \mathbb{Q}$ (after all, squares are nonnegative, so that $1 + \underbrace{a^2}_{\geq 0} + \underbrace{b^2}_{\geq 0} \geq 1 > 0$). I am not saying that you should...

Now, we define some specific binary operations on the set $\{0, 1\}$ of all bits, and on the set $\{0, 1\}^n$ of all length-n bitstrings (for a given n).

[1] assuming that $\mathbf{a}$ is long enough for that

Definition 1.6.3. We define a binary operation XOR on the set $\{0,1\}$ by setting

$$\begin{aligned} 0 \operatorname{XOR} 0 &= 0, \\ 0 \operatorname{XOR} 1 &= 1, \\ 1 \operatorname{XOR} 0 &= 1, \\ 1 \operatorname{XOR} 1 &= 0. \end{aligned}$$

This is a valid definition, because there are only four pairs $(a,b) \in \{0,1\} \times \{0,1\}$, and we have just defined $a \operatorname{XOR} b$ for each of these four options. We can also rewrite this definition as follows:

$$a \operatorname{XOR} b = \begin{cases} 1, & \text{if } a \neq b; \\ 0, & \text{if } a = b \end{cases} = \begin{cases} 1, & \text{if } \textbf{exactly} \text{ one of } a \text{ and } b \text{ is 1;} \\ 0, & \text{otherwise.} \end{cases}$$

For lack of a better name, we refer to $a \operatorname{XOR} b$ as the "XOR of a and b".

The name "XOR" is short for "exclusive or". In fact, if you identify bits with boolean truth values (so the bit 0 stands for "False" and the bit 1 stands for "True"), then $a \operatorname{XOR} b$ is precisely the truth value for "exactly one of a and b is True", which is also known as "a exclusive-or b".

Definition 1.6.4. Let m be a nonnegative integer. We define a binary operation XOR on the set $\{0,1\}^m$ (this is the set of all length-m bitstrings) by

$$(a_1, a_2, \ldots, a_m) \operatorname{XOR} (b_1, b_2, \ldots, b_m) = (a_1 \operatorname{XOR} b_1, a_2 \operatorname{XOR} b_2, \ldots, a_m \operatorname{XOR} b_m).$$

In other words, if $\mathbf{a}$ and $\mathbf{b}$ are two length-m bitstrings, then $\mathbf{a} \operatorname{XOR} \mathbf{b}$ is obtained by taking the XOR of each entry of $\mathbf{a}$ with the corresponding entry of $\mathbf{b}$, and packing these m XORs into a new length-m bitstring.

For example,

$$\begin{aligned} (1001) \operatorname{XOR} (1100) &= 0101; \\ (11011) \operatorname{XOR} (10101) &= 01110; \\ (11010) \operatorname{XOR} (01011) &= 10001; \\ (1) \operatorname{XOR} (0) &= 1; \\ () \operatorname{XOR} () &= (). \end{aligned}$$

Note that if $\mathbf{a}$ and $\mathbf{b}$ are two length-m bitstrings, then the 0's in the bitstring $\mathbf{a} \operatorname{XOR} \mathbf{b}$ are at the positions where $\mathbf{a}$ and $\mathbf{b}$ have equal entries, and the 1's in $\mathbf{a} \operatorname{XOR} \mathbf{b}$ are at the positions where $\mathbf{a}$ and $\mathbf{b}$ have different entries. Thus, $\mathbf{a} \operatorname{XOR} \mathbf{b}$ essentially pinpoints the differences between $\mathbf{a}$ and $\mathbf{b}$.

We observe the following simple properties of these operations XOR on bits and on bitstrings[2]:

- We have $a \operatorname{XOR} 0 = a$ for any bit a. (This can be trivially checked by considering both possibilities for a.)
- Thus, $\mathbf{a} \operatorname{XOR} \mathbf{0} = \mathbf{a}$ for any bitstring $\mathbf{a}$, where $\mathbf{0}$ denotes the bitstring $00\cdots0 = (0,0,\ldots,0)$ (of appropriate length – i.e., of the same length as $\mathbf{a}$).
- We have $a \operatorname{XOR} a = 0$ for any bit a. (This can be trivially checked by considering both possibilities for a.)
- Thus, $\mathbf{a} \operatorname{XOR} \mathbf{a} = \mathbf{0}$ for any bitstring $\mathbf{a}$. We shall refer to this as the *self-cancellation law*.
- We have $a \operatorname{XOR} b = b \operatorname{XOR} a$ for any bits a, b. (Again, this is easy to check by going through all four options for a and b.)
- Thus, $\mathbf{a} \operatorname{XOR} \mathbf{b} = \mathbf{b} \operatorname{XOR} \mathbf{a}$ for any bitstrings $\mathbf{a}, \mathbf{b}$.
- We have $a \operatorname{XOR} (b \operatorname{XOR} c) = (a \operatorname{XOR} b) \operatorname{XOR} c$ for any bits a, b, c. (Again, this is easy to check by going through all eight options for a, b, c.)
- Thus, $\mathbf{a} \operatorname{XOR} (\mathbf{b} \operatorname{XOR} \mathbf{c}) = (\mathbf{a} \operatorname{XOR} \mathbf{b}) \operatorname{XOR} \mathbf{c}$ for any bitstrings $\mathbf{a}, \mathbf{b}, \mathbf{c}$.
- Thus, for any bitstrings $\mathbf{a}$ and $\mathbf{b}$, we have

$$(\mathbf{a} \operatorname{XOR} \mathbf{b}) \operatorname{XOR} \mathbf{b} = \mathbf{a} \operatorname{XOR} \underbrace{(\mathbf{b} \operatorname{XOR} \mathbf{b})}_{=\mathbf{0}} = \mathbf{a} \operatorname{XOR} \mathbf{0} = \mathbf{a}.$$

(by the self-cancellation law)

This observation gives rise to a primitive cryptosystem (known as a *one-time pad*): If you have a secret bitstring $\mathbf{a}$ that you want to encrypt, and another secret bitstring $\mathbf{b}$ that can be used as a key, then you can encrypt $\mathbf{a}$ by XORing it with $\mathbf{b}$ (that is, you transform it into $\mathbf{a} \operatorname{XOR} \mathbf{b}$). Then, you can decrypt it again by XORing it with $\mathbf{b}$ again; indeed, if you do this, you will obtain $(\mathbf{a} \operatorname{XOR} \mathbf{b}) \operatorname{XOR} \mathbf{b} = \mathbf{a}$. This is a highly safe cryptosystem as long as you can safely communicate the key $\mathbf{b}$ to whomever needs to be able to decrypt (or encrypt) your secrets, and as long as you are able to generate uniformly random keys $\mathbf{b}$ of sufficient length. Its only weakness is its impracticality (in many situations): If the secret you want to encrypt is long (say, a whole book), your key will need to be equally long. Even storing such keys can become difficult.

[2] As a mnemonic, we shall try to use boldfaced letters like $\mathbf{a}$ and $\mathbf{b}$ for bitstrings and regular italic letters like a and b for single bits.

We shall refer to the properties $a \operatorname{XOR} b = b \operatorname{XOR} a$ and $\mathbf{a} \operatorname{XOR} \mathbf{b} = \mathbf{b} \operatorname{XOR} \mathbf{a}$ as *laws of commutativity*, and we shall refer to the properties $a \operatorname{XOR} (b \operatorname{XOR} c) = (a \operatorname{XOR} b) \operatorname{XOR} c$ and $\mathbf{a} \operatorname{XOR} (\mathbf{b} \operatorname{XOR} \mathbf{c}) = (\mathbf{a} \operatorname{XOR} \mathbf{b}) \operatorname{XOR} \mathbf{c}$ as *laws of associativity*. These are, of course, similar to well-known facts like $\alpha + \beta = \beta + \alpha$ and $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for numbers α, β, γ (which is why we are giving them the same names). This similarity is not coincidental. Just as for addition or multiplication of numbers, these laws lead to a notion of "XOR-products":

Proposition 1.6.5. Let m be a positive integer. Let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_m$ be m bitstrings. Then, the "XOR-product" expression

$$\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3 \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_m$$

is well-defined, in the sense that it does not depend on the parenthesization.

What do we mean by "parenthesization"? To clarify things, let us set $m = 4$. In this case, we want to make sense of the expression $\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4$. This expression does not make sense a priori, since it is a XOR of **four** bitstrings, whereas we have defined only the XOR of **two** bitstrings. But there are five ways to put parentheses around some of its sub-expressions such that the expression becomes meaningful:

$$\begin{aligned}
&(\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2) \operatorname{XOR} (\mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4), \\
&((\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2) \operatorname{XOR} \mathbf{a}_3) \operatorname{XOR} \mathbf{a}_4, \\
&\mathbf{a}_1 \operatorname{XOR} ((\mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3) \operatorname{XOR} \mathbf{a}_4), \\
&\mathbf{a}_1 \operatorname{XOR} (\mathbf{a}_2 \operatorname{XOR} (\mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4)), \\
&(\mathbf{a}_1 \operatorname{XOR} (\mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3)) \operatorname{XOR} \mathbf{a}_4.
\end{aligned}$$

Each of these five parenthesizations (= placements of parentheses) turns our expression $\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4$ into a combination of XOR's of **two** bitstrings each, and thus gives it meaning. The question is: Do these five parenthesizations give it the **same** meaning?

Well, let us calculate:

$$\begin{aligned}
&(\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2) \operatorname{XOR} (\mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4) \\
&= \mathbf{a}_1 \operatorname{XOR} \underbrace{(\mathbf{a}_2 \operatorname{XOR} (\mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4))}_{= (\mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3) \operatorname{XOR} \mathbf{a}_4} \\
&= \mathbf{a}_1 \operatorname{XOR} ((\mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3) \operatorname{XOR} \mathbf{a}_4) \\
&= \underbrace{(\mathbf{a}_1 \operatorname{XOR} (\mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3))}_{= (\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2) \operatorname{XOR} \mathbf{a}_3} \operatorname{XOR} \mathbf{a}_4 \\
&= ((\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2) \operatorname{XOR} \mathbf{a}_3) \operatorname{XOR} \mathbf{a}_4,
\end{aligned}$$

where we used the law of associativity in each step. This shows that our five parenthesizations yield the same result. Thus, they all give our "XOR-product"

expression $\mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \mathbf{a}_3 \operatorname{XOR} \mathbf{a}_4$ the same meaning; so we can say that this expression is well-defined. This confirms Proposition 1.6.5 for $m = 4$.

Of course, proving Proposition 1.6.5 is less simple. Such a proof appears in Exercise 4 on homework set #0 (for more general binary operations than XOR).

1.6.5. The $k = n$ case: an answer

Let us now return to our problem. We have n persons $1, 2, \ldots, n$ and a secret $\mathbf{a}$ (encoded as a bitstring). We want to give each person i some bitstring $\mathbf{a}_i$ such that only all n of them can recover $\mathbf{a}$ but any $n-1$ of them cannot gain any insight about $\mathbf{a}$.

We let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{n-1}$ be $n-1$ **uniformly** random bitstrings of the same length as $\mathbf{a}$. (Think of them as random gibberish.) Set

$$\mathbf{a}_n = \mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_{n-1}.$$

(This expression makes sense because of Proposition 1.6.5.)

Then,

$$\begin{aligned}
&\mathbf{a}_n \operatorname{XOR} \mathbf{a}_{n-1} \operatorname{XOR} \mathbf{a}_{n-2} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_1 \\
&= (\mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_{n-1}) \operatorname{XOR} \mathbf{a}_{n-1} \operatorname{XOR} \mathbf{a}_{n-2} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_1 \\
&= \mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \underbrace{\mathbf{a}_{n-1} \operatorname{XOR} \mathbf{a}_{n-1}}_{=\mathbf{0}} \operatorname{XOR} \mathbf{a}_{n-2} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_1 \\
&= \mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \underbrace{\mathbf{a}_{n-2} \operatorname{XOR} \mathbf{0}}_{=\mathbf{a}_{n-2}} \operatorname{XOR} \mathbf{a}_{n-2} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_1 \\
&= \mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \underbrace{\mathbf{a}_{n-2} \operatorname{XOR} \mathbf{a}_{n-2}}_{=\mathbf{0}} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_1 \\
&= \cdots \\
&= \mathbf{a}
\end{aligned}$$

(here, we have been unravelling the big XOR-product from the middle on, by cancelling equal bitstrings using the self-cancellation law and then removing the resulting $\mathbf{0}$ using the $\mathbf{a} \operatorname{XOR} \mathbf{0} = \mathbf{a}$ law). Hence, the n people together can decrypt the secret $\mathbf{a}$.

Can $n-1$ people gain any insight about it? The $n-1$ people $1, 2, \ldots, n-1$ certainly cannot, since all they know are the random bitstrings $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{n-1}$. But the $n-1$ people $2, 3, \ldots, n$ cannot gain any insight about $\mathbf{a}$ either: In fact, all they know are the random bitstrings $\mathbf{a}_2, \mathbf{a}_3, \ldots, \mathbf{a}_{n-1}$ and the bitstring

$$\mathbf{a}_n = \mathbf{a} \operatorname{XOR} \mathbf{a}_1 \operatorname{XOR} \mathbf{a}_2 \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{a}_{n-1};$$

therefore, all the information they have about $\mathbf{a}$ and $\mathbf{a}_1$ comes to them through $\mathbf{a} \operatorname{XOR} \mathbf{a}_1$, which says nothing about $\mathbf{a}$ as long as they know nothing about $\mathbf{a}_1$. (We used a bit of handwaving in this argument, but then again we never formally

defined what it means to "gain no insight"; this is done in courses on cryptography and information theory.) Similar arguments show that any other choice of $n-1$ persons remains equally clueless about $\mathbf{a}$. So we have solved the problem in the case $k = n$.

1.6.6. The $k = 2$ case

The next simple case is when $k = 2$. So we want to ensure that any 2 of our n people can together recover the secret, but no 1 person can learn anything about it alone.

A really nice approach was suggested by Nathan (a student in class): We pick n random bitstrings $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{n-1}$ of the same length as $\mathbf{a}$. Set

$$\mathbf{x}_n = \mathbf{a} \operatorname{XOR} \mathbf{x}_1 \operatorname{XOR} \mathbf{x}_2 \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{x}_{n-1};$$

thus, as in the $k = n$ case, we have

$$\mathbf{x}_n \operatorname{XOR} \mathbf{x}_{n-1} \operatorname{XOR} \mathbf{x}_{n-2} \operatorname{XOR} \cdots \operatorname{XOR} \mathbf{x}_1 = \mathbf{a}. \tag{2}$$

Each person i now receives the bitstring

$$\mathbf{a}_i = \mathbf{x}_1 \mathbf{x}_2 \cdots \mathbf{x}_{i-1} \mathbf{x}_{i+1} \mathbf{x}_{i+2} \cdots \mathbf{x}_n,$$

where the product stands for *concatenation* (i.e., the bitstring $\mathbf{a}_i$ is formed by writing down all of the bitstrings $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ one after the other but skipping $\mathbf{x}_i$). Thus, each person i can recover all the $n-1$ bitstrings $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_{i-1}, \mathbf{x}_{i+1}, \mathbf{x}_{i+2}, \ldots, \mathbf{x}_n$ (because their lengths are the length of $\mathbf{a}$, which is known), but knows nothing about $\mathbf{x}_i$ (his "blind spot"). Hence, 2 people together can recover all the n bitstrings $\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_n$ and therefore recover the secret $\mathbf{a}$ (by (2)). On the other hand, each single person has no insight about $\mathbf{a}$ (this is proven similarly to the $k = n$ case). So again, the problem is solved in this case.

1.6.7. The $k = 3$ case

Now, let us come to the case when $k = 3$. Here, I think, the usefulness of the XOR approach has come to its end: at least, I don't know how to make it work here. Instead, out of the blue, I will invoke something completely different: polynomials (let's say with rational coefficients).

Recall a fact you might have heard in high school:

Proposition 1.6.6. A polynomial $\mathbf{f}(x) = cx^2 + bx + a$ of degree ≤ 2 is uniquely determined by any three of its values. More precisely: If u, v, w are three fixed distinct numbers, then a polynomial $\mathbf{f}(x) = cx^2 + bx + a$ of degree ≤ 2 is uniquely determined by the values $\mathbf{f}(u), \mathbf{f}(v), \mathbf{f}(w)$.

> More precisely: If u, v, w are three fixed distinct numbers, and if p, q, r are three arbitrary numbers, then there is a unique polynomial $\mathbf{f}(x) = cx^2 + bx + a$ of degree ≤ 2 satisfying
>
> $$\mathbf{f}(u) = p, \qquad \mathbf{f}(v) = q, \qquad \text{and} \qquad \mathbf{f}(w) = r.$$

Here, the word "number" is deliberately left ambiguous, but you can think of rational or real numbers (Proposition 1.6.6 is definitely true for them).

Also recall that any bitstring of given length N can be encoded as an integer in $\{0, 1, \ldots, 2^N - 1\}$: Just read it as a number in binary. More precisely, any bitstring $a_{N-1}a_{N-2}\cdots a_0$ of length N becomes the integer $a_{N-1} \cdot 2^{N-1} + a_{N-2} \cdot 2^{N-2} + \cdots + a_0 \cdot 2^0 \in \{0, 1, \ldots, 2^N - 1\}$. For example, the bitstring 010110 of length 6 becomes the integer

$$0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 22 \in \left\{0, 1, \ldots, 2^6 - 1\right\}.$$

Choose two **uniformly random** bitstrings **c** and **b** (of the same length as **a**) and encode them as numbers c and b (as just explained). Encode the secret **a** as a number a as well (in the same way). Define the polynomial $\mathbf{f}(x) = cx^2 + bx + a$. Reveal to each person $i \in \{1, 2, \ldots, n\}$ the value $\mathbf{f}(i)$ – or, rather, a bitstring that encodes it in binary – as $\mathbf{a}_i$.

Any three of the n values $\mathbf{f}(i)$ uniquely determine the polynomial **f** (because of Proposition 1.6.6). Thus, any three people can use their bitstrings $\mathbf{a}_i$ to recover three values $\mathbf{f}(i)$ and therefore **f** and therefore a (as the constant term of **f**) and therefore **a** (by decoding a). So our method satisfies Requirement 1.

Now, let us see whether it satisfies Requirement 2. Any 2 people can recover two values $\mathbf{f}(i)$, which generally do not determine **f** uniquely. It is not hard to show that they do not even determine a uniquely; thus, they do not determine **a** uniquely. What's better: If you know just two values of **f**, there are infinitely many possible choices for **f**, and all of them have distinct constant terms (unless one of the two values you know is $\mathbf{f}(0)$, which of course pins down the constant term)[3]. So we get infinitely many possible values for a, and thus infinitely many possible values for **a**. This means that our 2 people don't gain any insight about **a**, right?

Not so fast! We cannot really have "infinitely many possible values for **a**", since **a** is bound to be a bitstring of a given length – there are only finitely many of those! You can only get infinitely many possible values for **f** if you forget how **f** was constructed (from c, b and a) and pretend that **f** is just a "uniformly random" polynomial (whatever this means). But no one can force the 2 people to do this; it is certainly not in their interest! Here are some things they might do with this knowledge:

[3] Prove this! (**Hint:** The constant term of a polynomial is just its value at 0. Thus, if you know two values of **f** at points other than 0 and also the constant term of **f**, then you simply know three values of **f**.)

- Let N be the length of **a** (which, as we said, is known). Thus, **c** and **b** are bitstrings of length N, so that c and b are integers in $\{0, 1, \ldots, 2^N - 1\}$. Assume that one of the 2 people is person 2. Now, person 2 knows $\mathbf{f}(2) = c2^2 + b2 + a = 4c + 2b + a$, and thus knows whether a is even or odd (because a is even resp. odd if and only if $4c + 2b + a$ is even resp. odd). This means she knows the last bit of the secret **a**. This is not "clueless".

- You might try to fix this by picking c and b to be uniformly random rational numbers instead (rather than using uniformly random bitstrings **c** and **b**).

  Unfortunately, there is no such thing as a "uniformly random rational number" (in the sense that, e.g., larger numbers aren't less likely to be picked than smaller numbers). Any probability distribution will make some numbers more likely than others, and this will usually cause information about **a** to "leak". For example, if c and b are chosen from the interval $[0, 2^N - 1]$, then person 1's knowledge of $\mathbf{f}(1) = c1^2 + b1 + a = c + b + a$ will sometimes reveal to person 1 that $a \geq 0.5 \cdot (2^N - 1)$ (namely, this will happen when $\mathbf{f}(1) \geq 2.5 \cdot (2^N - 1)$, which occasionally happens). This, again, is nontrivial information about the secret **a**, which a single person (or even two people) should not be having.

So we cannot make Requirement 2 hold, and the culprit is that there are too many numbers (namely, infinitely many). What would help is a finite "number system" in which we can add, subtract, multiply and divide (so that we can define polynomials over it, and a polynomial of degree ≤ 2 is still uniquely determined by any 3 values). Assuming that this "number system" is large enough that we can encode bitstrings using "numbers" of this system (instead of integers), we can then play the above game using this "number system" and obtain actually uniformly random numbers.

It turns out that such "number systems" exist. They are called *finite fields*, and we will construct them later in this course.

Assuming that they can be constructed, we thus obtain a method of solving the problem for $k = 3$. A similar method works for arbitrary k, using polynomials of degree $\leq k - 1$. This is called *Shamir's Secret Sharing Scheme*.

2. Elementary number theory

Let us now begin a systematic introduction to algebra. We start with studying integers and their divisibility properties – the beginnings of number theory. Part of these will be used directly in what will follow; part of these will inspire more general results and proofs.

2.1. Notations

Definition 2.1.1. Let $\mathbb{N} = \{0, 1, 2, \ldots\}$ be the set of **nonnegative** integers.
Let $\mathbb{P} = \{1, 2, 3, \ldots\}$ be the set of **positive** integers.
Let $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$ be the set of integers.
Let $\mathbb{Q}$ be the set of rational numbers.
Let $\mathbb{R}$ be the set of real numbers.

Be careful with the notation $\mathbb{N}$: While I use it for $\{0, 1, 2, \ldots\}$, various other authors use it for $\{1, 2, 3, \ldots\}$ instead. There is no consensus in sight on what $\mathbb{N}$ should mean.

Same holds for the word "natural number" (which I will avoid): It means "element of $\mathbb{N}$", so again its ultimate meaning depends on the author.

The word "list" shall always mean "ordered finite list" unless declared otherwise. Examples of lists of numbers are $(2, 5, 2)$, $(1, 9)$, the one-entry list (9) (not the same as the number 9 itself) and the empty list $()$. The word "tuple" means the same as "list", but more specifically, the word "k-tuple" (for some $k \in \mathbb{N}$) means "list with exactly k entries". For instance, $(5, 1, 5)$ is a 3-tuple. The word "sequence" means an ordered, but not necessarily finite, list.

2.2. Divisibility

We now go through the basics of divisibility of integers.

Definition 2.2.1. Let a and b be two integers. We say that $a \mid b$ (or "*a divides b*" or "*b is divisible by a*" or "*b is a multiple of a*") if there exists an integer c such that $b = ac$.
We furthermore say that $a \nmid b$ if a does not divide b.

Some authors define the "divisibility" relation a bit differently, in that they forbid $a = 0$. From the viewpoint of abstract algebra, this feels like an unnecessary exception, so we don't follow them.

Example 2.2.2. **(a)** We have $4 \mid 12$, since $12 = 4 \cdot 3$.
(b) We have $a \mid 0$ for any $a \in \mathbb{Z}$, since $0 = a \cdot 0$.
(c) An integer b satisfies $0 \mid b$ only when $b = 0$, since $0 \mid b$ implies $b = 0c = 0$ (for some $c \in \mathbb{Z}$).
(d) We have $a \mid a$ for any $a \in \mathbb{Z}$, since $a = a \cdot 1$.
(e) We have $1 \mid b$ for each $b \in \mathbb{Z}$, since $b = 1 \cdot b$.

I apologize in advance for the next proposition, in which vertical bars stand both for the "divides" relation and for the absolute value of a number. Unfortunately,

both of these uses are standard notation. Confusion is possible, but hopefully will not happen often[4].

Proposition 2.2.3. Let a and b be two integers.

(a) We have $a \mid b$ if and only if $|a| \mid |b|$. (Here, "$|a| \mid |b|$" means "$|a|$ divides $|b|$".)

(b) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

(c) Assume that $a \neq 0$. Then, $a \mid b$ if and only if $\dfrac{b}{a} \in \mathbb{Z}$.

Before we prove this proposition, let us recall a well-known fact: We have

$$|xy| = |x| \cdot |y| \tag{3}$$

for any two integers[5] x and y. (This can be easily proven by case distinction: x is either nonnegative or negative, and so is y.)

Proposition 2.2.3 **(a)** shows that both a and b in the statement "$a \mid b$" can be replaced by their absolute values. Thus, when we talk about divisibility of integers, the sign of the integers does not really matter – it usually suffices to work with nonnegative integers. We will often use this (tacitly, after a while) in proofs.

The next proposition shows some basic properties of the divisibility relation:

Proposition 2.2.4. (a) We have $a \mid a$ for every $a \in \mathbb{Z}$. (This is called the *reflexivity of divisibility*.)

(b) If $a, b, c \in \mathbb{Z}$ satisfy $a \mid b$ and $b \mid c$, then $a \mid c$. (This is called the *transitivity of divisibility*.)

(c) If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$, then $a_1 a_2 \mid b_1 b_2$.

Exercise 2.2.1. Let $a \in \mathbb{Z}$.

(a) Prove that $a \mid |a|$. (This means "a divides $|a|$".)

(b) Prove that $|a| \mid a$. (This means "$|a|$ divides a".)

Exercise 2.2.2. Let a and b be two integers such that $a \mid b$ and $b \mid a$. Prove that $|a| = |b|$.

Exercise 2.2.3. Let a, b, c be three integers such that $c \neq 0$. Prove that $a \mid b$ holds if and only if $ac \mid bc$.

[4] Unfortunately, the use of vertical bars for absolute values alone suffices to generate confusion! Just think of the meaning of "$|a|\,b\,|c|$" when a, b and c are three numbers. Does it stand for "$(|a|) \cdot b \cdot (|c|)$" (where I am using parentheses to make the ambiguity disappear) or for "$|(a \cdot |b| \cdot c)|$"? If you see any expressions in my notes that allow for more than one meaningful interpretation, please let me know!

[5] or real numbers

Exercise 2.2.4. Let $n \in \mathbb{Z}$. Let $a, b \in \mathbb{N}$ be such that $a \leq b$. Prove that $n^a \mid n^b$.

Exercise 2.2.5. Let g be a nonnegative integer such that $g \mid 1$. Prove that $g = 1$.

Exercise 2.2.6. Let $a, b \in \mathbb{Z}$ be such that $a \mid b$. Let $k \in \mathbb{N}$. Prove that $a^k \mid b^k$.

2.3. Congruence modulo n

The next definition is simple but crucial:

Definition 2.3.1. Let $n, a, b \in \mathbb{Z}$. We say that *a is congruent to b modulo n* if and only if $n \mid a - b$. We shall use the notation "$a \equiv b \bmod n$" for "a is congruent to b modulo n".

We furthermore shall use the notation "$a \not\equiv b \bmod n$" for "a is not congruent to b modulo n".

Example 2.3.2. **(a)** Is $3 \equiv 7 \bmod 2$? Yes, since $2 \mid 3 - 7 = -4$.

(b) Is $3 \equiv 6 \bmod 2$? No, since $2 \nmid 3 - 6 = -3$. So we have $3 \not\equiv 6 \bmod 2$.

Now, let a and b be two integers.

(c) We have $a \equiv b \bmod 0$ if and only if $a = b$. (Indeed, $a \equiv b \bmod 0$ is defined to mean $0 \mid a - b$, but the latter divisibility happens only when $a - b = 0$, which is tantamount to saying $a = b$.)

(d) We have $a \equiv b \bmod 1$ always, since $1 \mid a - b$ always holds (remember: 1 divides everything).

Note that being congruent modulo 2 means having the same parity: i.e., two even numbers will be congruent modulo 2, and two odd numbers will be, but an even number will never be congruent to an odd number modulo 2. (To be rigorous: This is not quite obvious at this point yet; but it will be easy once we have properly introduced division with remainder. See Exercise 2.7.1 **(i)** below for the proof.)

The word "modulo" in the phrase "a is congruent to b modulo n" originates with Gauss and means something like "with respect to". You should think of "a is congruent to b modulo n" as a relation between all three of the numbers a, b and n, but a and b are the "main characters" and n sets the scene.

Exercise 2.3.1. Let $a, b \in \mathbb{Z}$. Prove that $a + b \equiv a - b \bmod 2$.

We begin with a proposition so fundamental that we will always use it without saying:

Proposition 2.3.3. Let $n \in \mathbb{Z}$ and $a \in \mathbb{Z}$. Then, $a \equiv 0 \bmod n$ if and only if $n \mid a$.

Next come some staple properties of congruences:

Proposition 2.3.4. Let $n \in \mathbb{Z}$.
(a) We have $a \equiv a \bmod n$ for every $a \in \mathbb{Z}$.
(b) If $a, b, c \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$ and $b \equiv c \bmod n$, then $a \equiv c \bmod n$.
(c) If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$, then $b \equiv a \bmod n$.
(d) If $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \equiv b_1 \bmod n$ and $a_2 \equiv b_2 \bmod n$, then

$$a_1 + a_2 \equiv b_1 + b_2 \bmod n; \tag{4}$$
$$a_1 - a_2 \equiv b_1 - b_2 \bmod n; \tag{5}$$
$$a_1 a_2 \equiv b_1 b_2 \bmod n. \tag{6}$$

(e) Let $m \in \mathbb{Z}$ be such that $m \mid n$. If $a, b \in \mathbb{Z}$ satisfy $a \equiv b \bmod n$, then $a \equiv b \bmod m$.

In the above proof, we took care to explicitly cite Definition 2.2.1 and Definition 2.3.1 whenever we used them; in the following, we will omit references like this.

Proposition 2.3.4 **(d)** is saying that congruences modulo n (for a fixed integer n) can be added, subtracted and multiplied together. This does not mean that you can do everything with them that you can do with equalities. The next exercise shows that dividing congruences and taking a congruence to the power of another does not generally work:

Exercise 2.3.2. Let $n, a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \equiv b_1 \bmod n$ and $a_2 \equiv b_2 \bmod n$. Then, **in general**, neither $a_1/a_2 \equiv b_1/b_2 \bmod n$ nor $a_1^{a_2} \equiv b_1^{b_2} \bmod n$ is necessarily true. Of course, this is partly due to the fact that a_1/a_2, b_1/b_2 and $a_1^{a_2}$ and $b_1^{b_2}$ are not always integers in the first place (and being congruent modulo n only makes sense for integers, at least for now). But even when a_1/a_2, b_1/b_2 and $a_1^{a_2}$ and $b_1^{b_2}$ are integers, the congruences $a_1/a_2 \equiv b_1/b_2 \bmod n$ and $a_1^{a_2} \equiv b_1^{b_2} \bmod n$ are often false. Find examples of n, a_1, a_2, b_1, b_2 such that a_1/a_2, b_1/b_2 and $a_1^{a_2}$ and $b_1^{b_2}$ are integers but the congruences $a_1/a_2 \equiv b_1/b_2 \bmod n$ and $a_1^{a_2} \equiv b_1^{b_2} \bmod n$ are false.

However, we can divide a congruence $a \equiv b \bmod n$ by a nonzero integer d when all of a, b, n are divisible by d:

Exercise 2.3.3. Let $n, d, a, b \in \mathbb{Z}$, and assume that $d \neq 0$. Assume that d divides each of a, b, n, and assume that $a \equiv b \bmod n$. Prove that $a/d \equiv b/d \bmod n/d$.

We can also take a congruence to the k-th power when $k \in \mathbb{N}$:

Exercise 2.3.4. Let $n, a, b \in \mathbb{Z}$ be such that $a \equiv b \bmod n$. Prove that $a^k \equiv b^k \bmod n$ for each $k \in \mathbb{N}$.

(Note that the "n" is not being taken to the k-th power here.)
We can add not just two, but any finite number of congruences:

Exercise 2.3.5. Let n be an integer. Let S be a finite set. For each $s \in S$, let a_s and b_s be two integers. Assume that

$$a_s \equiv b_s \bmod n \qquad \text{for each } s \in S. \tag{7}$$

(a) Prove that

$$\sum_{s \in S} a_s \equiv \sum_{s \in S} b_s \bmod n. \tag{8}$$

(b) Prove that

$$\prod_{s \in S} a_s \equiv \prod_{s \in S} b_s \bmod n. \tag{9}$$

(Keep in mind that if the set S is empty, then $\sum_{s \in S} a_s = \sum_{s \in S} b_s = 0$ and $\prod_{s \in S} a_s = \prod_{s \in S} b_s = 1$; this holds by the definition of empty sums and of empty products.)

Exercise 2.3.6. Is it true that if $a_1, a_2, b_1, b_2, n_1, n_2 \in \mathbb{Z}$ satisfy $a_1 \equiv b_1 \bmod n_1$ and $a_2 \equiv b_2 \bmod n_2$, then $a_1 a_2 \equiv b_1 b_2 \bmod n_1 n_2$?

Exercise 2.3.7. Let $a, b, n \in \mathbb{Z}$. Prove that $a \equiv b \bmod n$ if and only if there exists some $d \in \mathbb{Z}$ such that $b = a + nd$.

Exercise 2.3.8. Let $a, b, c, n \in \mathbb{Z}$. Prove that we have $a - b \equiv c \bmod n$ if and only if $a \equiv b + c \bmod n$.

Exercise 2.3.9. Let $a, b, n \in \mathbb{Z}$. Prove that $a \equiv b \bmod n$ if and only if $a \equiv b \bmod -n$.

2.4. Chains of congruences

Convention 2.4.1. For this whole Section 2.4, we fix an integer n.

Chains of equalities are a fundamental piece of notation used throughout mathematics. For example, here is a chain of equalities:

$$\begin{aligned}
&(ad+bc)^2 + (ac-bd)^2 \\
&= (ad)^2 + 2ad \cdot bc + (bc)^2 + (ac)^2 - 2ac \cdot bd + (bd)^2 \\
&= a^2d^2 + 2abcd + b^2c^2 + a^2c^2 - 2abcd + b^2d^2 \\
&= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\
&= \left(a^2+b^2\right)\left(c^2+d^2\right)
\end{aligned}$$

(where a, b, c, d are arbitrary numbers). This chain proves the equality (1). But why does it really? If we look closely at this chain of equalities, we see that it has the form "$A = B = C = D = E$", where A, B, C, D, E are five numbers (namely, $A =$

$(ad+bc)^2+(ac-bd)^2$ and $B = (ad)^2+2ad\cdot bc+(bc)^2+(ac)^2-2ac\cdot bd+(bd)^2$ and so on). This kind of statement is called a "chain of equalities", and, a priori, it simply means that any two **adjacent** numbers in this chain are equal: $A = B$ and $B = C$ and $C = D$ and $D = E$. Without as much as noticing it, we have concluded that **any** two numbers in this chain are equal; thus, in particular, $A = E$, which is precisely the equality (1) we wanted to prove.

That this kind of "chaining" is possible is one of the most basic facts in mathematics. Let us define a chain of equalities formally:

Definition 2.4.2. If $a_1, a_2, \ldots, a_k$ are k objects[6], then the statement "$a_1 = a_2 = \cdots = a_k$" shall mean that

$$a_i = a_{i+1} \text{ holds for each } i \in \{1, 2, \ldots, k-1\}.$$

(In other words, it shall mean that $a_1 = a_2$ and $a_2 = a_3$ and $a_3 = a_4$ and $\cdots$ and $a_{k-1} = a_k$. This is vacuously true when $k \leq 1$. If $k = 2$, then it simply means that $a_1 = a_2$.)

Such a statement will be called a *chain of equalities*.

Proposition 2.4.3. Let $a_1, a_2, \ldots, a_k$ be k objects such that $a_1 = a_2 = \cdots = a_k$. Let u and v be two elements of $\{1, 2, \ldots, k\}$. Then, $a_u = a_v$.

So we have defined a chain of equalities to be true if and only if any two adjacent terms in this chain are equal (i.e., if "each equality sign in the chain is satisfied"). Proposition 2.4.3 shows that in such a chain, **any two** terms are equal. This is intuitively rather clear, but can also be formally proven by induction using the basic properties of equality (transitivity[7], reflexivity[8] and symmetry[9]).

But our goal is to understand basic number theory, not to scrutinize the foundations of mathematics. So let us recall that we have fixed an integer n, and consider congruences modulo n. We claim that these can be chained just as equalities:

Definition 2.4.4. If $a_1, a_2, \ldots, a_k$ are k integers, then the statement "$a_1 \equiv a_2 \equiv \cdots \equiv a_k \bmod n$" shall mean that

$$a_i \equiv a_{i+1} \bmod n \text{ holds for each } i \in \{1, 2, \ldots, k-1\}.$$

(In other words, it shall mean that $a_1 \equiv a_2 \bmod n$ and $a_2 \equiv a_3 \bmod n$ and $a_3 \equiv a_4 \bmod n$ and $\cdots$ and $a_{k-1} \equiv a_k \bmod n$. This is vacuously true when $k \leq 1$. If $k = 2$, then it simply means that $a_1 \equiv a_2 \bmod n$.)

Such a statement will be called a *chain of congruences modulo n*.

[6] "Objects" can be numbers, sets, tuples or any other well-defined things in mathematics.

[7] *Transitivity of equality* says that if a, b, c are three objects satisfying $a = b$ and $b = c$, then $a = c$.

[8] *Reflexivity of equality* says that every object a satisfies $a = a$.

[9] *Symmetry of equality* says that if a, b are two objects satisfying $a = b$, then $b = a$.

Proposition 2.4.5. Let $a_1, a_2, \ldots, a_k$ be k integers such that $a_1 \equiv a_2 \equiv \cdots \equiv a_k \bmod n$. Let u and v be two elements of $\{1, 2, \ldots, k\}$. Then, $a_u \equiv a_v \bmod n$.

Proposition 2.4.5 shows that any two terms in a chain of congruences modulo n must be congruent to each other modulo n. Again, this can be formally proven by induction; see [Grinbe15, proof of Proposition 2.16]. The ingredients of the proof are basic properties of congruence modulo n: transitivity, reflexivity and symmetry. These are fancy names for parts **(b)**, **(a)** and **(c)** of Proposition 2.3.4.

We will use Proposition 2.4.5 tacitly (just as you would use Proposition 2.4.3): i.e., every time we prove a chain of congruences like $a_1 \equiv a_2 \equiv \cdots \equiv a_k \bmod n$, we assume that the reader will automatically conclude that any two of its terms are congruent to each other modulo n (and will remember this conclusion). For instance, if we show that $1 \equiv 4 \equiv 34 \equiv 334 \equiv 304 \bmod 3$, then we automatically get the congruences $1 \equiv 304 \bmod 3$ and $334 \equiv 1 \bmod 3$ and $4 \equiv 334 \bmod 3$ and several others out of this chain.

Chains of congruences can also include equality signs. For example, if a, b, c, d are integers, then "$a \equiv b = c \equiv d \bmod n$" means that $a \equiv b \bmod n$ and $b = c$ and $c \equiv d \bmod n$. Such a chain is still a chain of congruences, because $b = c$ implies $b \equiv c \bmod n$ (by Proposition 2.3.4 **(a)**).

Just as there are chains of equalities and chains of congruences, there are chains of divisibilities:

Definition 2.4.6. If $a_1, a_2, \ldots, a_k$ are k integers, then the statement "$a_1 \mid a_2 \mid \cdots \mid a_k$" shall mean that

$$a_i \mid a_{i+1} \text{ holds for each } i \in \{1, 2, \ldots, k-1\}.$$

(In other words, it shall mean that $a_1 \mid a_2$ and $a_2 \mid a_3$ and $a_3 \mid a_4$ and $\cdots$ and $a_{k-1} \mid a_k$. This is vacuously true when $k \leq 1$. If $k = 2$, then it simply means that $a_1 \mid a_2$.)

Such a statement will be called a *chain of divisibilities*.

Proposition 2.4.7. Let $a_1, a_2, \ldots, a_k$ be k integers such that $a_1 \mid a_2 \mid \cdots \mid a_k$. Let u and v be two elements of $\{1, 2, \ldots, k\}$ such that $u \leq v$. Then, $a_u \mid a_v$.

Note that we had to require $u \leq v$ in this proposition, unlike the analogous propositions for chains of equalities and chains of congruences, because there is no "symmetry of divisibility" (i.e., if $a \mid b$, then we don't generally have $b \mid a$). The proof of Proposition 2.4.7 relies on the reflexivity of divisibility (Proposition 2.2.4 **(a)**) and on the transitivity of divisibility (Proposition 2.2.4 **(b)**).

Again, chains of divisibilities can include equality signs. For example, $4 \mid 3 \cdot 4 = 12 = 2 \cdot 6 \mid 4 \cdot 6 = 24$.

2.5. Substitutivity for congruences

In Section 2.4, we have learnt that congruences modulo an integer n can be chained together like equalities. A further important feature of congruences is the principle of *substitutivity for congruences*. This is yet another way in which congruences behave like equalities. We are not going to state it fully formally (as it is a meta-mathematical principle), but will merely explain its meaning. Later on, once we understand what the rings $\mathbb{Z}/n$ (for integer n) are, we will no longer need this principle, since it will just boil down to "equal things can be substituted for one another" (the whole point of $\mathbb{Z}/n$ is to "make congruent numbers equal"); but for now, we cannot treat "congruent modulo n" as "equal", so we have to state it.

You are probably used to making computations like these:

$$\begin{aligned}\underbrace{(a+b)^2}_{=a^2+2ab+b^2} + \underbrace{(a-b)^2}_{=a^2-2ab+b^2} &= \left(a^2+2ab+b^2\right) + \left(a^2-2ab+b^2\right) \\ &= \underbrace{a^2+a^2}_{=2a^2} + \underbrace{b^2+b^2}_{=2b^2} = 2a^2+2b^2\end{aligned}$$

(for any two numbers a and b). What is going on in these underbraces (like "$\underbrace{(a+b)^2}_{=a^2+2ab+b^2}$")? Something pretty simple is going on: You are replacing a number (in this case, $(a+b)^2$) by an equal number (in this case, $a^2+2ab+b^2$). This relies on a fundamental principle of mathematics (called the *principle of substitutivity for equalities*), which says that an object in an expression can indeed be replaced by any object equal to it (without changing the value of the expression). (This is also known as *Leibniz's equality law*.) To be precise, we are using this principle twice in some of our equality signs above, since we are making several replacements at the same time; but this is fine (we can just do the replacement one by one instead).

We would like to have a similar principle for congruences modulo n: We would like to be able to replace any integer by an integer congruent to it modulo n. For example, we would like to be able to say that if seven integers a, a', b, b', c, c', n satisfy $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$ and $c \equiv c' \bmod n$, then

$$\underbrace{b}_{\equiv b' \bmod n}\ \underbrace{c}_{\equiv c' \bmod n} + \underbrace{c}_{\equiv c' \bmod n}\ \underbrace{a}_{\equiv a' \bmod n} + \underbrace{a}_{\equiv a' \bmod n}\ \underbrace{b}_{\equiv b' \bmod n} \equiv b'c' + c'a' + a'b' \bmod n.$$

We have to be careful with this: For example, we run into troubles if division is involved in our expressions. For example, we have $6 \equiv 9 \bmod 3$, but we do not have $\underbrace{6}_{\equiv 9 \bmod 3}/3 \equiv 9/3 \bmod 3$. Similarly, exponentiation can be problematic. So we need to state the principle we are using here in clearer terms, so that we know what we can do.

Convention 2.5.1. For this whole Section 2.5, we fix an integer n.

The *principle of substitutivity for equalities* says the following:

> *Principle of substitutivity for equalities (PSE):* If two objects x and x' are equal, and if we have any expression A that involves the object x, then we can replace this x (or, more precisely, any arbitrary appearance of x in A) in A by x'; the value of the resulting expression A' will equal the value of A.

Here are two examples of how this principle can be used:

- If a, b, c, d, e, c' are numbers such that $c = c'$, then the PSE says that we can replace c by c' in the expression $a\left(b-\left(c+d\right)e\right)$, and the value of the resulting expression $a\left(b-\left(c'+d\right)e\right)$ will equal the value of $a\left(b-\left(c+d\right)e\right)$; that is, we have
$$a\left(b-\left(c+d\right)e\right) = a\left(b-\left(c'+d\right)e\right). \tag{10}$$
- If a, b, c, a' are numbers such that $a = a'$, then
$$\left(a-b\right)\left(a+b\right) = \left(a'-b\right)\left(a+b\right), \tag{11}$$
because the PSE allows us to replace the first a appearing in the expression $\left(a-b\right)\left(a+b\right)$ by an a'. (We can also replace the second a by a', of course.)

More generally, we can make several such replacements at the same time.

The PSE is one of the headstones of mathematical logic; it is the essence of what it means for two objects to be equal.

The *principle of substitutivity for congruences* is similar, but far less fundamental; it says the following:

> *Principle of substitutivity for congruences (PSC):* If two numbers x and x' are congruent to each other modulo n (that is, $x \equiv x' \bmod n$), and if we have any expression A that involves only integers, addition, subtraction and multiplication, and involves the object x, then we can replace this x (or, more precisely, any arbitrary appearance of x in A) in A by x'; the value of the resulting expression A' will be congruent to the value of A modulo n.

This principle is less general than the PSE, since it only applies to expressions that are built from integers and certain operations (note that division is not one of these operations). But it still lets us prove analogues of our above examples (10) and (11):

- If a, b, c, d, e, c' are integers such that $c \equiv c' \bmod n$, then the PSC says that we can replace c by c' in the expression $a\left(b-\left(c+d\right)e\right)$, and the value of the resulting expression $a\left(b-\left(c'+d\right)e\right)$ will be congruent to the value of $a\left(b-\left(c+d\right)e\right)$ modulo n; that is, we have

$$a\left(b-\left(c+d\right)e\right) \equiv a\left(b-\left(c'+d\right)e\right) \bmod n. \tag{12}$$

- If a, b, c, a' are integers such that $a \equiv a' \bmod n$, then

$$\left(a-b\right)\left(a+b\right) \equiv \left(a'-b\right)\left(a+b\right) \bmod n, \tag{13}$$

  because the PSC allows us to replace the first a appearing in the expression $\left(a-b\right)\left(a+b\right)$ by an a'. (We can also replace the second a by a', of course.)

We shall not prove the PSC, since we have not formalized it (after all, we have not defined what an "expression" is). But we shall prove the specific congruences (12) and (13) using Proposition 2.3.4; the way in which we prove these congruences is symptomatic: Every congruence obtained from the PSC can be proven in a manner like these. Thus, the proofs of (12) and (13) given below can serve as templates which can easily be adapted to any other situation in which an application of the PSC needs to be justified.

As we said, these two proofs are exemplary: Any congruence obtained from the PSC can be proven in such a way (starting with the congruence $x \equiv x' \bmod n$, and then "wrapping" it up in the expression A by repeatedly adding, multiplying and subtracting congruences that follow from Proposition 2.3.4 **(a)**).

When we apply the PSC, we shall use underbraces to point out which integers we are replacing. For example, when deriving (12) from this principle, we shall write

$$a\left(b-\left(\underbrace{c}_{\equiv c' \bmod n}+d\right)e\right) \equiv a\left(b-\left(c'+d\right)e\right) \bmod n,$$

in order to stress that we are replacing c by c'. Likewise, when deriving (13) from the PSC, we shall write

$$\left(\underbrace{a}_{\equiv a' \bmod n}-b\right)\left(a+b\right) \equiv \left(a'-b\right)\left(a+b\right) \bmod n,$$

in order to stress that we are replacing the first a (but not the second a) by a'.

The PSC allows us to replace a **single** integer x appearing in an expression by another integer x' that is congruent to x modulo n. Applying this principle many times, we thus conclude that we can also replace **several** integers at the same time (because we can get to the same result by performing these replacements one at a time, and Proposition 2.4.5 shows that the value of the final result will be congruent

to the value of the original result). For example, if seven integers a, a', b, b', c, c', n satisfy $a \equiv a' \bmod n$ and $b \equiv b' \bmod n$ and $c \equiv c' \bmod n$, then

$$bc + ca + ab \equiv b'c' + c'a' + a'b' \bmod n, \tag{14}$$

because we can replace all the six integers b, c, c, a, a, b in the expression $bc + ca + ab$ (listed in the order of their appearance in this expression) by b', c', c', a', a', b', respectively. If we want to derive this from the PSC, then we must perform the replacements one at a time, e.g., as follows:

$$\begin{aligned}
\underbrace{b}_{\equiv b' \bmod n} c + ca + ab &\equiv b' \underbrace{c}_{\equiv c' \bmod n} + ca + ab \equiv b'c' + \underbrace{c}_{\equiv c' \bmod n} a + ab \\
&\equiv b'c' + c' \underbrace{a}_{\equiv a' \bmod n} + ab \equiv b'c' + c'a' + \underbrace{a}_{\equiv a' \bmod n} b \\
&\equiv b'c' + c'a' + a' \underbrace{b}_{\equiv b' \bmod n} \equiv b'c' + c'a' + a'b' \bmod n.
\end{aligned}$$

Of course, we shall always just show the replacements as a single step:

$$\underbrace{b}_{\equiv b' \bmod n} \underbrace{c}_{\equiv c' \bmod n} + \underbrace{c}_{\equiv c' \bmod n} \underbrace{a}_{\equiv a' \bmod n} + \underbrace{a}_{\equiv a' \bmod n} \underbrace{b}_{\equiv b' \bmod n} \equiv b'c' + c'a' + a'b' \bmod n.$$

The PSC can be extended: The expression A can be allowed to involve not only integers, addition, subtraction, multiplication and x, but also k-th powers for $k \in \mathbb{N}$ (as long as k remains unchanged in our replacement) as well as finite sums and products (as long as the bounds of the sums and products are unchanged). This follows from Exercise 2.3.4 and Exercise 2.3.5.

Exercise 2.5.1. Let $n \in \mathbb{N}$. Show that $7 \mid 3^{2n+1} + 2^{n+2}$.

2.6. Division with remainder

The following fact you likely remember from high school:

Theorem 2.6.1. Let n be a positive integer. Let $u \in \mathbb{Z}$. Then, there exists a unique pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$.

We shall refer to this as the "*division-with-remainder theorem for integers*". Before we prove this theorem, let us introduce the notations that it justifies:

Definition 2.6.2. Let n be a positive integer. Let $u \in \mathbb{Z}$. Theorem 2.6.1 shows that there exists a unique pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ such that $u = qn + r$. Consider this pair.

(a) We denote the integer q by $u//n$, and refer to it as the *quotient of the division of u by n*.

(b) We denote the integer r by $u\%n$, and refer to it as the *remainder of the division of u by n*.

The words "quotient" and "remainder" are standard, but the notations "$u//n$" and "$u\%n$" are not (I have taken them from the Python programming language); be prepared to see other notations in the literature (e.g., the notations "$\operatorname{quo}(u,n)$" and "$\operatorname{rem}(u,n)$" for $u//n$ and $u\%n$, respectively).

Example 2.6.3. **(a)** We have $14//3 = 4$ and $14\%3 = 2$, because $(4,2)$ is the unique pair $(q,r) \in \mathbb{Z} \times \{0,1,2\}$ satisfying $14 = q \cdot 3 + r$.

(b) We have $18//3 = 6$ and $18\%3 = 0$, because $(6,0)$ is the unique pair $(q,r) \in \mathbb{Z} \times \{0,1,2\}$ satisfying $18 = q \cdot 3 + r$.

(c) We have $(-2)//3 = -1$ and $(-2)\%3 = 1$, because $(-1,1)$ is the unique pair $(q,r) \in \mathbb{Z} \times \{0,1,2\}$ satisfying $-2 = q \cdot 3 + r$.

(d) For each $u \in \mathbb{Z}$, we have $u//1 = u$ and $u\%1 = 0$, because $(u,0)$ is the unique pair $(q,r) \in \mathbb{Z} \times \{0\}$ satisfying $u = q \cdot 1 + r$.

But we have gotten ahead of ourselves: We need to prove Theorem 2.6.1 before we can use the notations "$u//n$" and "$u\%n$".

Let us split Theorem 2.6.1 into two parts: existence and uniqueness:

Lemma 2.6.4. Let n be a positive integer. Let $u \in \mathbb{Z}$. Then, there exists **at least one** pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$.

Lemma 2.6.5. Let n be a positive integer. Let $u \in \mathbb{Z}$. Then, there exists **at most one** pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$.

We begin by proving Lemma 2.6.5 (which is the easier one):

But we also need to prove Lemma 2.6.4. This lemma can be proven by induction on u, but not without some complications: Since it is stated for all integers u (rather than just for nonnegative or positive integers), the classical induction principle (with an induction base and a "u to $u+1$" step) cannot prove it directly. Instead, we have to either add a "u to $u-1$" step to our induction (resulting in a "two-sided induction" or "up- and down-induction" argument), or to treat the case of negative u separately. A proof using the first of these two methods can be found in [Grinbe15, proof of Proposition 2.150] (where n and u are denoted by N and n). We shall instead give a proof using the second method; thus, we first state the particular case of Lemma 2.6.4 when u is nonnegative:

Lemma 2.6.6. Let n be a positive integer. Let $u \in \mathbb{N}$. Then, there exists **at least one** pair $(q,r) \in \mathbb{Z} \times \{0,1,\ldots,n-1\}$ such that $u = qn + r$.

This lemma can be proven by induction on u as in [Grinbe15, proof of Proposition 2.150]. Let us instead prove it by **strong** induction on u. See [Grinbe15, §2.8] for an introduction to strong induction; in particular, recall that a strong induction needs no induction base (but often contains a case distinction in its "induction step" that, in some way, does give the first few values a special treatment). The proof of Lemma 2.6.6 that we give below follows a stupid but valid method of finding the

pair (q, r): Keep subtracting n from u until u becomes $< n$; then r will be the resulting number, whereas q will be the number of times you have subtracted n.

In order to derive Lemma 2.6.4 from Lemma 2.6.6 (that is, to extend Lemma 2.6.6 to the case of negative u), we shall need a simple but important trick: By adding a sufficiently high multiple of the positive integer n to u, we eventually obtain a nonnegative integer v (to which we can then apply Lemma 2.6.6). This trick can be crystallized in the following lemma:

Lemma 2.6.7. Let n be a positive integer. Let $u \in \mathbb{Z}$. Then, there exists a $v \in \mathbb{N}$ such that $u \equiv v \bmod n$.

Remark 2.6.8. We can visualize Theorem 2.6.1 as follows: Mark all the multiples of n on the real line. These multiples are evenly spaced points, with a distance of n between any two neighboring multiples. Thus, they subdivide the real line into infinitely many intervals of length n. More precisely, for each $a \in \mathbb{Z}$, let I_a be the interval $[an, (a+1)\, n) = \{x \in \mathbb{R} \mid an \leq x < (a+1)\, n\}$; then, every real belongs to exactly one of these intervals I_a. (This is intuitively clear – I am not saying this is a rigorous proof.) Thus, in particular, u belongs to I_q for some $q \in \mathbb{Z}$. This q is precisely the q in the unique pair $(q, r) \in \mathbb{Z} \times \{0, 1, \ldots, n-1\}$ satisfying $u = qn + r$. Moreover, the r from this pair specifies the relative position of u in the interval I_q.

(Unfortunately, it is not clear to me whether this intuition can be turned into a proper proof of Theorem 2.6.1, since it relies on the fact that every real number belongs to exactly one of the intervals I_a, which fact may well require Theorem 2.6.1 for its proof.)

The following properties of the quotient and the remainder are simple but will be used all the time:

Corollary 2.6.9. Let n be a positive integer. Let $u \in \mathbb{Z}$.
(a) Then, $u\%n \in \{0, 1, \ldots, n-1\}$ and $u\%n \equiv u \bmod n$.
(b) We have $n \mid u$ if and only if $u\%n = 0$.
(c) If $c \in \{0, 1, \ldots, n-1\}$ is such that $c \equiv u \bmod n$, then $c = u\%n$.
(d) We have $u = (u//n)\, n + (u\%n)$.

Before we prove this corollary, let us explain its purpose. Corollary 2.6.9 **(a)** says that $u\%n$ is a number in the set $\{0, 1, \ldots, n-1\}$ that is congruent to u modulo n. Corollary 2.6.9 **(c)** says that $u\%n$ is the **only** such number (as it says that any further such number c must be equal to $u\%n$). Corollary 2.6.9 **(b)** gives an algorithm to check whether $n \mid u$ holds (namely, compute $u\%n$ and check whether $u\%n = 0$). Corollary 2.6.9 **(d)** is a trivial consequence of the definition of quotient and remainder.

Exercise 2.6.1. Let n be a positive integer. Let u and v be integers. Prove that $u \equiv v \bmod n$ if and only if $u\%n = v\%n$.

The following exercise provides an analogue of Theorem 2.6.1, in which r is required to be an integer satisfying $|r| \leq n/2$ rather than an element of $\{0, 1, \ldots, n-1\}$. Note, however, that r is not always unique in this case.

Exercise 2.6.2. Let n be a positive integer. Let $u \in \mathbb{Z}$.

(a) Prove that there exists a pair $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ such that $u = qn + r$ and $|r| \leq n/2$.

(b) Prove that this pair is not unique in general (i.e., find n and u for which it is not unique).

Remark 2.6.10. There is a simple visualization that makes Exercise 2.6.2 **(a)** intuitively obvious: Mark all the multiples of n on the real line. These multiples are evenly spaced points, with a distance of n between any two neighboring multiples. Hence, every point on the real line is at most a distance of $n/2$ away from the closest multiple of n. Applying this to the point u, we conclude that u is at most a distance of $n/2$ away from the closest multiple of n. In other words, if qn is the closest multiple of n to u (or one of the two closest multiples of n, if u is in the middle between two multiples), then $|u - qn| \leq n/2$. Thus, if we set $r = u - qn$, then $u = qn + r$ and $|r| \leq n/2$. This proves Exercise 2.6.2 **(a)** intuitively.

This point of view also makes Exercise 2.6.2 **(b)** evident: When the point u is exactly in the middle of one of the length-n intervals between multiples of n, then there are two multiples of n equally close to u, and we can pick either of them; hence, the pair (q, r) is not unique.

Convention 2.6.11. The symbols $//$ and $\%$ will be granted higher precedence (in the sense of operator precedence) than addition. This means that an expression of the form "$c + a//n + b$" will always be interpreted as "$c + (a//n) + b$", rather than as "$(c + a)//(n + b)$" (or in any other way). Likewise, an expression of the form "$c + a\%n + b$" will always be interpreted as "$c + (a\%n) + b$", rather than as "$(c + a)\%(n + b)$".

Exercise 2.6.3. Let u and v be two integers. Let n be a positive integer.

(a) Prove that $u\%n + v\%n - (u + v)\%n \in \{0, n\}$.

(b) Prove that $(u + v)//n - u//n - v//n \in \{0, 1\}$.

Exercise 2.6.4. Let n be a positive integer. Prove the following:

(a) The map

$$\begin{aligned} \mathbb{Z} \times \{0, 1, \ldots, n-1\} &\to \mathbb{Z}, \\ (q, r) &\mapsto qn + r \end{aligned}$$

is a bijection.

(b) The map

$$\begin{aligned} \mathbb{N} \times \{0,1,\ldots,n-1\} &\to \mathbb{N}, \\ (q,r) &\mapsto qn+r \end{aligned}$$

is a bijection.

(c) Any $q \in \mathbb{Z}$ and $r \in \{0,1,\ldots,n-1\}$ satisfy $(qn+r)\,//\,n = q$.

(d) Any $q \in \mathbb{Z}$ and $r \in \{0,1,\ldots,n-1\}$ satisfy $(qn+r)\,\%n = r$.

2.7. Even and odd numbers

Recall the following:

Definition 2.7.1. Let u be an integer.

(a) We say that u is *even* if u is divisible by 2.

(b) We say that u is *odd* if u is not divisible by 2.

So an integer is either even or odd (but not both at the same time). The following exercise collects various properties of even and odd integers:

Exercise 2.7.1. Let u be an integer.

(a) Prove that u is even if and only if $u\%2 = 0$.

(b) Prove that u is odd if and only if $u\%2 = 1$.

(c) Prove that u is even if and only if $u \equiv 0 \bmod 2$.

(d) Prove that u is odd if and only if $u \equiv 1 \bmod 2$.

(e) Prove that u is odd if and only if $u+1$ is even.

(f) Prove that exactly one of the two numbers u and $u+1$ is even.

(g) Prove that $u(u+1) \equiv 0 \bmod 2$.

(h) Prove that $u^2 \equiv -u \equiv u \bmod 2$.

(i) Let v be a further integer. Prove that $u \equiv v \bmod 2$ holds if and only if u and v are either both odd or both even.

Exercise 2.7.2. **(a)** Prove that each even integer u satisfies $u^2 \equiv 0 \bmod 4$.

(b) Prove that each odd integer u satisfies $u^2 \equiv 1 \bmod 4$.

(c) Prove that no two integers x and y satisfy $x^2 + y^2 \equiv 3 \bmod 4$.

(d) Prove that if x and y are two integers satisfying $x^2 + y^2 \equiv 2 \bmod 4$, then x and y are both odd.

Exercise 2.7.2 **(c)** establishes our previous experimental observation that an integer of the form $4k+3$ with integer k (that is, an integer that is larger by 3 than a multiple of 4) can never be written as a sum of two perfect squares.

Exercise 2.7.3. (a) Prove that the map

$$\begin{aligned}\{i \in \mathbb{N} \mid i \text{ is even}\} &\to \{d \in \mathbb{N} \mid d \equiv 1 \bmod 4\}, \\ i &\mapsto 2i+1\end{aligned}$$

is well-defined and is a bijection.

(b) Prove that the map

$$\begin{aligned}\{i \in \mathbb{N} \mid i \text{ is odd}\} &\to \{d \in \mathbb{N} \mid d \equiv 3 \bmod 4\}, \\ i &\mapsto 2i+1\end{aligned}$$

is well-defined and is a bijection.

Note that the map defined in Exercise 2.7.3 **(a)** sends $0, 2, 4, 6, 8, \ldots$ to $1, 5, 9, 13, 17, \ldots$, while the map defined in Exercise 2.7.3 **(b)** sends $1, 3, 5, 7, 9, \ldots$ to $3, 7, 11, 15, 19, \ldots$.

2.8. The floor function

We shall now briefly introduce the floor function (following [Grinbe16]), as it is closely connected to division with remainder.

Definition 2.8.1. Let x be a real number. Then, $\lfloor x \rfloor$ is defined to be the unique integer n satisfying $n \leq x < n+1$. This integer $\lfloor x \rfloor$ is called the *floor* of x, or the *integer part* of x.

Remark 2.8.2. (a) Why is $\lfloor x \rfloor$ well-defined? I mean, why does the unique integer n in Definition 2.8.1 exist, and why is it unique? This question is trickier than it sounds and relies on the construction of real numbers. However, in the case when x is rational, the well-definedness of $\lfloor x \rfloor$ follows from Proposition 2.8.3 below.

(b) What we call $\lfloor x \rfloor$ is typically called $[x]$ in older books (such as [NiZuMo91]). I suggest avoiding the notation $[x]$ wherever possible; it has too many different meanings (whereas $\lfloor x \rfloor$ almost always means the floor of x).

(c) The map $\mathbb{R} \to \mathbb{Z}$, $x \mapsto \lfloor x \rfloor$ is called the *floor function* or the *greatest integer function*.

There is also a *ceiling function*, which sends each $x \in \mathbb{R}$ to the unique integer n satisfying $n - 1 < x \leq n$; this latter integer is called $\lceil x \rceil$. The two functions are connected by the rule $\lceil x \rceil = -\lfloor -x \rfloor$ (for all $x \in \mathbb{R}$).

The floor and the ceiling functions are some of the simplest examples of discontinuous functions.

(d) Here are some examples of floors:

$$\begin{aligned}\lfloor n \rfloor &= n \qquad \text{for every } n \in \mathbb{Z}; \\ \lfloor 1.32 \rfloor &= 1; \qquad \lfloor \pi \rfloor = 3; \qquad \lfloor 0.98 \rfloor = 0; \\ \lfloor -2.3 \rfloor &= -3; \qquad \lfloor -0.4 \rfloor = -1.\end{aligned}$$

(e) You might have the impression that $\lfloor x \rfloor$ is "what remains from x if the digits behind the comma are removed". This impression is highly imprecise. For one, it is completely broken for negative x (for example, $\lfloor -2.3 \rfloor$ is -3, not -2). But more importantly, the operation of "removing the digits behind the comma" from a number is not well-defined; in fact, the periodic decimal representations $0.999\ldots$ and $1.000\ldots$ belong to the same real number (1), but removing their digits behind the comma leaves us with different integers.

(f) A related map is the map $\mathbb{R} \to \mathbb{Z},\ x \mapsto \left\lfloor x + \dfrac{1}{2} \right\rfloor$. It sends each real x to the integer that is closest to x, choosing the larger one in the case of a tie. This is one of the many things that are commonly known as "rounding" a number.

Proposition 2.8.3. Let a and b be integers such that $b > 0$. Then, $\left\lfloor \dfrac{a}{b} \right\rfloor$ is well-defined and equals $a//b$.

See [Grinbe16] and [NiZuMo91, §4.1] for further properties of the floor function.

2.9. Common divisors, the Euclidean algorithm and the Bezout theorem

We are next going to define and study the divisors of an integer, as well as the common divisors of several integers. These concepts form the backbone of most of number theory, and will later be extended to some more complicated notions than integers (e.g., Gaussian integers and polynomials).

2.9.1. Divisors

Definition 2.9.1. Let $b \in \mathbb{Z}$. The *divisors* of b are defined as the integers that divide b.

Be aware that some authors use a mildly different definition of "divisors"; namely, they additionally require them to be positive. We don't make such a requirement.

For example, the divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$. Of course, the negative divisors of an integer b are merely the reflections of the positive divisors through the origin[10] (this follows easily from Proposition 2.2.3 **(a)**); thus, the positive divisors are usually the only ones of interest.

Here are some basic properties of divisors:

Proposition 2.9.2. **(a)** If $b \in \mathbb{Z}$, then 1 and b are divisors of b.

(b) The divisors of 0 are all the integers.

(c) Let $b \in \mathbb{Z}$ be nonzero. Then, all divisors of b belong to the set $\{-|b|, -|b|+1, \ldots, |b|\} \setminus \{0\}$.

[10] "Reflection through the origin" is just a poetic way to say "negative"; i.e., the reflection of a number a through the origin is $-a$.

Thanks to Proposition 2.9.2, we have a method to find all divisors of an integer b: If $b = 0$, then Proposition 2.9.2 **(b)** directly yields the result; otherwise, Proposition 2.9.2 **(c)** shows that there is only a finite set of numbers we have to check. When b is large, this is slow, but to some extent that is because the problem is computationally hard (or at least suspected to be hard).

2.9.2. Common divisors

It is somewhat more interesting to consider the common divisors of two or more integers:

Definition 2.9.3. Let $b_1, b_2, \ldots, b_k$ be integers. Then, the *common divisors* of $b_1, b_2, \ldots, b_k$ are defined to be the integers a that satisfy

$$(a \mid b_i \text{ for all } i \in \{1, 2, \ldots, k\}) \tag{15}$$

(in other words, that divide all of the integers $b_1, b_2, \ldots, b_k$). We let $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ denote the set of these common divisors.

Note that the concept of common divisors encompasses the concept of divisors: The common divisors of a single integer b are merely the divisors of b. Thus, $\operatorname{Div}(b)$ is the set of all divisors of b whenever $b \in \mathbb{Z}$. (Of course, speaking of "common divisors" of just one integer is like speaking of a conspiracy of just one person. But the definition fits, and we algebraists don't exclude cases just because they are ridiculous.)

(Also, the common divisors of an empty list of integers are all the integers, because the requirement (15) is vacuously true for $k = 0$. In other words, $\operatorname{Div}() = \mathbb{Z}$.)

Here are some more interesting examples of common divisors:

Example 2.9.4. (a) The common divisors of 6 and 8 are $-2, -1, 1, 2$. (In order to see this, just observe that the divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$, whereas the divisors of 8 are $-8, -4, -2, -1, 1, 2, 4, 8$; now you can find the common divisors of 6 and 8 by taking the numbers common to these two lists.) Thus,

$$\operatorname{Div}(6, 8) = \{-2, -1, 1, 2\}.$$

(b) The common divisors of 6 and 14 are $-2, -1, 1, 2$ again. (In order to see this, just observe that the divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$, whereas the divisors of 14 are $-14, -7, -2, -1, 1, 2, 7, 14$.)

(c) The common divisors of 6, 10 and 15 are -1 and 1. (In order to see this, note that:

- The divisors of 6 are $-6, -3, -2, -1, 1, 2, 3, 6$.
- The divisors of 10 are $-10, -5, -2, -1, 1, 2, 5, 10$.
- The divisors of 15 are $-15, -5, -3, -1, 1, 3, 5, 15$.

The only numbers common to these three lists are -1 and 1.) However:

- The common divisors of 6 and 10 are $-2, -1, 1, 2$.
- The common divisors of 6 and 15 are $-3, -1, 1, 3$.
- The common divisors of 10 and 15 are $-5, -1, 1, 5$.

This illustrates the fact that three numbers can have pairwise nontrivial common divisors (where "nontrivial" means "distinct from 1 and -1"), but the only common divisors of all three of them may still be just 1 and -1.

Proposition 2.9.5. Let $b_1, b_2, \ldots, b_k$ be finitely many integers that are not all 0. Then, the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ has a largest element, and this largest element is a positive integer.

The following exercise shows that the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$ depends only on the **set** $\{b_1, b_2, \ldots, b_k\}$, but not on the numbers $b_1, b_2, \ldots, b_k$ themselves. Thus, for example, any integers a, b and c satisfy $\operatorname{Div}(a, b, c, a) = \operatorname{Div}(c, a, b)$ (since $\{a, b, c, a\} = \{c, a, b\}$) and $\operatorname{Div}(a, a, b, a) = \operatorname{Div}(a, b, b)$ (since $\{a, a, b, a\} = \{a, b, b\}$).

Exercise 2.9.1. Let $b_1, b_2, \ldots, b_k$ be finitely many integers. Let $c_1, c_2, \ldots, c_\ell$ be finitely many integers. Prove that if

$$\{b_1, b_2, \ldots, b_k\} = \{c_1, c_2, \ldots, c_\ell\},$$

then

$$\operatorname{Div}(b_1, b_2, \ldots, b_k) = \operatorname{Div}(c_1, c_2, \ldots, c_\ell).$$

2.9.3. Greatest common divisors

Proposition 2.9.5 allows us to make a crucial definition:

Definition 2.9.6. Let $b_1, b_2, \ldots, b_k$ be finitely many integers. The *greatest common divisor* of $b_1, b_2, \ldots, b_k$ is defined as follows:

- If $b_1, b_2, \ldots, b_k$ are not all 0, then it is defined as the largest element of the set $\operatorname{Div}(b_1, b_2, \ldots, b_k)$. This largest element is well-defined (by Proposition 2.9.5), and is a positive integer (by Proposition 2.9.5 again).
- If $b_1, b_2, \ldots, b_k$ are all 0, then it is defined to be 0. (This is a slight abuse of the word "greatest common divisor", because 0 is not actually the greatest among the common divisors of $b_1, b_2, \ldots, b_k$ in this case. In fact, when $b_1, b_2, \ldots, b_k$ are all 0, **every** integer is a common divisor of $b_1, b_2, \ldots, b_k$, so that there is no greatest among these common divisors, because there is no

"greatest integer". Nevertheless, defining the greatest common divisor of $b_1, b_2, \ldots, b_k$ to be 0 in this case will prove to be a good decision, as it will greatly reduce the number of exceptions in our results.)

Thus, in either case, this greatest common divisor is a nonnegative integer. We denote it by $\gcd(b_1, b_2, \ldots, b_k)$. (Some authors also call it $(b_1, b_2, \ldots, b_k)$, which is rather dangerous as the same notation stands for a k-tuple. We shall avoid this notation at all cost, but you should be aware of it when reading number-theoretical literature.)

We shall also use the word "*gcd*" as shorthand for "greatest common divisor".

The greatest common divisors you will most commonly see are those of two integers. Indeed, any other gcd can be rewritten in terms of these: for example,

$$\gcd(a, b, c, d, e) = \gcd(a, \gcd(b, \gcd(c, \gcd(d, e))))$$

for all $a, b, c, d, e \in \mathbb{Z}$. This is, in fact, a consequence of Proposition 2.9.21 **(d)** (which we will prove later), applied several times.

First, let us observe several properties of greatest common divisors:

Proposition 2.9.7. **(a)** We have $\gcd(a, 0) = \gcd(a) = |a|$ for all $a \in \mathbb{Z}$.
(b) We have $\gcd(a, b) = \gcd(b, a)$ for all $a, b \in \mathbb{Z}$.
(c) We have $\gcd(a, ua + b) = \gcd(a, b)$ for all $a, b, u \in \mathbb{Z}$.
(d) If $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \bmod a$, then $\gcd(a, b) = \gcd(a, c)$.
(e) If $a, b \in \mathbb{Z}$ are such that a is positive, then $\gcd(a, b) = \gcd(a, b\%a)$.
(f) We have $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$ for all $a, b \in \mathbb{Z}$.
(g) We have $\gcd(-a, b) = \gcd(a, b)$ for all $a, b \in \mathbb{Z}$.
(h) We have $\gcd(a, -b) = \gcd(a, b)$ for all $a, b \in \mathbb{Z}$.
(i) If $a, b \in \mathbb{Z}$ satisfy $a \mid b$, then $\gcd(a, b) = |a|$.
(j) The greatest common divisor of the empty list of integers is $\gcd() = 0$.

Proposition 2.9.7 is not difficult and we could start proving it right away. However, such a proof would require some annoying case distinctions due to the special treatment that the "$b_1, b_2, \ldots, b_k$ are all 0" case required in Definition 2.9.6. Fortunately, we can circumnavigate these annoyances by stating a simple rule for how the gcd of k integers $b_1, b_2, \ldots, b_k$ can be computed from their set of common divisors (including the case when $b_1, b_2, \ldots, b_k$ are all 0):

Lemma 2.9.8. Let $b_1, b_2, \ldots, b_k$ be finitely many integers. Then,

$$\gcd(b_1, b_2, \ldots, b_k) = \begin{cases} \max(\operatorname{Div}(b_1, b_2, \ldots, b_k)), & \text{if } 0 \notin \operatorname{Div}(b_1, b_2, \ldots, b_k); \\ 0, & \text{if } 0 \in \operatorname{Div}(b_1, b_2, \ldots, b_k). \end{cases}$$

(Here, $\max S$ denotes the largest element of a set S of integers, whenever this largest element exists.)

A corollary of Lemma 2.9.8 is the following:

Lemma 2.9.9. Let $b_1, b_2, \ldots, b_k$ be finitely many integers. Let $c_1, c_2, \ldots, c_\ell$ be finitely many integers. If

$$\operatorname{Div}(b_1, b_2, \ldots, b_k) = \operatorname{Div}(c_1, c_2, \ldots, c_\ell),$$

then

$$\gcd(b_1, b_2, \ldots, b_k) = \gcd(c_1, c_2, \ldots, c_\ell).$$

Lemma 2.9.9 tells us that in order to prove that two lists of integers have the same gcd, it suffices to check that they have the same set of common divisors. Since many of the claims of Proposition 2.9.7 are equalities between gcds, we can thus reduce them to equalities between sets of common divisors. Let us state these equalities as a lemma, which we will then use as a stepping stone in our proof of Proposition 2.9.7:

Lemma 2.9.10. **(a)** We have $\operatorname{Div}(a, 0) = \operatorname{Div}(a)$ for all $a \in \mathbb{Z}$.
(b) We have $\operatorname{Div}(a, b) = \operatorname{Div}(b, a)$ for all $a, b \in \mathbb{Z}$.
(c) We have $\operatorname{Div}(a, ua + b) = \operatorname{Div}(a, b)$ for all $a, b, u \in \mathbb{Z}$.
(d) If $a, b, c \in \mathbb{Z}$ satisfy $b \equiv c \bmod a$, then $\operatorname{Div}(a, b) = \operatorname{Div}(a, c)$.
(e) If $a, b \in \mathbb{Z}$ are such that a is positive, then $\operatorname{Div}(a, b) = \operatorname{Div}(a, b\%a)$.
(f) We have $\operatorname{Div}(a, b) \subseteq \operatorname{Div}(a)$ and $\operatorname{Div}(a, b) \subseteq \operatorname{Div}(b)$ for all $a, b \in \mathbb{Z}$.
(g) We have $\operatorname{Div}(-a, b) = \operatorname{Div}(a, b)$ for all $a, b \in \mathbb{Z}$.
(h) We have $\operatorname{Div}(a, -b) = \operatorname{Div}(a, b)$ for all $a, b \in \mathbb{Z}$.
(i) If $a, b \in \mathbb{Z}$ satisfy $a \mid b$, then $\operatorname{Div}(a, b) = \operatorname{Div}(a)$.
(j) The set of common divisors of the empty list of integers is $\operatorname{Div}() = \mathbb{Z}$.

Remark 2.9.11. Proposition 2.9.7 **(c)** says that if we add a multiple of a to b, then $\gcd(a, b)$ does not change. Similarly, if we add a multiple of b to a, then $\gcd(a, b)$ does not change (i.e., we have $\gcd(vb + a, b) = \gcd(a, b)$ for all $a, b, v \in \mathbb{Z}$).

However, if we **simultaneously** add a multiple of a to b and a multiple of b to a, then $\gcd(a, b)$ may well change: i.e., we may have $\gcd(vb + a, ua + b) \neq \gcd(a, b)$ for all $a, b, u, v \in \mathbb{Z}$. Examples are easy to find (just take $v = 1$ and $u = 1$).

Proposition 2.9.7 gives a quick way to compute $\gcd(a, b)$ for two nonnegative integers a and b, by repeatedly applying division with remainder. For example, let

us compute $\gcd(210,45)$ as follows:

$$\begin{aligned}
\gcd(210,45) &= \gcd(45,210) && \text{(by Proposition 2.9.7 \textbf{(b)})} \\
&= \gcd\left(45, \underbrace{210\%45}_{=30}\right) && \text{(by Proposition 2.9.7 \textbf{(e)})} \\
&= \gcd(45,30) \\
&= \gcd(30,45) && \text{(by Proposition 2.9.7 \textbf{(b)})} \\
&= \gcd\left(30, \underbrace{45\%30}_{=15}\right) && \text{(by Proposition 2.9.7 \textbf{(e)})} \\
&= \gcd(30,15) \\
&= \gcd(15,30) && \text{(by Proposition 2.9.7 \textbf{(b)})} \\
&= \gcd\left(15, \underbrace{30\%15}_{=0}\right) && \text{(by Proposition 2.9.7 \textbf{(e)})} \\
&= \gcd(15,0) = |15| && \text{(by Proposition 2.9.7 \textbf{(a)})} \\
&= 15.
\end{aligned}$$

This method of computing $\gcd(a,b)$ is called the *Euclidean algorithm*, and is usually much faster than the divisors of a or the divisors of b can be found!

The following exercise shows that the number $\gcd(b_1,b_2,\ldots,b_k)$ depends only on the **set** $\{b_1,b_2,\ldots,b_k\}$, but not on the numbers $b_1,b_2,\ldots,b_k$ themselves. Thus, for example, any integers a, b and c satisfy $\gcd(a,b,c,a) = \gcd(c,a,b)$ (since $\{a,b,c,a\} = \{c,a,b\}$) and $\gcd(a,a,b,a) = \gcd(a,b,b)$ (since $\{a,a,b,a\} = \{a,b,b\}$).

Exercise 2.9.2. Let $b_1,b_2,\ldots,b_k$ be finitely many integers. Let $c_1,c_2,\ldots,c_\ell$ be finitely many integers. Prove that if

$$\{b_1,b_2,\ldots,b_k\} = \{c_1,c_2,\ldots,c_\ell\},$$

then

$$\gcd(b_1,b_2,\ldots,b_k) = \gcd(c_1,c_2,\ldots,c_\ell).$$

2.9.4. Bezout's theorem

The following fact about gcds is one of the most important facts in number theory:

Theorem 2.9.12. Let a and b be two integers. Then, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that

$$\gcd(a,b) = xa + yb.$$

Theorem 2.9.12 is often stated as follows: "If a and b are two integers, then $\gcd(a,b)$ is a $\mathbb{Z}$-linear combination of a and b". The notion "$\mathbb{Z}$-linear combination of a and b" simply means "a number of the form $xa+yb$ with $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$" (this is exactly the notion of a "linear combination" in linear algebra, except that now the scalars must come from $\mathbb{Z}$), so this is just a restatement of Theorem 2.9.12.

Theorem 2.9.12 is known as *Bezout's theorem* (or *Bezout's identity*)[11]. We shall prove it in several steps. The first step is to show it when a and b are nonnegative:

Lemma 2.9.13. Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Then, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that

$$\gcd(a,b) = xa + yb.$$

Next, we shall prove Theorem 2.9.12 when $a \in \mathbb{N}$ but b may be negative:

Lemma 2.9.14. Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$. Then, there exist integers $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ such that

$$\gcd(a,b) = xa + yb.$$

Now, we can prove the whole Theorem 2.9.12:

Exercise 2.9.3. Let u be an integer.

(a) Prove that $u^b - 1 \equiv u^a - 1 \bmod u^{b-a} - 1$ for any $a \in \mathbb{N}$ and $b \in \mathbb{N}$ satisfying $b \geq a$.

(b) Prove that $\gcd\left(u^a - 1, u^b - 1\right) = \left|u^{\gcd(a,b)} - 1\right|$ for all $a \in \mathbb{N}$ and $b \in \mathbb{N}$.

2.9.5. First applications of Bezout's theorem

An important corollary of Theorem 2.9.12 is the following fact:

Theorem 2.9.15. Let $a, b \in \mathbb{Z}$. Then:

(a) For each $m \in \mathbb{Z}$, we have the following logical equivalence:

$$(m \mid a \text{ and } m \mid b) \iff (m \mid \gcd(a,b)). \tag{16}$$

(b) The common divisors of a and b are precisely the divisors of $\gcd(a,b)$.

(c) We have $\operatorname{Div}(a,b) = \operatorname{Div}(\gcd(a,b))$.

The three parts of this theorem are saying the same thing from slightly different perspectives; the importance of the theorem nevertheless justifies this repetition. To prove the theorem, we first show the following:

[11] or *Bezout's theorem for integers* if you want to be more precise (as there are similar theorems for other objects)

Lemma 2.9.16. Let $m, a, b \in \mathbb{Z}$ be such that $m \mid a$ and $m \mid b$. Then, $m \mid \gcd(a, b)$.

The following corollary of Theorem 2.9.12 lets us "combine" two divisibilities $a \mid c$ and $b \mid c$. In fact, Proposition 2.2.4 **(c)** would already allow us to "combine" them to form $ab \mid cc = c^2$; but we can also "combine" them to $ab \mid \gcd(a, b) \cdot c$ using the following fact:

Theorem 2.9.17. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid c$ and $b \mid c$. Then, $ab \mid \gcd(a, b) \cdot c$.

Example 2.9.18. Let $a = 6$ and $b = 10$ and $c = 30$. Then, $a = 6 \mid 30 = c$ and $b = 10 \mid 30 = c$. Thus, Theorem 2.9.17 yields $ab \mid \gcd(a, b) \cdot c$. And indeed, this is true, since $ab = 6 \cdot 10 \mid 2 \cdot 30 = \gcd(a, b) \cdot c$ (because $\gcd(a, b) = \gcd(6, 10) = 2$). Note that this latter divisibility is actually an equality: we have $6 \cdot 10 = 2 \cdot 30$. Note also that we do **not** obtain $ab \mid c$ (and indeed, this does not hold).

Here is another corollary of Theorem 2.9.12 whose usefulness will become clearer later on:

Theorem 2.9.19. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid bc$. Then, $a \mid \gcd(a, b) \cdot c$.

At this point, you should see that Theorem 2.9.19 allows "strengthening" divisibilities: You give it a "weak" divisibility $a \mid bc$, and obtain a "stronger" divisibility $a \mid \gcd(a, b) \cdot c$ from it (stronger because $\gcd(a, b)$ is usually smaller than b).

Theorem 2.9.20. Let $s, a, b \in \mathbb{Z}$. Then,

$$\gcd(sa, sb) = |s| \gcd(a, b).$$

Exercise 2.9.4. Let $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ satisfy $a_1 \mid b_1$ and $a_2 \mid b_2$. Prove that

$$\gcd(a_1, a_2) \mid \gcd(b_1, b_2).$$

Exercise 2.9.5. Let $a, b \in \mathbb{Z}$.
(a) Prove that $\gcd(a, |b|) = \gcd(a, b)$.
(b) Prove that $\gcd(|a|, b) = \gcd(a, b)$.
(c) Prove that $\gcd(|a|, |b|) = \gcd(a, b)$.

2.9.6. gcds of multiple numbers

The following theorem generalizes some of the previous facts to gcds of multiple integers:

Theorem 2.9.21. Let $b_1, b_2, \ldots, b_k$ be integers.

(a) For each $m \in \mathbb{Z}$, we have the following logical equivalence:

$$(m \mid b_i \text{ for all } i \in \{1, 2, \ldots, k\}) \iff (m \mid \gcd(b_1, b_2, \ldots, b_k)).$$

(b) The common divisors of $b_1, b_2, \ldots, b_k$ are precisely the divisors of $\gcd(b_1, b_2, \ldots, b_k)$.

(c) We have $\operatorname{Div}(b_1, b_2, \ldots, b_k) = \operatorname{Div}(\gcd(b_1, b_2, \ldots, b_k))$.

(d) If $k > 0$, then

$$\gcd(b_1, b_2, \ldots, b_k) = \gcd(\gcd(b_1, b_2, \ldots, b_{k-1}), b_k).$$

Theorem 2.9.21 **(d)** is the reason why most properties of gcds of multiple numbers can be derived from corresponding properties of gcds of two numbers. For example, we can easily prove the following analogue of Theorem 2.9.20 for gcds of three numbers:

Exercise 2.9.6. Let $s, a, b, c \in \mathbb{Z}$. Prove that $\gcd(sa, sb, sc) = |s| \gcd(a, b, c)$.

More generally, Theorem 2.9.20 can be generalized to any finite number of integers:

Exercise 2.9.7. Let $s \in \mathbb{Z}$, and let $a_1, a_2, \ldots, a_k$ be integers. Prove that $\gcd(sa_1, sa_2, \ldots, sa_k) = |s| \gcd(a_1, a_2, \ldots, a_k)$.

Bezout's theorem (Theorem 2.9.12) also holds for any finite number of integers:

Theorem 2.9.22. Let $b_1, b_2, \ldots, b_k$ be integers. Then, there exist integers $x_1, x_2, \ldots, x_k$ such that

$$\gcd(b_1, b_2, \ldots, b_k) = x_1 b_1 + x_2 b_2 + \cdots + x_k b_k.$$

Once again, we can restate Theorem 2.9.22 by using the concept of a $\mathbb{Z}$-linear combination. Let us define this concept finally:

Definition 2.9.23. Let $b_1, b_2, \ldots, b_k$ be numbers. A *$\mathbb{Z}$-linear combination* of $b_1, b_2, \ldots, b_k$ shall mean a number of the form $x_1 b_1 + x_2 b_2 + \cdots + x_k b_k$, where $x_1, x_2, \ldots, x_k$ are integers.

Thus, Theorem 2.9.22 can be restated as follows:

Theorem 2.9.24. Let $b_1, b_2, \ldots, b_k$ be integers. Then, $\gcd(b_1, b_2, \ldots, b_k)$ is a $\mathbb{Z}$-linear combination of $b_1, b_2, \ldots, b_k$.

For future reference, let us restate Theorem 2.9.21 **(a)** as follows:

Corollary 2.9.25. Let $b_1, b_2, \ldots, b_k$ be integers. For each $m \in \mathbb{Z}$, we have the following logical equivalence:

$$(m \mid b_1 \text{ and } m \mid b_2 \text{ and } \cdots \text{ and } m \mid b_k) \iff (m \mid \gcd(b_1, b_2, \ldots, b_k)).$$

Theorem 2.9.26. Let $b_1, b_2, \ldots, b_k$ be integers, and let $c_1, c_2, \ldots, c_\ell$ be integers. Then,

$$\begin{aligned}&\gcd(b_1, b_2, \ldots, b_k, c_1, c_2, \ldots, c_\ell) \\ &= \gcd(\gcd(b_1, b_2, \ldots, b_k), \gcd(c_1, c_2, \ldots, c_\ell)).\end{aligned}$$

Our proof of this theorem will rely on a simple trick, which we state as a lemma:

Lemma 2.9.27. Let a and b be two integers.
(a) If each $m \in \mathbb{Z}$ satisfies the implication $(m \mid a) \Longrightarrow (m \mid b)$, then $a \mid b$.
(b) If each $m \in \mathbb{Z}$ satisfies the equivalence $(m \mid a) \Longleftrightarrow (m \mid b)$, then $|a| = |b|$.

Lemma 2.9.27 **(b)** says that the divisors of an integer a uniquely determine $|a|$ (that is, they uniquely determine a up to sign). Thus, when you want to prove that two integers have the same absolute values, it suffices to prove that they have the same divisors. If you know that your two integers are nonnegative, then you can prove this way that they are equal (since their absolute values are just themselves). This is exactly how we will prove that the left and right hand sides in Theorem 2.9.26 are equal.

Lemma 2.9.27 is a simple case of what is known in category theory as the *Yoneda lemma*.

2.9.7. On converses of Bezout's theorem

Some words of warning are in order. Theorem 2.9.12 says that if a and b are two integers, then $\gcd(a, b)$ is a $\mathbb{Z}$-linear combination of a and b. Note the indefinite article "a" here: There are (usually) many $\mathbb{Z}$-linear combinations of a and b, but only one gcd. It is definitely not true that every $\mathbb{Z}$-linear combination of a and b must be $\gcd(a, b)$. However, all these $\mathbb{Z}$-linear combinations are **multiples** of the gcd, as the following (simple) proposition says:

Proposition 2.9.28. Let a and b be two integers. Then, any integers x and y satisfy $\gcd(a, b) \mid xa + yb$.

A similar proposition holds for $\mathbb{Z}$-linear combinations of any number of integers $b_1, b_2, \ldots, b_k$.

2.10. Coprime integers

2.10.1. Definition

The concept of a gcd leads to one of the most important notions of number theory:

Definition 2.10.1. Let a and b be two integers. We say that a is *coprime* to b if and only if $\gcd(a,b) = 1$.

Instead of "coprime", some authors say "relatively prime" or even "prime" (but the latter language risks confusion with a more standard notion of "prime" that we will see later on).

Example 2.10.2. **(a)** The number 2 is coprime to 3, since $\gcd(2,3) = 1$.

(b) The number 6 is not coprime to 15, since $\gcd(6,15) = 3 \neq 1$.

(c) Let a be an integer. We claim (as a generalization of part **(a)**) that the number a is coprime to $a+1$. To prove this, we note that

$$\gcd\left(a, \underbrace{a}_{=1a} + 1\right) = \gcd(a, 1a+1) = \gcd(a,1)$$

(by Proposition 2.9.7 **(c)**, applied to $u = 1$ and $b = 1$)

$$\mid 1 \qquad \text{(by Proposition 2.9.7 \textbf{(f)}, applied to } b = 1\text{)},$$

and thus $\gcd(a, a+1) = 1$ (by Exercise 2.2.5, since $\gcd(a,a+1)$ is a nonnegative integer), which means that a is coprime to $a+1$.

(d) Let a be an integer. When is a coprime to $a+2$? If we try to compute $\gcd(a,a+2)$, we find

$$\gcd\left(a, \underbrace{a}_{=1a} + 2\right) = \gcd(a, 1a+2) = \gcd(a,2)$$

(by Proposition 2.9.7 **(c)**, applied to $u = 1$ and $b = 2$).

It remains to find $\gcd(a,2)$. Proposition 2.9.7 **(f)** (applied to $b = 2$) yields $\gcd(a,2) \mid a$ and $\gcd(a,2) \mid 2$. Since $\gcd(a,2)$ is a nonnegative integer and is a divisor of 2 (because $\gcd(a,2) \mid 2$), we see that $\gcd(a,2)$ must be either 1 or 2 (since the only nonnegative divisors of 2 are 1 and 2). If a is even, then 2 is a common divisor of a and 2, and thus must be the greatest common divisor of a and 2 (because a common divisor of a and 2 cannot be greater than 2); in other words, we have $\gcd(a,2) = 2$ in this case. On the other hand, if a is odd, then 2 is not a common divisor of a and 2 (since 2 does not divide a), and thus cannot be the greatest common divisor of a and 2; hence, in this case, we have $\gcd(a,2) \neq 2$ and thus $\gcd(a,2) = 1$. Summarizing, we conclude that

$$\gcd(a,2) = \begin{cases} 2, & \text{if } a \text{ is even;} \\ 1, & \text{if } a \text{ is odd.} \end{cases}$$

Now, recall that $\gcd(a, a+2) = \gcd(a, 2) = \begin{cases} 2, & \text{if } a \text{ is even;} \\ 1, & \text{if } a \text{ is odd.} \end{cases}$ Hence, a is coprime to $a+2$ if and only if a is odd.

Following the book [GrKnPa94], we introduce a slightly quaint notation:

Definition 2.10.3. Let a and b be two integers. We write "$a \perp b$" to signify that a is coprime to b.

Note that the "$\perp$" relation is symmetric:

Proposition 2.10.4. Let a and b be two integers. Then, $a \perp b$ if and only if $b \perp a$.

Definition 2.10.5. Let a and b be two integers. Proposition 2.10.4 shows that a is coprime to b if and only if b is coprime to a. Hence, we shall sometimes use a more symmetric terminology for this situation: We shall say that "a and b *are coprime*" to mean that a is coprime to b (or, equivalently, that b is coprime to a).

Exercise 2.10.1. Let $a \in \mathbb{Z}$. Prove the following:
(a) We have $1 \perp a$.
(b) We have $0 \perp a$ if and only if $|a| = 1$.

2.10.2. Properties of coprime integers

We can now state multiple theorems about coprime numbers. The first one states that we can "cancel" a factor b from a divisibility $a \mid bc$ as long as this factor is coprime to a:

Theorem 2.10.6. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid bc$ and $a \perp b$. Then, $a \mid c$.

I like to think of Theorem 2.10.7 as a way of removing "unsolicited guests" from divisibilities. Indeed, it says that we can remove the factor b from $a \mid bc$ if we know that b is "unrelated" (i.e., coprime) to a.

The next theorem lets us "combine" two divisibilities $a \mid c$ and $b \mid c$ to $ab \mid c$ as long as a and b are coprime:

Theorem 2.10.7. Let $a, b, c \in \mathbb{Z}$ satisfy $a \mid c$ and $b \mid c$ and $a \perp b$. Then, $ab \mid c$.

Theorem 2.10.7 can be restated as follows: If a and b are two coprime divisors of an integer c, then ab is also a divisor of c. This is often helpful when proving divisibilities where the left hand side (i.e., the number in front of the "|" sign) can be split into a product of two mutually coprime factors. Similar reasoning works with several coprime factors (see Exercise 2.10.3 below).

The next theorem (still part of the fallout of Bezout's theorem) is important, but we will not truly appreciate it until later:

Theorem 2.10.8. Let $a, n \in \mathbb{Z}$.
(a) There exists an $a' \in \mathbb{Z}$ such that $aa' \equiv \gcd(a, n) \bmod n$.
(b) If $a \perp n$, then there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \bmod n$.
(c) If there exists an $a' \in \mathbb{Z}$ such that $aa' \equiv 1 \bmod n$, then $a \perp n$.

If $a, n \in \mathbb{Z}$, then an integer $a' \in \mathbb{Z}$ satisfying $aa' \equiv 1 \bmod n$ is called a *modular inverse* of a modulo n. The word "modular inverse" is chosen in analogy to the usual concept of an "inverse" in $\mathbb{Z}$ (which stands for an integer $a' \in \mathbb{Z}$ satisfying $aa' = 1$; this exists if and only if a equals 1 or -1). Theorem 2.10.8 **(b)** shows that such a modular inverse always exists when $a \perp n$; Theorem 2.10.8 **(c)** is the converse of this statement (i.e., it says that if a modular inverse of a modulo n exists, then $a \perp n$).

Theorem 2.10.9. Let $a, b, c \in \mathbb{Z}$ such that $a \perp c$ and $b \perp c$. Then, $ab \perp c$.

Let us generalize Theorem 2.10.9 to products of several numbers instead of just the two numbers a and b:

Exercise 2.10.2. Let $c \in \mathbb{Z}$. Let $a_1, a_2, \ldots, a_k$ be integers such that each $i \in \{1, 2, \ldots, k\}$ satisfies $a_i \perp c$. Prove that $a_1 a_2 \cdots a_k \perp c$.

We can similarly generalize Theorem 2.10.7 to show that the product of several mutually coprime divisors of an integer c must again be a divisor of c:

Exercise 2.10.3. Let $c \in \mathbb{Z}$. Let $b_1, b_2, \ldots, b_k$ be integers that are mutually coprime (i.e., they satisfy $b_i \perp b_j$ for all $i \neq j$). Assume that $b_i \mid c$ for each $i \in \{1, 2, \ldots, k\}$. Prove that $b_1 b_2 \cdots b_k \mid c$.

Exercise 2.10.4. Let $a, b \in \mathbb{Z}$ be such that $a \perp b$. Let $n, m \in \mathbb{N}$. Prove that $a^n \perp b^m$.

The above results have one important application to congruences. Recall that if a, b, c are integers satisfying $ab = ac$, then we can "cancel" a from the equality $ab = ac$ to obtain $b = c$ as long as a is nonzero. Something similar is true for congruences modulo n, but the condition "a is nonzero" has to be replaced by "a is coprime to n":

Lemma 2.10.10. Let a, b, c, n be integers such that $a \perp n$ and $ab \equiv ac \bmod n$. Then, $b \equiv c \bmod n$.

Lemma 2.10.10 says that we can cancel an integer a from a congruence $ab \equiv ac \bmod n$ as long as a is coprime to n. Let us give two proofs of this lemma, to illustrate the uses of some of the previous results:

For future use, let us restate Exercise 2.10.2 in a form that uses "unordered" finite products $\prod_{i \in I} b_i$ instead of $a_1 a_2 \cdots a_k$:

Exercise 2.10.5. Let $c \in \mathbb{Z}$. Let I be a finite set. For each $i \in I$, let b_i be an integer such that $b_i \perp c$. Prove that $\prod_{i \in I} b_i \perp c$.

Exercise 2.10.6. Let a, b, c be three integers such that $a \equiv b \bmod c$. Prove that if $a \perp c$, then $b \perp c$.

Exercise 2.10.7. Let $a, b \in \mathbb{Z}$. Prove that $b - a \perp b$ holds if and only if $a \perp b$.

2.10.3. An application to sums of powers

Let us show an application of Theorem 2.10.7. First, we shall prove a simple lemma:

Lemma 2.10.11. Let $d \in \mathbb{N}$. Let x and y be integers.
(a) We have $x - y \mid x^d - y^d$.
(b) We have $x + y \mid x^d + y^d$ if d is odd.

Next, let us recall a basic fact from combinatorics (the "Little Gauss" sum):

Proposition 2.10.12. Let $n \in \mathbb{N}$. Then,

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Proposition 2.10.12 tells us what the sum $1 + 2 + \cdots + n$ of the first n positive integers is. One might also ask what the sum $1^2 + 2^2 + \cdots + n^2$ of their squares is, and similarly for higher powers. While this is tangential to our course, let us collect some formulas for this:

Proposition 2.10.13. Let $n \in \mathbb{N}$. Then:
(a) We have $1 + 2 + \cdots + n = \frac{1}{2} n (n+1)$.
(b) We have $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6} n (n+1) (2n+1)$.
(c) We have $1^3 + 2^3 + \cdots + n^3 = \frac{1}{4} n^2 (n+1)^2$.
(d) We have $1^4 + 2^4 + \cdots + n^4 = \frac{1}{30} n (2n+1) (n+1) \left(3n + 3n^2 - 1\right)$.
(e) We have $1^5 + 2^5 + \cdots + n^5 = \frac{1}{12} n^2 (n+1)^2 \left(2n + 2n^2 - 1\right)$.

Each part of Proposition 2.10.13 can be straightforwardly proven by induction on n; we don't need ingenious arguments like the one we gave above for Proposition 2.10.12 (and in fact, such arguments cannot always be found).

You probably see a pattern in Proposition 2.10.13: It appears that for each positive integer d, there exists some polynomial $p_d(x)$ of degree $d+1$ with rational coefficients such

that each $n \in \mathbb{N}$ satisfies $1^d + 2^d + \cdots + n^d = p_d(n)$. This is indeed the case. Indeed, this is proven (e.g.) in [Galvin17, Proposition 23.2] and in [Grinbe17, Theorem 3.7]. The polynomial $p_d(x)$ is uniquely determined for each d, and can be explicitly computed via the formula

$$p_d(x) = \sum_{k=1}^{d} k! \left\{ {d \atop k} \right\} \binom{x+1}{k+1},$$

where $\binom{x+1}{k+1} = \dfrac{(x+1)\,x\,(x-1)\cdots(x-k+1)}{(k+1)!}$ and where $\left\{ {d \atop k} \right\}$ is a *Stirling number of the 2nd kind*. Without going into the details of what Stirling numbers of the 2nd kind are, let me say that $k! \left\{ {d \atop k} \right\}$ is the number of surjective maps from $\{1, 2, \ldots, d\}$ to $\{1, 2, \ldots, k\}$. For example,

$$\begin{aligned} p_2(x) &= \sum_{k=1}^{2} k! \left\{ {2 \atop k} \right\} \binom{x+1}{k+1} = \underbrace{1! \left\{ {2 \atop 1} \right\}}_{=1} \binom{x+1}{2} + \underbrace{2! \left\{ {2 \atop 2} \right\}}_{=2} \binom{x+1}{3} \\ &= \binom{x+1}{2} + 2\binom{x+1}{3} = \frac{(x+1)\,x}{2} + 2 \cdot \frac{(x+1)\,x\,(x-1)}{6} \\ &= \frac{1}{6} x\,(x+1)\,(2x+1), \end{aligned}$$

and thus

$$1^2 + 2^2 + \cdots + n^2 = p_2(n) = \frac{1}{6} n\,(n+1)\,(2n+1) \qquad \text{for each } n \in \mathbb{N}.$$

This recovers the claim of Proposition 2.10.13 **(b)**. The combinatorial proof presented in [Galvin17, Proposition 23.2] is highly recommended reading for anyone interested in this kind of formulas.

Let us note that the polynomials $p_d(x)$ do **not** have integer coefficients, but nevertheless all their values $p_d(n)$ for $n \in \mathbb{N}$ are integers.

Let us now show the power of Theorem 2.10.7 on the following exercise:

Exercise 2.10.8. Let $n \in \mathbb{N}$. Let d be an odd positive integer. Prove that

$$1 + 2 + \cdots + n \mid 1^d + 2^d + \cdots + n^d.$$

[**Hint:** Use Proposition 2.10.12 to reduce the claim to proving that $n\,(n+1) \mid 2\left(1^d + 2^d + \cdots + n^d\right)$. But Theorem 2.10.7 shows that in order to prove this, it suffices to prove $n \mid 2\left(1^d + 2^d + \cdots + n^d\right)$ and $n+1 \mid 2\left(1^d + 2^d + \cdots + n^d\right)$, because $n \perp n+1$.]

2.10.4. More properties of gcds and coprimality

The following is a random collection of further exercises on gcds.

Exercise 2.10.9. Let a, b, x, y be integers such that $xa + yb = 1$. Prove that $a \perp b$.

Exercise 2.10.10. Let $u, v, x, y \in \mathbb{Z}$. Prove that $\gcd(u, v) \cdot \gcd(x, y) = \gcd(ux, uy, vx, vy)$.

Exercise 2.10.11. Let $a, b, c \in \mathbb{Z}$.
(a) Prove that $\gcd(a, b) \cdot \gcd(a, c) = \gcd(ag, bc)$, where $g = \gcd(a, b, c)$.
(b) Prove that $\gcd(a, b) \cdot \gcd(a, c) = \gcd(a, bc)$ if $b \perp c$.

Exercise 2.10.12. Let a and b be two integers that are not both zero. Let $g = \gcd(a, b)$. Prove that $\dfrac{a}{g}$ and $\dfrac{b}{g}$ are integers satisfying $\dfrac{a}{g} \perp \dfrac{b}{g}$.

Exercise 2.10.13. Let a and b be two integers. Let $k \in \mathbb{N}$. Prove that $\gcd\left(a^k, b^k\right) = (\gcd(a, b))^k$.

The next exercise is simply claiming the well-known fact that any rational number can be written as a reduced fraction:

Exercise 2.10.14. Let $r \in \mathbb{Q}$. Prove that there exist two **coprime** integers a and b satisfying $r = a/b$.

As an application of some of the preceding results, we can prove that certain numbers are irrational:

Exercise 2.10.15. Prove the following:
(a) If a positive integer u is not a perfect square[12], then $\sqrt{u}$ is irrational.
(b) If u and v are two positive integers, then $\sqrt{u} + \sqrt{v}$ is irrational unless both u and v are perfect squares.

Exercise 2.10.15 invites a rather natural generalization: If $u_1, u_2, \ldots, u_k$ are several positive integers that are not all perfect squares, then must $\sqrt{u_1} + \sqrt{u_2} + \cdots + \sqrt{u_k}$ always be irrational? It turns out that the answer is "yes", but this is not as easy to prove anymore as the two cases $k = 1$ and $k = 2$ that we handled in Exercise 2.10.15. Proofs of the general version can be found in [Boreic08] (actually, a stronger statement is proven there, although it takes some work to derive ours from it).

Let us generalize Exercise 2.10.10 a bit:

Exercise 2.10.16. Let $x, y \in \mathbb{Z}$, and let $a_1, a_2, \ldots, a_k$ be finitely many integers. Prove that

$$\gcd(a_1, a_2, \ldots, a_k) \cdot \gcd(x, y) = \gcd(a_1 x, a_2 x, \ldots, a_k x, a_1 y, a_2 y, \ldots, a_k y).$$

[12] A *perfect square* means the square of an integer.

We can extend this exercise further to several integers instead of x and y, but this extension would be notationally awkward, so we only state it for the case of three integers:

Exercise 2.10.17. Let $x, y, z \in \mathbb{Z}$, and let $a_1, a_2, \ldots, a_k$ be finitely many integers. Prove that

$$\begin{aligned}&\gcd(a_1, a_2, \ldots, a_k) \cdot \gcd(x, y, z) \\ &= \gcd(a_1x, a_2x, \ldots, a_kx, a_1y, a_2y, \ldots, a_ky, a_1z, a_2z, \ldots, a_kz).\end{aligned}$$

We leave it to the reader to state and solve an exercise generalizing Exercise 2.10.16 and Exercise 2.10.17.

Exercise 2.10.18. Let $a, b, c \in \mathbb{Z}$. Prove that

$$\gcd(b, c) \cdot \gcd(c, a) \cdot \gcd(a, b) = \gcd(a, b, c) \cdot \gcd(bc, ca, ab).$$

Exercise 2.10.19. Let n be a positive integer. Let $[n]$ denote the set $\{1, 2, \ldots, n\}$. Let Z be the set of all pairs $(x, y) \in [n]^2$ satisfying $x \perp y$ and $x + y > n$. (For example, if $n = 5$, then

$$Z = \{(1,5), (2,5), (3,4), (3,5), (4,3), (4,5), (5,1), (5,2), (5,3), (5,4)\}.\ )$$

Prove that

$$\sum_{(x,y) \in Z} \frac{1}{xy} = 1.$$

2.11. Lowest common multiples

Common multiples are, in a sense, a "mirror version" of common divisors. Here is their definition:

Definition 2.11.1. Let $b_1, b_2, \ldots, b_k$ be integers. Then, the *common multiples* of $b_1, b_2, \ldots, b_k$ are defined to be the integers a that satisfy

$$(b_i \mid a \text{ for all } i \in \{1, 2, \ldots, k\}).$$

(In other words, a *common multiple* of $b_1, b_2, \ldots, b_k$ is an integer that is a multiple of each of $b_1, b_2, \ldots, b_k$.) We let $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$ denote the set of these common multiples.

Example 2.11.2. The common multiples of $4, 6$ are $\ldots, -36, -24, -12, 0, 12, 24, 36, \ldots$, that is, all multiples of 12.

The common multiples of $1, 2, 3$ are all multiples of 6.

Note that the common multiples of a single integer b are simply the multiples of b. (Also, the common multiples of an empty list of integers are all the integers; in other words, $\operatorname{Mul}() = \mathbb{Z}$.)

Note that the definition of common multiples of $b_1, b_2, \ldots, b_k$ (Definition 2.11.1) is the same as the definition of common divisors of $b_1, b_2, \ldots, b_k$ except that the divisibility has been flipped (i.e., it says "$b_i \mid a$" instead of "$a \mid b_i$"). This is why common multiples are a "mirror version" of common divisors. This analogy is not perfect – in particular, (for example) two nonzero integers have infinitely many common multiples but only finitely many common divisors. We shall now introduce lowest common multiples, which correspond to greatest common divisors in this analogy. However, we have to prove a simple proposition first:

Proposition 2.11.3. Let $b_1, b_2, \ldots, b_k$ be finitely many nonzero integers. Then, the set $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$ has a smallest positive element.

Proposition 2.11.3 is similar to Proposition 2.9.5 (and will play a similar role), but note the differences: It requires **all** of $b_1, b_2, \ldots, b_k$ to be nonzero (unlike Proposition 2.9.5, which needed only one of them to be nonzero), and it does not claim finiteness of any set.

Definition 2.11.4. Let $b_1, b_2, \ldots, b_k$ be finitely many integers. The *lowest common multiple* of $b_1, b_2, \ldots, b_k$ is defined as follows:

- If $b_1, b_2, \ldots, b_k$ are all nonzero, then it is defined as the smallest positive element of the set $\operatorname{Mul}(b_1, b_2, \ldots, b_k)$. This smallest positive element is well-defined (by Proposition 2.11.3), and is a positive integer (obviously).
- If $b_1, b_2, \ldots, b_k$ are not all nonzero (i.e., at least one of $b_1, b_2, \ldots, b_k$ is zero), then it is defined to be 0.

Thus, in either case, this lowest common multiple is a nonnegative integer. We denote it by $\operatorname{lcm}(b_1, b_2, \ldots, b_k)$. (Some authors also call it $[b_1, b_2, \ldots, b_k]$.)

We shall also use the word "*lcm*" as shorthand for "lowest common multiple".

Some authors say "*least common multiple*" instead of "lowest common multiple".

We are slightly abusing the word "lowest common multiple", of course; it would be more precise to say "lowest **positive** common multiple", and even this would only hold for the case when $b_1, b_2, \ldots, b_k$ are all nonzero. Taken literally, a "lowest common multiple" of 2 and 3 would not exist, since 2 and 3 have infinitely many negative common multiples.

Note that the lcm of a single number is the absolute value of this number: i.e., we have $\operatorname{lcm}(a) = |a|$ for each $a \in \mathbb{Z}$. (This is easy to prove.) Also, the lcm of an empty list of numbers is 1: that is, $\operatorname{lcm}() = 1$.

We observe a trivial property of lcms, which (for the sake of brevity) we only state for two integers a and b despite it holding for any number of integers (with the same proof):

Proposition 2.11.5. Let $a, b \in \mathbb{Z}$.
(a) We have $0 \in \operatorname{Mul}(a, b)$.
(b) We have $\operatorname{lcm}(a, b) \in \operatorname{Mul}(a, b)$.
(c) We have $a \mid \operatorname{lcm}(a, b)$ and $b \mid \operatorname{lcm}(a, b)$.

The following theorem yields a good way of computing lcms of two numbers (since we already know how to compute gcds via the Euclidean algorithm):

Theorem 2.11.6. Let $a, b \in \mathbb{Z}$. Then, $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = |ab|$.

Next, we state an analogue of Theorem 2.9.15 (with all divisibilities flipped):

Theorem 2.11.7. Let $a, b \in \mathbb{Z}$. Then:
(a) For each $m \in \mathbb{Z}$, we have the following logical equivalence:

$$(a \mid m \text{ and } b \mid m) \iff (\operatorname{lcm}(a, b) \mid m). \tag{17}$$

(b) The common multiples of a and b are precisely the multiples of $\operatorname{lcm}(a, b)$.
(c) We have $\operatorname{Mul}(a, b) = \operatorname{Mul}(\operatorname{lcm}(a, b))$.

Again, the three parts of this theorem are saying the same thing from slightly different perspectives. Our proof of Theorem 2.11.7 will rely on the following lemma:

Lemma 2.11.8. Let $m, a, b \in \mathbb{Z}$ be such that $a \mid m$ and $b \mid m$. Then, $\operatorname{lcm}(a, b) \mid m$.

Lemma 2.11.8 is similar to Lemma 2.9.16, but its proof is not:
Our next claim is an analogue of Theorem 2.9.21:

Theorem 2.11.9. Let $b_1, b_2, \ldots, b_k$ be integers.
(a) For each $m \in \mathbb{Z}$, we have the following logical equivalence:

$$(b_i \mid m \text{ for all } i \in \{1, 2, \ldots, k\}) \iff (\operatorname{lcm}(b_1, b_2, \ldots, b_k) \mid m).$$

(b) The common multiples of $b_1, b_2, \ldots, b_k$ are precisely the multiples of $\operatorname{lcm}(b_1, b_2, \ldots, b_k)$.
(c) We have $\operatorname{Mul}(b_1, b_2, \ldots, b_k) = \operatorname{Mul}(\operatorname{lcm}(b_1, b_2, \ldots, b_k))$.
(d) If $k > 0$, then

$$\operatorname{lcm}(b_1, b_2, \ldots, b_k) = \operatorname{lcm}(\operatorname{lcm}(b_1, b_2, \ldots, b_{k-1}), b_k).$$

Exercise 2.11.1. Let $a, b \in \mathbb{Z}$.
(a) Prove that $\operatorname{lcm}(a,b) = \operatorname{lcm}(b,a)$.
(b) Prove that $\operatorname{lcm}(-a,b) = \operatorname{lcm}(a,b)$.
(c) Prove that $\operatorname{lcm}(a,-b) = \operatorname{lcm}(a,b)$.
(d) Prove the following: If $a \mid b$, then $\operatorname{lcm}(a,b) = |b|$.
(e) Let $s \in \mathbb{Z}$. Prove that $\operatorname{lcm}(sa,sb) = |s| \operatorname{lcm}(a,b)$.

Exercise 2.11.2. Let a, b, c be three integers.
(a) Prove that $\gcd(a,b,c) \cdot \operatorname{lcm}(bc,ca,ab) = |abc|$.
(b) Prove that $\operatorname{lcm}(a,b,c) \cdot \gcd(bc,ca,ab) = |abc|$.

2.12. The Chinese remainder theorem (elementary form)

Theorem 2.12.1. Let m and n be two coprime integers. Let $a, b \in \mathbb{Z}$.
(a) There exists an integer $x \in \mathbb{Z}$ such that

$$(x \equiv a \bmod m \text{ and } x \equiv b \bmod n).$$

(b) If x_1 and x_2 are two such integers x, then $x_1 \equiv x_2 \bmod mn$.

Theorem 2.12.1 is known as the *Chinese remainder theorem*. More precisely, there is a sizeable cloud of results that share this name; Theorem 2.12.1 is one of the most elementary and basic of these results. A more general result is Theorem 2.12.4 further below. However, the strongest and most general "Chinese remainder theorems" rely on concepts from abstract algebra such as rings and ideals; it will take us a while to get to them.

Theorem 2.12.1 has gotten its name from the fact that a first glimpse of it appears in "Master Sun's Mathematical Manual" from the 3rd century AD; it took centuries until it become a theorem with proof and precise statement.

The claim of Theorem 2.12.1 **(b)** is often restated as "This integer x (i.e., the integer x satisfying $(x \equiv a \bmod m \text{ and } x \equiv b \bmod n)$) is unique modulo mn". The "modulo mn" here signifies that what we are not claiming literal uniqueness (which would mean that if x_1 and x_2 are two such integers x, then $x_1 = x_2$), but merely claiming a weaker form (namely, that if x_1 and x_2 are two such integers x, then $x_1 \equiv x_2 \bmod mn$).

Example 2.12.2. Theorem 2.12.1 **(a)** (applied to $m = 5$, $n = 6$ and $a = 3$ and $b = 2$) shows that there exists an integer $x \in \mathbb{Z}$ such that

$$(x \equiv 3 \bmod 5 \text{ and } x \equiv 2 \bmod 6).$$

We will soon find such an integer, after we have proved Theorem 2.12.1.

Example 2.12.3. Assume that we want to find an $x \in \mathbb{Z}$ such that

$$(x \equiv 3 \bmod 5 \text{ and } x \equiv 2 \bmod 6).$$

To compute such an x, let us follow the proof of Theorem 2.12.1 **(a)** above.

We need a modular inverse $5'$ of 5 modulo 6. Such an inverse is 5, since $5 \cdot 5 \equiv 1 \bmod 6$. (In this particular case, finding this modular inverse was easy, because all we had to do is to test the 6 numbers $0, 1, 2, 3, 4, 5$; it is clear that a modular inverse of a modulo m, if it exists, can be found within the set $\{0, 1, \ldots, m-1\}$. In general, there is a quick way to find a modular inverse of an integer a modulo an integer m using the "Extended Euclidean algorithm".)

We need a modular inverse $6'$ of 6 modulo 5. Such an inverse is 1, since $6 \cdot 1 \equiv 1 \bmod 5$.

Now, the proof of Theorem 2.12.1 **(a)** tells us that $x_0 = 6 \cdot 6' \cdot 3 + 5 \cdot 5' \cdot 2$ is an integer $x \in \mathbb{Z}$ such that $(x \equiv 3 \bmod 5 \text{ and } x \equiv 2 \bmod 6)$. This x_0 is

$$6 \cdot 6' \cdot 3 + 5 \cdot 5' \cdot 2 = 6 \cdot 1 \cdot 3 + 5 \cdot 5 \cdot 2 = 68.$$

So we have found an $x \in \mathbb{Z}$ such that $(x \equiv 3 \bmod 5 \text{ and } x \equiv 2 \bmod 6)$, namely $x = 68$. (We can easily check this: $68 \equiv 3 \bmod 5$ since $68 - 3 = 5 \cdot 13$; and $68 \equiv 2 \bmod 6$ since $68 - 2 = 6 \cdot 11$.)

There is also a version of Theorem 2.12.1 for multiple integers:

Theorem 2.12.4. Let $m_1, m_2, \ldots, m_k$ be k mutually coprime integers. Let $a_1, a_2, \ldots, a_k \in \mathbb{Z}$.

(a) There exists an integer x such that

$$(x \equiv a_i \bmod m_i \text{ for all } i \in \{1, 2, \ldots, k\}). \tag{18}$$

(b) If x_1 and x_2 are two such integers x, then $x_1 \equiv x_2 \bmod m_1 m_2 \cdots m_k$.

Again, Theorem 2.12.4 **(b)** is often stated in the form "This integer x is unique modulo $m_1 m_2 \cdots m_k$".

Clearly, Theorem 2.12.1 is the particular case of Theorem 2.12.4 obtained for $k = 2$.

2.13. Primes

2.13.1. Definition and the Sieve of Eratosthenes

Definition 2.13.1. Let p be an integer greater than 1. We say that p is *prime* if the only positive divisors of p are 1 and p. A prime integer is often just called *a prime*.

Note that we required p to be greater than 1 here. Thus, 1 does not count as prime even though its only positive divisor is 1 itself.

Example 2.13.2. (a) The only positive divisors of 7 are 1 and 7. Thus, 7 is a prime.

(b) The positive divisors of 14 are 1, 2, 7 and 14. These are more than just 1 and 14. Thus, 14 is not a prime.

(c) None of the numbers $4, 6, 8, 10, 12, 14, 16, \ldots$ (that is, the multiples of 2 that are larger than 2) is a prime. Indeed, if p is any of these numbers, then p has a positive divisor other than 1 and p (namely, 2), and therefore does not meet the definition of "prime".

(d) None of the numbers $6, 9, 12, 15, 18, \ldots$ (that is, the multiples of 3 that are larger than 3) is a prime. Indeed, if p is any of these numbers, then p has a positive divisor other than 1 and p (namely, 3), and therefore does not meet the definition of "prime".

Parts **(c)** and **(d)** of Example 2.13.2 suggest a method for finding all primes up to a given integer:

Example 2.13.3. Let us say we want to find all primes that are ≤ 30.

Step 1: All such primes must lie in $\{2, 3, \ldots, 30\}$ (since a prime is always an integer greater than 1); thus, let us first write down all elements of $\{2, 3, \ldots, 30\}$:

$$\begin{array}{cccccccccc} & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 & 29 & 30 \end{array}.$$

(We are using a table just in order to fit these elements on a page.)

We now plan to remove non-prime numbers from this table until only primes are left.

Step 2: First, let us remove all multiples of 2 that are larger than 2 from our table, because none of them is a prime (see Example 2.13.2 **(c)**). We thus are left with

$$\begin{array}{ccccccc} & 2 & 3 & & 5 & 7 & 9 \\ 11 & & 13 & & 15 & 17 & 19 \\ 21 & & 23 & & 25 & 27 & 29 \end{array}.$$

Step 3: Next, let us remove all multiples of 3 that are larger than 3 from our table, because none of them is a prime (see Example 2.13.2 **(d)**). We thus are left with

$$\begin{array}{ccccccc} & 2 & 3 & & 5 & 7 & \\ 11 & & 13 & & & 17 & 19 \\ & & 23 & & 25 & & 29 \end{array}.$$

(Note that some of these multiples have already been removed in Step 2.)

Step 4: Next, let us remove all multiples of 4 that are larger than 4 from our table, because none of them is a prime (for similar reasons). It turns out that this does not change the table at all, because all such multiples have already been removed in Step 2. This is not a coincidence: Since 4 itself has been removed, we know that 4 was a multiple of some number $d < 4$ (in this case, $d = 2$) whose

multiples have been removed; therefore, all multiples of 4 are also multiples of d and thus have been removed along with 4.

Step 5: Next, let us remove all multiples of 5 that are larger than 5 from our table, because none of them is a prime (for similar reasons). We thus are left with

$$\begin{array}{cccccc} & 2 & 3 & & 5 & & 7 & \\ 11 & & 13 & & & 17 & & 19 \\ & & 23 & & & & 29 & \end{array}.$$

Step 6: Next, let us remove all multiples of 6 that are larger than 6 from our table, because none of them is a prime. Just as Step 4, this does not change the table, since all such multiples have already been removed in Step 2.

Step 7: Next, let us remove all multiples of 7 that are larger than 7 from our table, because none of them is a prime. Again, this does not change the table, since all such multiples have already been removed.

Proceed likewise until Step 30, at which point the table has become

$$\begin{array}{cccccc} & 2 & 3 & & 5 & & 7 & \\ 11 & & 13 & & & 17 & & 19 \\ & & 23 & & & & 29 & \end{array}.$$

(You are reading it right: None of the steps from Step 6 to Step 30 causes any changes to the table, since all multiples that these steps attempt to remove have already been removed beforehand.)

The resulting table has the following property: If p is an element of this table, then p cannot be a multiple of any $d \in \{2,3,\ldots,p-1\}$ (because if it was such a multiple, then it would have been removed from the table in Step d or earlier). In other words, if p is an element of this table, then p cannot have any divisor $d \in \{2,3,\ldots,p-1\}$. In other words, if p is an element of this table, then the only positive divisors of p are 1 and p. In other words, if p is an element of this table, then p is prime. Conversely, any prime ≤ 30 is in our table, since the only numbers we have removed from the table were guaranteed to be non-prime. Thus, the table now contains all the primes ≤ 30 and only them. So we conclude that the primes ≤ 30 are $2,3,5,7,11,13,17,19,23,29$.

This method of finding primes is known as the *sieve of Eratosthenes*. We could have made it more efficient using the following two tricks:

- If a number $d \in \{2,3,\ldots,30\}$ has been removed from the table before Step d, then we know immediately that Step d will not change the table (because all multiples of d have already been removed before this step). Thus, we do not need to make this step.
- If $d \in \{2,3,\ldots,30\}$ satisfies $d^2 > 30$, then Step d will not change the table[13]. Thus, we only need to take the Steps d with $d^2 \leq 30$.

Together, these tricks tell us that the only steps we need to take are the Steps 2, 3 and 5.

2.13.2. Basic properties of primes

Proposition 2.13.4. Let p be a prime. Then, each $i \in \{1, 2, \ldots, p-1\}$ is coprime to p.

Note that this proposition characterizes primes: If $p > 1$ is an integer such that each $i \in \{1, 2, \ldots, p-1\}$ is coprime to p, then p is prime. (The proof of this is left as an easy exercise.)

Proposition 2.13.5. Let p be a prime. Let $a \in \mathbb{Z}$. Then, either $p \mid a$ or $p \perp a$.

We note that a converse of Proposition 2.13.5 holds as well: If $p > 1$ is an integer such that each $a \in \mathbb{Z}$ satisfies either $p \mid a$ or $p \perp a$, then p is a prime. This is easy to prove and left to the reader.

Exercise 2.13.1. Let p and q be two distinct primes. Prove that $p \perp q$.

Theorem 2.13.6. Let p be a prime. Let $a, b \in \mathbb{Z}$ such that $p \mid ab$. Then, $p \mid a$ or $p \mid b$.

Again, Theorem 2.13.6 has a converse:

Exercise 2.13.2. Let $p > 1$ be an integer. Assume that for every $a, b \in \mathbb{Z}$ satisfying $p \mid ab$, we must have $p \mid a$ or $p \mid b$. Prove that p is prime.

There is also a version of Theorem 2.13.6 for products of multiple integers:

[13] *Proof.* Let $d \in \{2, 3, \ldots, 30\}$ be such that $d^2 > 30$. We must show that Step d will not change the table.

Indeed, at Step d, we remove all multiples of d that are larger than d from our table. But all these multiples (at least the ones that appear in our table) have already been removed from this table before Step d.

Here is why: Let $m \in \{2, 3, \ldots, 30\}$ be a multiple of d that is larger than d. Then, $d \mid m$ (since m is a multiple of d) and thus $m/d \in \mathbb{Z}$. Hence, m/d is a positive integer (since m/d is clearly positive) and $m/d > 1$ (since m is larger than d). Furthermore, $m/d \mid m$ (since $m = (m/d)\, d$), so that m is a multiple of m/d. But $d > 1$ (since $d \in \{2, 3, \ldots, 30\}$) and thus $m/d < m$. In other words, $m > m/d$. Hence, m is a multiple of m/d that is larger than m/d.

Furthermore, $d^2 > 30 \geq m$ (since $m \in \{2, 3, \ldots, 30\}$). Dividing both sides of this inequality by d, we obtain $d > m/d$. Hence, $m/d < d$, so that $m/d \in \{2, 3, \ldots, d-1\}$ (since $m/d > 1$). Thus, before Step d begins, Step m/d has already happened. Of course, Step m/d has removed m from the table (since m is a multiple of m/d that is larger than m/d). Therefore, the number m has already been removed from the table before Step d.

Now, forget that we fixed m. We thus have shown that if $m \in \{2, 3, \ldots, 30\}$ is a multiple of d that is larger than d, then m has already been removed from the table before Step d. In other words, all multiples of d that we try to remove at Step d have already been removed before Step d. Therefore, Step d does not change our table.

Proposition 2.13.7. Let p be a prime. Let $a_1, a_2, \ldots, a_k$ be integers such that $p \mid a_1 a_2 \cdots a_k$. Then, $p \mid a_i$ for some $i \in \{1, 2, \ldots, k\}$.

We could prove Proposition 2.13.7 by induction on k. But here is a more direct argument:

Exercise 2.13.3. Let p be a prime. Let k be a positive integer. Let $a \in \mathbb{Z}$. Prove that $a \perp p^k$ holds if and only if $p \nmid a$.

2.13.3. Prime factorization I

The next simple proposition says that every integer $n > 1$ is divisible by at least one prime:

Proposition 2.13.8. Let $n > 1$ be an integer. Then, there exists at least one prime p such that $p \mid n$.

Definition 2.13.9. Let n be an integer. A *prime factor* of n means a prime p such that $p \mid n$. Some say "prime divisor" instead of "prime factor".

Thus, Proposition 2.13.8 says that each integer $n > 1$ has at least one prime divisor.

Proposition 2.13.10. Let n be a positive integer. Then, n can be written as a product of finitely many primes.

Example 2.13.11. (a) The integer 60 can be written as a product of four primes: namely, $60 = 2 \cdot 2 \cdot 3 \cdot 5$.

(b) The integer 1 is the product of 0 many primes (because a product of 0 many primes is the empty product, which is defined to be 1).

Proposition 2.13.10 shows that every positive integer n can be represented as a product of finitely many primes. Such a representation – or, more precisely, the list of the primes it contains – will be called the *prime factorization* of n. Rigorously speaking, this means that we make the following definition:

Definition 2.13.12. Let n be a positive integer. A *prime factorization* of n means a tuple $(p_1, p_2, \ldots, p_k)$ of primes such that $n = p_1 p_2 \cdots p_k$.

Keep in mind that "tuple" always means "ordered tuple" unless we say otherwise.

Example 2.13.13. (a) The prime factorizations of 12 are

$$(2,2,3), \qquad (2,3,2), \qquad (3,2,2).$$

Indeed, these three 3-tuples are prime factorizations of 12 because $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$. It is not hard to check that they are the only prime factorizations of 12.

(b) If p is a prime, then the only prime factorization of p is the 1-tuple (p).

(c) If p is a prime and $i \in \mathbb{N}$, then the only prime factorization of p^i is the i-tuple $\left(\underbrace{p, p, \ldots, p}_{i \text{ times}}\right)$. This is not quite obvious at this point (though it is not hard to derive from Proposition 2.13.7).

(d) The only prime factorization of 1 is the 0-tuple $()$.

This example suggests that all prime factorizations of a given positive integer n are equal to each other up to the order of their entries (i.e., are permutations of each other). This is indeed true, and we are going to prove this soon (in Theorem 2.13.31 below).

2.13.4. Permutations

First of all: what is a "permutation", and what exactly does "equal to each other up to the order of their entries" mean?

Informally speaking, a permutation of a tuple[14] $(a_1, a_2, \ldots, a_k)$ is a tuple obtained from $(a_1, a_2, \ldots, a_k)$ by rearranging its entries (without inserting new entries, or removing or duplicating existing entries). To be rigorous, we need to encode this rearrangement via a bijective map $\sigma : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$ which will tell us which entry of our original tuple will go to which position in the rearranged tuple. Such bijective maps, too, are called permutations – but permutations of sets, not of tuples. So let us first define permutations of a set, and then use this to define permutations of a tuple:

Definition 2.13.14. Let A be a set. A *permutation* of A means a bijective map $A \to A$.

Example 2.13.15. (a) The map $\{1,2,3,4\} \to \{1,2,3,4\}$ that sends $1,2,3,4$ to $3,1,4,2$ (respectively) is a permutation of $\{1,2,3,4\}$.

(b) The map $\{1,2,3\} \to \{1,2,3\}$ that sends $1,2,3$ to $2,3,1$ (respectively) is a permutation of $\{1,2,3\}$.

(c) For each set A, the identity map $\mathrm{id} : A \to A$ is a permutation of A.

Thus, we have defined permutations of a set. We shall later study such permutations in more detail, at least for finite sets A.

[14] Recall: a prime factorization is a tuple.

Now we can define permutations of a tuple:

Definition 2.13.16. Let $(p_1, p_2, \ldots, p_k)$ be a k-tuple. A *permutation* of $(p_1, p_2, \ldots, p_k)$ means a k-tuple of the form $\left(p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(k)}\right)$ where σ is a permutation of the set $\{1, 2, \ldots, k\}$. A permutation of $(p_1, p_2, \ldots, p_k)$ is also known as a *rearrangement* of $(p_1, p_2, \ldots, p_k)$.

Example 2.13.17. (a) The 4-tuple $(1, 3, 1, 2)$ is a permutation of the 4-tuple $(3, 2, 1, 1)$. In fact, if we denote the 4-tuple $(3, 2, 1, 1)$ by (p_1, p_2, p_3, p_4), then there exists a permutation σ of the set $\{1, 2, 3, 4\}$ such that $(1, 3, 1, 2) = \left(p_{\sigma(1)}, p_{\sigma(2)}, p_{\sigma(3)}, p_{\sigma(4)}\right)$. (Actually, there exist two such permutations σ: One of them sends $1, 2, 3, 4$ to $3, 1, 4, 2$, while the other sends $1, 2, 3, 4$ to $4, 1, 3, 2$.)

(b) Any k-tuple is a permutation of itself. Indeed, if $(p_1, p_2, \ldots, p_k)$ is any k-tuple, then $(p_1, p_2, \ldots, p_k) = \left(p_{\sigma(1)}, p_{\sigma(2)}, \ldots, p_{\sigma(k)}\right)$ if we let σ be the identity map $\mathrm{id} : \{1, 2, \ldots, k\} \to \{1, 2, \ldots, k\}$.

The following fact is easy and fundamental:

Proposition 2.13.18. Let $(p_1, p_2, \ldots, p_k)$ be a k-tuple. If $(q_1, q_2, \ldots, q_k)$ is a permutation of $(p_1, p_2, \ldots, p_k)$, then $(p_1, p_2, \ldots, p_k)$ is a permutation of $(q_1, q_2, \ldots, q_k)$.

Now, we can say what we mean when we say that two tuples differ only in the order of their entries:

Definition 2.13.19. We say that two tuples *differ only in the order of their entries* if they are permutations of each other.

The next lemma that we shall use is a basic fact from elementary combinatorics:

Lemma 2.13.20. Let P be a set. Let $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ be two tuples of elements of P. Assume that for each $p \in P$, we have

$$\begin{aligned}&(\text{the number of times } p \text{ appears in } (a_1, a_2, \ldots, a_k))\\ &= (\text{the number of times } p \text{ appears in } (b_1, b_2, \ldots, b_\ell)).\end{aligned} \tag{19}$$

Then, the two tuples $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ differ only in the order of their entries (i.e., are permutations of each other). (In other words, we have $k = \ell$, and there exists a permutation σ of the set $\{1, 2, \ldots, \ell\}$ such that $(a_1, a_2, \ldots, a_k) = \left(b_{\sigma(1)}, b_{\sigma(2)}, \ldots, b_{\sigma(\ell)}\right)$.)

Lemma 2.13.20 is an intuitively obvious fact: It says that if two tuples (of any objects – e.g., numbers) have the property that any object occurs as often in the first tuple as it does in the second tuple, then the two tuples differ only in the order of

their entries. From the formal point of view, though, it is a statement that needs proof. Let us merely sketch how such a proof can be obtained, without going into the details:

Lemma 2.13.20 has a converse that is much simpler:

Lemma 2.13.21. Let P be a set. Let $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ be two tuples of elements of P. Assume that these two tuples $(a_1, a_2, \ldots, a_k)$ and $(b_1, b_2, \ldots, b_\ell)$ differ only in the order of their entries (i.e., are permutations of each other). Then, for each $p \in P$, we have

$$\begin{aligned}&(\text{the number of times } p \text{ appears in } (a_1, a_2, \ldots, a_k))\\ &= (\text{the number of times } p \text{ appears in } (b_1, b_2, \ldots, b_\ell))\,.\end{aligned}$$

We leave the proof of this lemma to the reader.

2.13.5. p-valuations

Now, let us come back to number theory. We first claim that a nonzero integer n can only be divisible by finitely many powers of a given prime p. More precisely:

Lemma 2.13.22. Let p be a prime. Let n be a nonzero integer. Then, there exists a largest $m \in \mathbb{N}$ such that $p^m \mid n$.

The proof of this lemma will rely on a simple inequality, which we leave as an exercise:

Exercise 2.13.4. Let p be an integer such that $p > 1$. Prove that $p^k > k$ for each $k \in \mathbb{N}$.

Definition 2.13.23. Let p be a prime.

(a) Let n be a nonzero integer. Then, $v_p(n)$ shall denote the largest $m \in \mathbb{N}$ such that $p^m \mid n$. This is well-defined (by Lemma 2.13.22). This nonnegative integer $v_p(n)$ will be called the *p-valuation* (or the *p-adic valuation*) of n.

(b) We extend this definition of $v_p(n)$ to the case of $n = 0$ as follows: Set $v_p(0) = \infty$, where ∞ is a new symbol. This symbol ∞ is supposed to model "positive infinity"; in particular, we take it to satisfy the following rules:

- We have $k + \infty = \infty + k = \infty$ for all integers k.
- We have $\infty + \infty = \infty$.
- Each integer k satisfies $k < \infty$ and $\infty > k$ (and thus $k \leq \infty$ and $\infty \geq k$).
- No integer k satisfies $k \geq \infty$ or $\infty \leq k$ (or $k > \infty$ or $\infty < k$).

- If S is a nonempty set of integers, then $\min\left(S \cup \{\infty\}\right) = \min S$ (provided that $\min S$ exists).
- We have $\min\{\infty\} = \infty$.
- If S is any set of integers, then $\max\left(S \cup \{\infty\}\right) = \infty$.

(Note, however, that ∞ is not supposed to be a "first class citizen" of the number system. In particular, $\infty - \infty$ is not defined. More generally, $k - \infty$ is never defined, whatever k is. Indeed, any definition of $k - \infty$ would break some of the familiar rules of arithmetic. The only operations that we shall subject ∞ to are addition, minimum and maximum.)

Note that the rules for the symbol ∞ yield that

$$k + \infty = \infty + k = \max\{k, \infty\} = \infty$$

and

$$\min\{k, \infty\} = k$$

for each $k \in \mathbb{Z} \cup \{\infty\}$. It is not hard to see that basic properties of inequalities (such as "if $a \leq b$ and $b \leq c$, then $a \leq c$") and of addition (such as "$(a+b)+c = a+(b+c)$") and of the interplay between inequalities and addition (such as "if $a \leq b$, then $a + c \leq b + c$") are still valid in $\mathbb{Z} \cup \{\infty\}$ (that is, they still hold if we plug ∞ for one or more of the variables). However, of course, we cannot "cancel" ∞ from equalities (i.e., we cannot cancel ∞ from $a + \infty = b + \infty$ to obtain $a = b$) or inequalities.

Example 2.13.24. (a) We have $v_5(50) = 2$. Indeed, 2 is the largest $m \in \mathbb{N}$ such that $5^m \mid 50$ (because $5^2 = 25 \mid 50$ but $5^3 = 125 \nmid 50$).

(b) We have $v_5(51) = 0$. Indeed, 0 is the largest $m \in \mathbb{N}$ such that $5^m \mid 51$ (because $5^0 = 1 \mid 51$ but $5^1 = 5 \nmid 51$).

(c) We have $v_5(55) = 1$. Indeed, 1 is the largest $m \in \mathbb{N}$ such that $5^m \mid 55$ (because $5^1 = 5 \mid 55$ but $5^2 = 25 \nmid 55$).

(d) We have $v_5(0) = \infty$ (by Definition 2.13.23 **(b)**).

Definition 2.13.23 **(a)** can be restated in the following more intuitive way: Given a prime p and a nonzero integer n, we let $v_p(n)$ be the number of times we can divide n by p without leaving $\mathbb{Z}$. Definition 2.13.23 **(b)** is consistent with this picture, because we can clearly divide 0 by p infinitely often without leaving $\mathbb{Z}$. From this point of view, the following lemma should be obvious:

Lemma 2.13.25. Let p be a prime. Let $i \in \mathbb{N}$. Let $n \in \mathbb{Z}$. Then, $p^i \mid n$ if and only if $v_p(n) \geq i$.

Corollary 2.13.26. Let p be a prime. Let $n \in \mathbb{Z}$. Then, $v_p(n) = 0$ if and only if $p \nmid n$.

Here is another property of p-valuations that is useful in their study:

Lemma 2.13.27. Let p be a prime. Let $n \in \mathbb{Z}$ be nonzero. Then:
(a) There exists a nonzero integer u such that $u \perp p$ and $n = up^{v_p(n)}$.
(b) If $i \in \mathbb{N}$ and $w \in \mathbb{Z}$ are such that $w \perp p$ and $n = wp^i$, then $v_p(n) = i$.

Before we prove this formally, let us show the idea behind this lemma. Recall that, given a prime p and a nonzero integer n, the number $v_p(n)$ counts how often we can divide n by p without leaving $\mathbb{Z}$. What happens after we have divided n by p this many times? We get a number u that is still an integer, but is no longer divisible by p, and thus must be coprime to p (by Proposition 2.13.5). This is what Lemma 2.13.27 **(a)** says. Lemma 2.13.27 **(b)** is a converse statement: It says that if we divide n by p some number of times (say, i times) and obtain an integer coprime to p, then i must be $v_p(n)$.

The next property of p-adic valuations is crucial, as it reveals how they can be computed and bounded:

Theorem 2.13.28. Let p be a prime.
(a) We have $v_p(ab) = v_p(a) + v_p(b)$ for any two integers a and b.
(b) We have $v_p(a+b) \geq \min\left\{v_p(a), v_p(b)\right\}$ for any two integers a and b.
(c) We have $v_p(1) = 0$.
(d) We have $v_p(q) = \begin{cases} 1, & \text{if } q = p; \\ 0, & \text{if } q \neq p \end{cases}$ for any prime q.

Note that Theorem 2.13.28 **(a)** gives a formula for $v_p(ab)$ in terms of $v_p(a)$ and $v_p(b)$, but there is no such formula for $v_p(a+b)$ (since $v_p(a)$ and $v_p(b)$ do not uniquely determine $v_p(a+b)$). Thus, Theorem 2.13.28 **(b)** only gives a bound.

Corollary 2.13.29. Let p be a prime. Let $a_1, a_2, \ldots, a_k$ be k integers. Then, $v_p(a_1 a_2 \cdots a_k) = v_p(a_1) + v_p(a_2) + \cdots + v_p(a_k)$.

Exercise 2.13.5. Let p be a prime. Let $n \in \mathbb{Z}$. Prove that $v_p(|n|) = v_p(n)$.

Exercise 2.13.6. Let p be a prime. Let $a \in \mathbb{Z}$ and $k \in \mathbb{N}$. Prove that $v_p\left(a^k\right) = kv_p(a)$.

Exercise 2.13.7. Let $p_1, p_2, \ldots, p_u$ be finitely many distinct primes. Let $a_1, a_2, \ldots, a_u$ be nonnegative integers.
(a) Prove that $v_{p_i}\left(p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}\right) = a_i$ for each $i \in \{1, 2, \ldots, u\}$.
(b) Prove that $v_p\left(p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}\right) = 0$ for each prime p satisfying $p \notin \{p_1, p_2, \ldots, p_u\}$.

2.13.6. Prime factorization II

Proposition 2.13.30. Let n be a positive integer. Let $(a_1, a_2, \ldots, a_k)$ be a prime factorization of n. Let p be a prime. Then,

$$\begin{aligned}&(\text{the number of times } p \text{ appears in the tuple } (a_1, a_2, \ldots, a_k))\\ &= (\text{the number of } i \in \{1, 2, \ldots, k\} \text{ such that } a_i = p)\\ &= v_p(n).\end{aligned}$$

We are finally ready to prove the so-called *Fundamental Theorem of Arithmetic*:

Theorem 2.13.31. Let n be a positive integer.
(a) There exists a prime factorization of n.
(b) Any two such factorizations differ only in the order of their entries (i.e., are permutations of each other).

2.13.7. The canonical factorization

You have seen finite products such as[15]

$$\prod_{i \in \{1,2,3,4,5\}} i = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5! = 120 \qquad \text{and}$$
$$\prod_{i \in \{3,5,7\}} \left(i^2 + 1\right) = \left(3^2 + 1\right) \cdot \left(5^2 + 1\right) \cdot \left(7^2 + 1\right) = 13000.$$

Sometimes, infinite products (i.e., products ranging over infinite sets) also make sense. Many examples of well-defined infinite products arise from analysis and have to do with convergence. Here, we are doing algebra and thus shall only consider a very elementary, non-analytic meaning of convergence. Namely, we will consider infinite products that have only finitely many factors different from 1. For example, the product $2 \cdot 7 \cdot 4 \cdot \underbrace{1 \cdot 1 \cdot 1 \cdot 1 \cdot \cdots}_{\text{infinitely many 1's}}$ is of such form. It is easy to give a meaning to such products: Just throw away all the 1's (since multiplying by 1 does not change a number) and take the product of the remaining (finitely many) numbers. So, for example, our product $2 \cdot 7 \cdot 4 \cdot \underbrace{1 \cdot 1 \cdot 1 \cdot 1 \cdot \cdots}_{\text{infinitely many 1's}}$ should evaluate to $2 \cdot 7 \cdot 4 = 56$.

[15] Here and in the following, $n!$ denotes the product $1 \cdot 2 \cdot \cdots \cdot n$ whenever $n \in \mathbb{N}$. Thus, in particular,

$$0! = (\text{empty product}) = 1, \qquad 1! = 1, \qquad 2! = 1 \cdot 2 = 2,$$
$$3! = 1 \cdot 2 \cdot 3 = 6, \qquad 4! = 1 \cdot 2 \cdot 3 \cdot 4 = 24, \qquad 5! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120.$$

This is indeed a meaningful and useful definition. For example, the set of all prime numbers is infinite (by Theorem 2.13.43 below), but nevertheless, for each nonzero integer n, the product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ (where the "$\prod\limits_{p \text{ prime}}$" symbol means a product ranging over all primes p) is well-defined due to having only finitely many factors different from 1:

Lemma 2.13.32. Let n be a nonzero integer.

(a) We have $v_p(n) = 0$ for every prime $p > |n|$. (Note that "for every prime $p > |n|$" is shorthand for "for every prime p satisfying $p > |n|$".)

(b) The product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ has only finitely many factors different from 1.

(Here and in the following, the "$\prod\limits_{p \text{ prime}}$" symbol means a product ranging over all primes p.)

Corollary 2.13.33. Let n be a positive integer. Then,

$$n = \prod_{p \text{ prime}} p^{v_p(n)}.$$

Here, the infinite product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ is well-defined (according to Lemma 2.13.32 **(b)**).

This expression $n = \prod\limits_{p \text{ prime}} p^{v_p(n)}$ is called the *canonical factorization* of n.

The next exercise says that a nonnegative integer n is uniquely determined by the family $\left(v_p(n)\right)_{p \text{ prime}}$ of its p-valuations for all primes p:

Exercise 2.13.8. Let n and m be two nonnegative integers. Assume that

$$v_p(n) = v_p(m) \qquad \text{for every prime } p. \tag{20}$$

Prove that $n = m$.

Corollary 2.13.34. Let n be a nonzero integer. Then,

$$|n| = \prod_{p \text{ prime}} p^{v_p(n)}.$$

Here, the infinite product $\prod\limits_{p \text{ prime}} p^{v_p(n)}$ is well-defined (according to Lemma 2.13.32 **(b)**).

We can furthermore use p-adic valuations to check divisibility of integers:

Proposition 2.13.35. Let n and m be integers. Then, $n \mid m$ if and only if each prime p satisfies $v_p(n) \leq v_p(m)$.

Let us extract one of the steps of our above proof into a separate lemma, since we shall use the same reasoning later on:

Lemma 2.13.36. For each prime p, let a_p and b_p be nonnegative integers such that

$$a_p \leq b_p. \tag{21}$$

Assume that all but finitely many primes p satisfy $b_p = 0$. Then, the products $\prod\limits_{p \text{ prime}} p^{a_p}$ and $\prod\limits_{p \text{ prime}} p^{b_p}$ are both well-defined and satisfy

$$\prod_{p \text{ prime}} p^{a_p} \mid \prod_{p \text{ prime}} p^{b_p}. \tag{22}$$

Corollary 2.13.37. For each prime p, let b_p be a nonnegative integer. Assume that all but finitely many primes p satisfy $b_p = 0$. Let $n = \prod\limits_{p \text{ prime}} p^{b_p}$. Then,

$$v_q(n) = b_q \qquad \text{for each prime } q.$$

Exercise 2.13.9. Let n be a nonzero integer. Let a and b be two integers. Assume that

$$a \equiv b \bmod p^{v_p(n)} \qquad \text{for every prime } p. \tag{23}$$

Prove that $a \equiv b \bmod n$.

Canonical factorizations can also be used to describe gcds and lcms:

Proposition 2.13.38. Let n and m be two nonzero integers. Then,

$$\gcd(n,m) = \prod_{p \text{ prime}} p^{\min\left\{v_p(n), v_p(m)\right\}} \tag{24}$$

and

$$\operatorname{lcm}(n,m) = \prod_{p \text{ prime}} p^{\max\left\{v_p(n), v_p(m)\right\}}. \tag{25}$$

Example 2.13.39. For this example, set $n = 3^2 \cdot 5 \cdot 7^8$ and $m = 2 \cdot 3^3 \cdot 7^2$. Let us compute $\gcd(n,m)$ and $\operatorname{lcm}(n,m)$ using Proposition 2.13.38.

From $n = 3^2 \cdot 5 \cdot 7^8$, we obtain (using Corollary 2.13.37) that

$$v_3(n) = 2, \qquad v_5(n) = 1, \qquad v_7(n) = 8, \qquad \text{and}$$
$$v_p(n) = 0 \text{ for each prime } p \notin \{3,5,7\}.$$

Similarly, from $m = 2 \cdot 3^3 \cdot 7^2$, we obtain

$$v_2(m) = 1, \qquad v_3(m) = 3, \qquad v_7(m) = 2, \qquad \text{and}$$
$$v_p(n) = 0 \text{ for each prime } p \notin \{2,3,7\}.$$

Now, (24) yields

$$\begin{aligned}
&\gcd(n,m) \\
&= \prod_{p \text{ prime}} p^{\min\left\{v_p(n), v_p(m)\right\}} \\
&= \underbrace{2^{\min\{v_2(n),v_2(m)\}}}_{=2^{\min\{0,1\}}=2^0} \cdot \underbrace{3^{\min\{v_3(n),v_3(m)\}}}_{=3^{\min\{2,3\}}=3^2} \cdot \underbrace{5^{\min\{v_5(n),v_5(m)\}}}_{=5^{\min\{1,0\}}=5^0} \\
&\quad \cdot \underbrace{7^{\min\{v_7(n),v_7(m)\}}}_{=7^{\min\{8,2\}}=7^2} \cdot \prod_{\substack{p \text{ prime;} \\ p \notin \{2,3,5,7\}}} \underbrace{p^{\min\left\{v_p(n), v_p(m)\right\}}}_{\substack{=1 \\ \text{(since } v_p(n)=0 \text{ and } v_p(m)=0 \\ \text{and thus } \min\left\{v_p(n), v_p(m)\right\} = \min\{0,0\} = 0\text{)}}} \\
&= 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^2 = 3^2 \cdot 7^2.
\end{aligned}$$

Likewise, (25) yields

$$\begin{aligned}
&\operatorname{lcm}(n,m) \\
&= \prod_{p \text{ prime}} p^{\max\left\{v_p(n), v_p(m)\right\}} \\
&= \underbrace{2^{\max\{v_2(n),v_2(m)\}}}_{=2^{\max\{0,1\}}=2^1} \cdot \underbrace{3^{\max\{v_3(n),v_3(m)\}}}_{=3^{\max\{2,3\}}=3^3} \cdot \underbrace{5^{\max\{v_5(n),v_5(m)\}}}_{=5^{\max\{1,0\}}=5^1} \\
&\quad \cdot \underbrace{7^{\max\{v_7(n),v_7(m)\}}}_{=7^{\max\{8,2\}}=7^8} \cdot \prod_{\substack{p \text{ prime;} \\ p \notin \{2,3,5,7\}}} \underbrace{p^{\max\left\{v_p(n), v_p(m)\right\}}}_{\substack{=1 \\ \text{(since } v_p(n)=0 \text{ and } v_p(m)=0 \\ \text{and thus } \max\left\{v_p(n), v_p(m)\right\} = \max\{0,0\} = 0\text{)}}} \\
&= 2^1 \cdot 3^3 \cdot 5^1 \cdot 7^8.
\end{aligned}$$

Proposition 2.13.38 can be generalized to the case of k integers $b_1, b_2, \ldots, b_k$ instead of two integers n, m:

Proposition 2.13.40. Let $b_1, b_2, \ldots, b_k$ be finitely many nonzero integers, with $k > 0$. Then,

$$\gcd(b_1, b_2, \ldots, b_k) = \prod_{p \text{ prime}} p^{\min\left\{v_p(b_1), v_p(b_2), \ldots, v_p(b_k)\right\}} \tag{26}$$

an

$$\operatorname{lcm}(b_1, b_2, \ldots, b_k) = \prod_{p \text{ prime}} p^{\max\left\{v_p(b_1), v_p(b_2), \ldots, v_p(b_k)\right\}}. \tag{27}$$

We can use Propositions 2.13.38 and 2.13.40 to reprove certain facts about lcms and gcds. For example, let us prove Theorem 2.11.6 and solve Exercise 2.11.2:

Exercise 2.13.10. Let n and m be two integers. Let p be a prime.
(a) Prove that $v_p(\gcd(n,m)) = \min\{v_p(n), v_p(m)\}$.
(b) Prove that $v_p(\operatorname{lcm}(n,m)) = \max\{v_p(n), v_p(m)\}$.

Exercise 2.13.11. Let a, b, c be three integers.
(a) Prove that $\gcd(a, \operatorname{lcm}(b,c)) = \operatorname{lcm}(\gcd(a,b), \gcd(a,c))$.
(b) Prove that $\operatorname{lcm}(a, \gcd(b,c)) = \gcd(\operatorname{lcm}(a,b), \operatorname{lcm}(a,c))$.

The two parts of Exercise 2.13.11 can be regarded as "distributivity laws", but for the binary operations gcd and lcm (or lcm and gcd, respectively) instead of $+$ and $\cdot$.

2.13.8. Coprimality through prime factors

Proposition 2.13.41. Let n and m be two integers. Then, $n \perp m$ if and only if there exists no prime p that divides both n and m.

Corollary 2.13.42. Let n and m be two nonzero integers. Then:
(a) The infinite sum $\sum_{p \text{ prime}} v_p(n) v_p(m)$ is well-defined (i.e., all but finitely many primes p satisfy $v_p(n) v_p(m) = 0$).
(b) We have $n \perp m$ if and only if

$$\sum_{p \text{ prime}} v_p(n) v_p(m) = 0.$$

Corollary 2.13.42 **(b)** is the reason for the notation "$\perp$" that we are using for coprimality. In fact, when n is a positive integer, we can regard the p-valuations $v_p(n)$ as the "coordinates" of n in an (infinite-dimensional) Cartesian coordinate system. Then, the sum $\sum_{p \text{ prime}} v_p(n) v_p(m)$ in Corollary 2.13.42 is something like a "dot product" between n and m. Thus, Corollary 2.13.42 **(b)** shows that two integers n and m are coprime if and only if their "dot product" is 0. But for vectors in a Euclidean space, the dot product is 0 if and only if the vectors are orthogonal. Thus, coprime integers are like orthogonal vectors. Of course, this analogy should be taken with a grain of salt; in particular, our "dot product" is far from being bilinear[16].

[16] Or, rather, it is bilinear **with respect to multiplication**: If we denote $\sum_{p \text{ prime}} v_p(n) v_p(m)$ by $\langle n, m \rangle$, then we have

$$\langle n_1 n_2, m \rangle = \langle n_1, m \rangle + \langle n_2, m \rangle \qquad \text{and} \qquad \langle n, m_1 m_2 \rangle = \langle n, m_1 \rangle + \langle n, m_2 \rangle$$

for arbitrary integers n_1, n_2, m, n, m_1, m_2.

2.13.9. There are infinitely many primes

Theorem 2.13.43. There are infinitely many primes.

Note that our proof of Theorem 2.13.43 is constructive: It gives an algorithm to construct arbitrarily many distinct primes. This algorithm is not very efficient, since $p_1 p_2 \cdots p_k + 1$ can be very large even if $p_1, p_2, \ldots, p_k$ are fairly small. In practice, the sieve of Eratosthenes is much better for generating primes. Much faster algorithms are known.

Exercise 2.13.12. Let p be a prime. Let $a \in \mathbb{Z}$ be such that $a^2 \equiv 1 \bmod p$. Prove that $a \equiv 1 \bmod p$ or $a \equiv -1 \bmod p$.

Exercise 2.13.13. Let p be a prime. Let $k \in \mathbb{N}$. Prove that the nonnegative divisors of p^k are $p^0, p^1, \ldots, p^k$.

2.14. Euler's totient function (ϕ-function)

2.14.1. Definition and some formulas

Recall that $\mathbb{P}$ stands for the set of all positive integers.

Definition 2.14.1. We define a function $\phi : \mathbb{P} \to \mathbb{N}$ as follows: For each $n \in \mathbb{P}$, we let $\phi(n)$ be the number of all $i \in \{1, 2, \ldots, n\}$ that are coprime to n. In other words,

$$\phi(n) = |\{i \in \{1, 2, \ldots, n\} \mid i \perp n\}|. \tag{28}$$

This function ϕ is called *Euler's totient function* or just *ϕ-function*.

Example 2.14.2. (a) We have $\phi(12) = 4$, since the number of all $i \in \{1, 2, \ldots, 12\}$ that are coprime to 12 is 4 (indeed, these i are 1, 5, 7 and 11).

(b) We have $\phi(13) = 12$, since the number of all $i \in \{1, 2, \ldots, 13\}$ that are coprime to 13 is 12 (indeed, these i are $1, 2, \ldots, 12$).

(c) We have $\phi(14) = 6$, since the number of all $i \in \{1, 2, \ldots, 14\}$ that are coprime to 14 is 6 (indeed, these i are $1, 3, 5, 9, 11, 13$).

(d) We have $\phi(1) = 1$, since the number of all $i \in \{1, 2, \ldots, 1\}$ that are coprime to 1 is 1 (indeed, the only such i is 1).

The ϕ-function ϕ is denoted by φ by some authors.

Proposition 2.14.3. Let p be a prime. Then, $\phi(p) = p - 1$.

Proposition 2.14.3 can be generalized as follows:

Exercise 2.14.1. Let p be a prime. Let k be a positive integer. Prove that $\phi\left(p^k\right) = (p-1)\,p^{k-1}$.

Theorem 2.14.4. Let m and n be two coprime positive integers. Then, $\phi(mn) = \phi(m)\cdot\phi(n)$.

We will prove Theorem 2.14.4 later (in Section 2.16.3).

Theorem 2.14.5. Let n be a positive integer. Then,

$$\phi(n) = \prod_{\substack{p \text{ prime;} \\ p\mid n}} \left((p-1)\,p^{v_p(n)-1}\right) = n\cdot \prod_{\substack{p \text{ prime;} \\ p\mid n}} \left(1-\frac{1}{p}\right).$$

Theorem 2.14.5 will be proven in Section 2.16.3.

Exercise 2.14.2. Let n be a positive integer.
(a) Prove that

$$n-\phi(n) = \left|\{i\in\{1,2,\ldots,n\} \mid \text{we don't have } i\perp n\}\right|.$$

(b) We have $n-\phi(n)\geq 0$.
(c) Let d be a positive divisor of n. Prove that $d-\phi(d)\leq n-\phi(n)$.
(d) Let d be a positive divisor of n such that $d\neq n$. Prove that $d-\phi(d) < n-\phi(n)$.

2.14.2. The totient sum theorem

Theorem 2.14.6. Let n be a positive integer. Then,

$$\sum_{d\mid n}\phi(d) = n.$$

Here and in the following, the symbol "$\sum_{d\mid n}$" stands for "sum over all **positive** divisors d of n".

For example, for $n=12$, Theorem 2.14.6 states that

$$\phi(1)+\phi(2)+\phi(3)+\phi(4)+\phi(6)+\phi(12) = 12.$$

Before we prove Theorem 2.14.6, let us motivate an argument via a classical puzzle:

Exercise 2.14.3. You have a corridor with 1000 lamps, which are initially all off. Each lamp has a lightswitch controlling its state.

Every night, a ghost glides through the corridor (always in the same direction) and flips some of the switches:

On the 1st night, the ghost flips every switch.

On the 2nd night, the ghost flips switches $2, 4, 6, 8, 10, \ldots$.

On the 3rd night, the ghost flips switches $3, 6, 9, 12, 15, \ldots$.

etc.

(That is: For each $k \in \{1, 2, \ldots, 1000\}$, the ghost spends the k-th night flipping switches $k, 2k, 3k, \ldots$.)

Which lamps will be on after 1000 nights?

In more rigorous terms, Exercise 2.14.3 is simply asking which of the numbers $1, 2, \ldots, 1000$ have an odd number of positive divisors. (Indeed, the situation after 1000 nights looks as follows: For each $n \in \{1, 2, \ldots, 1000\}$, the n-th switch has been flipped exactly once for each positive divisor of n; thus, the n-th lamp is on if and only if n has an odd number of positive divisors.)

Experiments reveal that among the first 10 positive integers, only three have an odd number of positive divisors: namely, 1, 4 and 9. (For example, 9 has the 3 positive divisors 1, 3 and 9.) This suggests the following:

Proposition 2.14.7. A positive integer n has an odd number of positive divisors if and only if n is a perfect square.

Having proven Proposition 2.14.7, we now can answer Exercise 2.14.3: The 31 lamps $1^2, 2^2, \ldots, 31^2$ (and no others) will be on after the 1000 nights. (Indeed, these 31 lamps correspond to the 31 perfect squares in the set $\{1, 2, \ldots, 1000\}$.)

The bijection F from the proof of Proposition 2.14.7 will serve us well in our proof of Theorem 2.14.6. Beside that, we need the following lemma:

Lemma 2.14.8. Let n be a positive integer. Let d be a positive divisor of n. Then,

$$(\text{the number of } i \in \{1, 2, \ldots, n\} \text{ such that } \gcd(i, n) = d) = \phi(n/d).$$

Exercise 2.14.4. Let $n \in \mathbb{N}$ satisfy $n > 2$. Prove that $\phi(n)$ is even.

Exercise 2.14.5. Let $n \in \mathbb{N}$ satisfy $n > 1$. Prove that

$$\sum_{\substack{i \in \{1,2,\ldots,n\}; \\ i \perp n}} i = n\phi(n)/2.$$

2.15. Fermat, Euler, Wilson

2.15.1. Fermat and Euler: statements

The following theorem is known as *Fermat's Little Theorem* (often abbreviated as "FLT"):

Theorem 2.15.1. Let p be a prime. Let $a \in \mathbb{Z}$.
(a) If $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$.
(b) We always have $a^p \equiv a \bmod p$.

The word "little" in the name of Theorem 2.15.1 is meant to distinguish the theorem from "Fermat's Last Theorem", a much more difficult result only proven in the 1990s. (Unfortunately, the latter result is also abbreviated as "FLT".)

We will prove Theorem 2.15.1 soon, by showing a more general result (Theorem 2.15.3). But before we do so, let us convince ourselves that the parts **(a)** and **(b)** of Theorem 2.15.1 are equivalent:

Remark 2.15.2. Theorem 2.15.1 **(b)** follows from Theorem 2.15.1 **(a)**, because (using the notations of Theorem 2.15.1):

- If $p \nmid a$, then Theorem 2.15.1 **(a)** yields $a^{p-1} \equiv 1 \bmod p$, thus $a^p = a \underbrace{a^{p-1}}_{\equiv 1 \bmod p} \equiv a1 = a \bmod p$.
- If $p \mid a$, then both a^p and a are $\equiv 0 \bmod p$ (because $p \mid a$ entails $a \equiv 0 \bmod p$ and thus $a^p \equiv 0^p = 0 \bmod p$ (since $p > 0$)), and therefore $a^p \equiv 0 \equiv a \bmod p$.

Conversely, Theorem 2.15.1 **(a)** follows from Theorem 2.15.1 **(b)** by the following argument: Let p and a be as in Theorem 2.15.1. Assume that $p \nmid a$. Then, $p \perp a$ (by Proposition 2.13.5), so that $a \perp p$. Thus, we can "cancel" a from any congruence modulo p (by Lemma 2.10.10). Doing this to the congruence $a^p \equiv a \bmod p$ (which follows from Theorem 2.15.1 **(b)**), we obtain $a^{p-1} \equiv 1 \bmod p$.

The next result is known as *Euler's theorem*:

Theorem 2.15.3. Let n be a positive integer. Let $a \in \mathbb{Z}$ be coprime to n.
Then, $a^{\phi(n)} \equiv 1 \bmod n$.

Theorem 2.15.3 yields Theorem 2.15.1 **(a)**, since $\phi(p) = p - 1$ when p is prime[17]. Since we also know that Theorem 2.15.1 **(b)** follows from Theorem 2.15.1 **(a)**, we see that a proof of Theorem 2.15.3 will immediately yield the whole Theorem 2.15.1. Before we give said proof, let us show an example of how Theorem 2.15.3 can be used:

[17] See below for details of this argument.

Exercise 2.15.1. What is the last digit of 3^{4^5}?

Notational remark: An expression of the form "a^{b^c}" always means $a^{(b^c)}$, not $\left(a^b\right)^c$. (Actually, there is no need for an extra notation for $\left(a^b\right)^c$, because $\left(a^b\right)^c = a^{bc}$.)

Theorem 2.15.3 is also the reason why certain rational numbers (such as $\frac{2}{7} = 0.\overline{285714}$ [18]) have purely periodic decimal expansions, while others (such as $\frac{1}{12} = 0.08\overline{3} = 0.0833333\ldots$ or $\frac{1}{2} = 0.5\overline{0} = 0.50000\ldots$) have their periods start only after some initial nonrepeating block. We refer [ConradE, §4] to the details of this.[19]

2.15.2. Proving Euler and Fermat

Our proof of Theorem 2.15.3 will rely on the following lemma:

Lemma 2.15.4. Let n be a positive integer. Then,

$$\phi(n) = \left|\{i \in \{0,1,\ldots,n-1\} \mid i \perp n\}\right|.$$

The next exercise shows an amusing (and useful) corollary of Fermat's Little Theorem: a situation in which congruent exponents lead to congruent powers (albeit under rather specific conditions, and with the congruent powers being congruent modulo a different number than the exponents):

Exercise 2.15.2. Let p be a prime. Let $a \in \mathbb{Z}$ be such that $p \nmid a$. Let $u, v \in \mathbb{N}$ satisfy $u \equiv v \bmod p-1$. Prove that $a^u \equiv a^v \bmod p$.

2.15.3. The Pigeonhole Principles

In our above proof of Theorem 2.15.3, we have proven that the map $f : C \to C$ (that we constructed) is injective and surjective. It turns out that this was, to some extent, wasteful: It would have been enough to prove one of the two properties only (i.e., injectivity **or** surjectivity). The reason for this are the following two basic facts about finite sets:

[18] The bar ($\overline{}$) over the "285714" means that we are repeating 285714 over and over. So $0.\overline{285714} = 0.285714285714285714\ldots$.

[19] In brief, the rule is as follows: Any fraction $\frac{a}{b}$ with $a, b \in \mathbb{Z}$ (and $b \neq 0$) has such a decimal representation with a period. (A *period* means a part that gets repeated over and over.) A fraction $\frac{a}{b}$ is called *purely periodic* if its period (in decimal notation) begins straight after the decimal point. So $\frac{2}{7}$ is purely periodic but $\frac{1}{12}$ and $\frac{1}{2}$ are not. Now, the answer is that a fraction $\frac{a}{b}$ (with $a \perp b$) is purely periodic if and only if $b \perp 10$ (in other words, $2 \nmid b$ and $5 \nmid b$). This can be proven using Theorem 2.15.3.

Theorem 2.15.5 (Pigeonhole Principle for Injections)**.** Let A and B be two finite sets such that $|A| \geq |B|$. Let $f : A \to B$ be an injective map. Then, f is bijective.

Theorem 2.15.6 (Pigeonhole Principle for Surjections)**.** Let A and B be two finite sets such that $|A| \leq |B|$. Let $f : A \to B$ be an surjective map. Then, f is bijective.

Theorem 2.15.5 is called the *Pigeonhole Principle for Injections*, due to the following interpretation: If a pigeons sit in b pigeonholes with $a \geq b$ (that is, there are at least as many pigeons as there are pigeonholes), and if no two pigeons are sharing the same hole, then every hole must have at least one pigeon in it. (This corresponds to the statement of Theorem 2.15.5 if you let A be the set of pigeons, B be the set of holes, and f be the map that sends each pigeon to the hole it is sitting in. The injectivity of f is then precisely the statement that no two pigeons are sharing the same hole.)

Likewise, Theorem 2.15.6 is called the *Pigeonhole Principle for Surjections*, due to the following interpretation: If a pigeons sit in b pigeonholes with $a \leq b$ (that is, there are at most as many pigeons as there are pigeonholes), and if each hole contains at least one pigeon, then no two pigeons are sharing the same hole.

Theorem 2.15.5 and Theorem 2.15.6 are both basic facts of set theory; how to prove them depends on how you define the size of a finite set in the first place. See [Grinbe15, solution to Exercise 1.1] for one way of proving them (more precisely, Theorem 2.15.5 is the "$\Longrightarrow$" direction of [Grinbe15, Lemma 1.5], while Theorem 2.15.6 is the "$\Longrightarrow$" direction of [Grinbe15, Lemma 1.4]).

Now, Theorem 2.15.5 can be used to simplify our above proof of Theorem 2.15.3. Indeed, in the latter proof, once we have shown that f is injective, we can immediately apply Theorem 2.15.5 (to $A = C$ and $B = C$) in order to conclude that f is bijective (since C is a finite set and satisfies $|C| \geq |C|$). The proof of surjectivity of f is thus unnecessary. Alternatively, we could have omitted the proof of injectivity of f, and instead used the surjectivity of f to apply Theorem 2.15.6 (to $A = C$ and $B = C$) in order to conclude that f is bijective (since C is a finite set and satisfies $|C| \leq |C|$). Either way, we would have obtained a shorter proof.

2.15.4. Wilson

The next theorem is known as *Wilson's theorem*:

Theorem 2.15.7. Let p be a prime. Then, $(p-1)! \equiv -1 \bmod p$.

We shall prove Theorem 2.15.7 using modular inverses modulo p. The main idea is that we can "pair up" each factor in the product $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ with its modular inverse modulo p, where of course we take the unique modular inverse that belongs to the set $\{1, 2, \ldots, p-1\}$. This relies on the following lemma:

Lemma 2.15.8. Let p be a prime. Set $A = \{1, 2, \ldots, p-1\}$.

(a) If a_1 and a_2 are two elements of A satisfying $a_1 \equiv a_2 \bmod p$, then $a_1 = a_2$.

(b) For each $a \in A$, there exists a unique $a' \in A$ satisfying $aa' \equiv 1 \bmod p$.

(c) Define a map $J : A \to A$ as follows: For each $a \in A$, we let $J(a)$ denote the unique $a' \in A$ satisfying $aa' \equiv 1 \bmod p$. (This unique a' indeed exists, by Lemma 2.15.8 **(b)**.)

Then, this map J is a bijection satisfying $J \circ J = \mathrm{id}$.

Remark 2.15.9. Let S be a set. An *involution* on S means a map $f : S \to S$ satisfying $f \circ f = \mathrm{id}$. Thus, Lemma 2.15.8 **(c)** says that the map $J : A \to A$ defined in this lemma is an involution on A.

We are now ready to prove Theorem 2.15.7:
Later, in Section 3.5, we shall give a different version of this proof.
Theorem 2.15.7 has a converse:

Exercise 2.15.3. If an integer $p > 1$ satisfies $(p-1)! \equiv -1 \bmod p$, then prove that p is a prime.

(This is actually easier to prove than Theorem 2.15.7 itself.)

Exercise 2.15.4. Let p be a prime. Prove that

$$(p-1)! \equiv p - 1 \bmod 1 + 2 + \cdots + (p-1).$$

Exercise 2.15.5. Let p be an odd prime. Write p in the form $p = 2k+1$ for some $k \in \mathbb{N}$. Prove that $k!^2 \equiv -(-1)^k \bmod p$.

[**Hint:** Each $j \in \mathbb{Z}$ satisfies $j(p-j) \equiv -j^2 \bmod p$.]

2.16. The Chinese Remainder Theorem as a bijection

2.16.1. The bijection $K_{m,n}$

Here comes another of the many facts known as the "Chinese Remainder Theorem":

Theorem 2.16.1. Let m and n be two coprime positive integers. Then, the map

$$K_{m,n} : \{0, 1, \ldots, mn-1\} \to \{0, 1, \ldots, m-1\} \times \{0, 1, \ldots, n-1\},$$
$$a \mapsto (a\%m, a\%n)$$

is well-defined and is a bijection.

Example 2.16.2. (a) Theorem 2.16.1 (applied to $m = 3$ and $n = 2$) says that the map

$$K_{3,2} : \{0,1,2,3,4,5\} \to \{0,1,2\} \times \{0,1\}, \\ a \mapsto (a\%3, a\%2)$$

is a bijection. This map sends

$$\begin{array}{cccccc} 0, & 1, & 2, & 3, & 4, & 5 \\ (0,0), & (1,1), & (2,0), & (0,1), & (1,0), & (2,1), \end{array} \quad \text{to}$$

respectively (since $0\%3 = 0$ and $0\%2 = 0$ and $1\%3 = 1$ and $1\%2 = 1$ and $2\%3 = 2$ and $2\%2 = 0$ and so on). This list of values shows that this map is bijective (since it takes on every possible value in $\{0,1,2\} \times \{0,1\}$ exactly once). Theorem 2.16.1 says that this holds for arbitrary coprime m and n.

(b) Let us see how Theorem 2.16.1 fails when m and n are **not** coprime. For example, take $m = 6$ and $n = 4$. Then, the map

$$K_{6,4} : \{0,1,\ldots,23\} \to \{0,1,2,3,4,5\} \times \{0,1,2,3\}, \\ a \mapsto (a\%6, a\%4)$$

is **not** a bijection. Indeed, it is neither injective (for example, it sends both 0 and 12 to the same pair $(0,0)$) nor surjective (for example, it never takes the value $(1,2)$).

2.16.2. Coprime remainders

For the rest of this section, we shall use the following notation:

Definition 2.16.3. Let n be a positive integer. Then, let C_n be the subset $\{i \in \{0,1,\ldots,n-1\} \mid i \perp n\}$ of $\{0,1,\ldots,n-1\}$.

For instance,

$$C_4 = \{1,3\}, \qquad C_5 = \{1,2,3,4\}, \qquad C_6 = \{1,5\} \qquad \text{and} \qquad C_1 = \{0\}.$$

Now, we claim the following:

Proposition 2.16.4. Let m and n be two coprime positive integers. Consider the map $K_{m,n}$ defined in Theorem 2.16.1. Then,

$$K_{m,n}(C_{mn}) = C_m \times C_n.$$

(Here, $K_{m,n}(C_{mn})$ denotes the image of the subset C_{mn} of $\{0,1,\ldots,mn-1\}$ under the map $K_{m,n}$; that is, $K_{m,n}(C_{mn}) = \{K_{m,n}(x) \mid x \in C_{mn}\}$.)

Example 2.16.5. Theorem 2.16.1 (applied to $m = 3$ and $n = 5$) says that the map

$$K_{3,5} : \{0,1,\ldots,14\} \to \{0,1,2\} \times \{0,1,2,3,4\}, \\ a \mapsto (a\%3, a\%5)$$

is a bijection. Proposition 2.16.4 (applied to $m = 3$ and $n = 5$) says that this map satisfies $K_{3,5}(C_{15}) = C_3 \times C_5$. In view of

$$C_{15} = \{i \in \{0,1,\ldots,14\} \mid i \perp 15\} = \{1,2,4,7,8,11,13,14\}, \\ C_3 = \{i \in \{0,1,2\} \mid i \perp 3\} = \{1,2\}, \qquad \text{and} \\ C_5 = \{i \in \{0,1,2,3,4\} \mid i \perp 5\} = \{1,2,3,4\},$$

this rewrites as

$$K_{3,5}(\{1,2,4,7,8,11,13,14\}) = \{1,2\} \times \{1,2,3,4\}.$$

And indeed, this can easily be checked: The map $K_{3,5}$ sends

$$\begin{array}{cccccccc} 1, & 2, & 4, & 7, & 8, & 11, & 13, & 14, \quad \text{to} \\ (1,1), & (2,2), & (1,4), & (1,2), & (2,3), & (2,1), & (1,3) & (2,4), \end{array}$$

respectively, which entails

$$K_{3,5}(\{1,2,4,7,8,11,13,14\}) \\ = \{(1,1),(2,2),(1,4),(1,2),(2,3),(2,1),(1,3),(2,4)\} = \{1,2\} \times \{1,2,3,4\}.$$

2.16.3. Proving the formula for ϕ

We now can prove Theorem 2.14.4:

We now take aim at proving Theorem 2.14.5. First, let us extend Theorem 2.14.4 to products of k mutually coprime integers:

Exercise 2.16.1. Let $n_1, n_2, \ldots, n_k$ be mutually coprime positive integers. Prove that $\phi(n_1 n_2 \cdots n_k) = \phi(n_1) \cdot \phi(n_2) \cdot \cdots \cdot \phi(n_k)$.

Exercise 2.16.2. Let I be a finite set. For each $i \in I$, let n_i be a positive integer. Assume that

$$\text{every two distinct elements } i \text{ and } j \text{ of } I \text{ satisfy } n_i \perp n_j. \tag{29}$$

Prove that

$$\phi\left(\prod_{i \in I} n_i\right) = \prod_{i \in I} \phi(n_i).$$

We are finally ready to prove Theorem 2.14.5:

Theorem 2.15.3 generalizes Theorem 2.15.1 **(a)**. Likewise, the following exercise generalizes Theorem 2.15.1 **(b)**:

Exercise 2.16.3. Let a be an integer, and let n be a positive integer. Prove that $a^n \equiv a^{n-\phi(n)} \bmod n$.

[**Hint:** Use Exercises 2.13.9 and 2.14.2 and Theorems 2.15.3 and 2.14.4.]

2.17. Binomial coefficients

2.17.1. Definitions and basics

Next, we shall introduce and briefly study binomial coefficients. While binomial coefficients belong more to (enumerative) combinatorics than to algebra, they are used significantly in algebra, so we have to derive some of their properties.

Here is the definition of binomial coefficients (at least the one I am going to follow in these notes):

Definition 2.17.1. Let $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$. Then, we define the *binomial coefficient* $\binom{n}{k}$ as follows:

(a) If $k \in \mathbb{N}$, then we set

$$\binom{n}{k} = \frac{n\left(n-1\right)\left(n-2\right)\cdots\left(n-k+1\right)}{k!} = \frac{\prod_{i=0}^{k-1}\left(n-i\right)}{k!}.$$

(b) If $k \notin \mathbb{N}$, then we set $\binom{n}{k} = 0$.

This definition is exactly the definition of $\binom{n}{k}$ that we used in homework set #0. It is also almost exactly the definition given in [GrKnPa94, (5.1)] (except that we are allowing k to be non-integer, while the authors of [GrKnPa94] do not). Definition 2.17.1 **(a)** is also identical with the definition of binomial coefficients in [Grinbe15]. Our choice to require $n \in \mathbb{Q}$ is more or less arbitrary – we could have as well made the same definition for $n \in \mathbb{R}$ or $n \in \mathbb{C}$ (but I am not aware of this generality being of much use).

Generally, when you read literature on binomial coefficients, be aware that some authors use somewhat different definitions of $\binom{n}{k}$. All known definitions give the same results when n and k are nonnegative integers, but in the other cases there may be discrepancies.

Here are some examples of binomial coefficients:

Example 2.17.2. **(a)** Definition 2.17.1 **(a)** yields $\binom{n}{2} = \frac{n(n-1)}{2!} = \frac{n(n-1)}{2}$ for all $n \in \mathbb{Q}$. Thus, for example,

$$\binom{5}{2} = \frac{5 \cdot 4}{2} = 10.$$

(b) Definition 2.17.1 **(a)** yields $\binom{n}{3} = \frac{n(n-1)(n-2)}{3!} = \frac{n(n-1)(n-2)}{6}$ for all $n \in \mathbb{Q}$. Thus, for example,

$$\begin{aligned}
\binom{5}{3} &= \frac{5 \cdot 4 \cdot 3}{6} = \frac{60}{6} = 10; \\
\binom{1}{3} &= \frac{1 \cdot 0 \cdot (-1)}{6} = \frac{0}{6} = 0; \\
\binom{-2}{3} &= \frac{(-2) \cdot (-3) \cdot (-4)}{6} = \frac{-24}{6} = -4; \\
\binom{1/2}{3} &= \frac{(1/2) \cdot (-1/2) \cdot (-3/2)}{6} = \frac{3/8}{6} = \frac{1}{16}.
\end{aligned}$$

(c) Definition 2.17.1 **(a)** yields $\binom{n}{1} = \frac{n}{1!} = \frac{n}{1} = n$ for all $n \in \mathbb{Q}$.

(d) Definition 2.17.1 **(b)** yields $\binom{4}{1/2} = 0$ (since $1/2 \notin \mathbb{N}$).

The binomial coefficients $\binom{n}{k}$ for $n \in \mathbb{N}$ and $k \in \{0, 1, \ldots, n\}$ are particularly important. They are usually tabulated in a triangle-shaped table known as *Pascal's triangle*, which starts as follows:

$$\begin{array}{ccccccccccccccccccc}
 & & & & & & & 1 & & & & & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & & & & & \\
 & & & & & 1 & & 2 & & 1 & & & & & & & & & \\
 & & & & 1 & & 3 & & 3 & & 1 & & & & & & & & \\
 & & & 1 & & 4 & & 6 & & 4 & & 1 & & & & & & & \\
 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & & & & & \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & & & & & \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 & & & & \\
 & & & & & & & & & & & & & & & & & & \ddots
\end{array}.$$

In this table, the binomial coefficient $\binom{n}{k}$ appears as the k-th entry (from the left) of the n-th row (but we count the rows from 0; that is, the topmost row, consisting just of a single "1", is actually the 0-th row). We advise the reader to peruse the Wikipedia article for the history and the multiple illustrious properties of Pascal's triangle.

The expression $\binom{n}{k}$ is pronounced as "n choose k". The reason for the word "choose" will become clearer once we have seen Theorem 2.17.10 further below.

Some of these properties are so fundamental that we are going to list them right now:

Theorem 2.17.3. Let $n \in \mathbb{N}$ and $k \in \mathbb{N}$ be such that $n \geq k$. Then,

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Several authors use the formula $\binom{n}{k} = \frac{n!}{k!\,(n-k)!}$ as a definition of the binomial coefficients. However, this definition has the massive disadvantage of being less general than Definition 2.17.1 (since it only covers the case when $n, k \in \mathbb{N}$ and $n \geq k$). To us, this formula is not a definition, but a result that can be proven.

Theorem 2.17.4. Let $n \in \mathbb{N}$ and $k \in \mathbb{Q}$ be such that $k > n$. Then,

$$\binom{n}{k} = 0.$$

Theorem 2.17.5. Let $n \in \mathbb{Q}$. Then,

$$\binom{n}{0} = 1.$$

Theorem 2.17.6. Let $n \in \mathbb{N}$ and $k \in \mathbb{Q}$. Then,

$$\binom{n}{k} = \binom{n}{n-k}.$$

Theorem 2.17.6 is known as the *symmetry of binomial coefficients*. Note that it fails if $n \notin \mathbb{N}$; thus, be careful when applying it!

Theorem 2.17.7. Let $n \in \mathbb{Q}$ and $k \in \mathbb{Z}$. Then,

$$\binom{-n}{k} = (-1)^k \binom{k+n-1}{k}.$$

Theorem 2.17.7 is one of the versions of the *upper negation formula*.

Theorem 2.17.8. Any $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$ satisfy

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Theorem 2.17.8 is known as the *recurrence of the binomial coefficients*, and is the reason why each entry of Pascal's triangle is the sum of the two entries above it[20].

Theorem 2.17.9. Any $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$ satisfy

$$k\binom{n}{k} = n\binom{n-1}{k-1}.$$

2.17.2. Combinatorial interpretation

The next property of binomial coefficients is one of the major motivations for defining them:

Theorem 2.17.10. Let $n \in \mathbb{N}$ and $k \in \mathbb{Q}$. Let N be an n-element set. Then, $\binom{n}{k}$ is the number of k-element subsets of N.

We shall refer to Theorem 2.17.10 as the *Combinatorial interpretation of binomial coefficients*. Theorem 2.17.10 can be restated as "$\binom{n}{k}$ is the number of ways to choose k elements (with no repetitions and with no regard for the order) from a given n-element set (when $n \in \mathbb{N}$)". This is the reason why $\binom{n}{k}$ is called "n choose k". Note, however, that Theorem 2.17.10 does not directly help us compute $\binom{n}{k}$ when $n \notin \mathbb{N}$.

Corollary 2.17.11. Let $n \in \mathbb{N}$ and $k \in \mathbb{Q}$. Then, $\binom{n}{k}$ is a nonnegative integer.

Proposition 2.17.12. Let $n \in \mathbb{Z}$ and $k \in \mathbb{Q}$. Then, $\binom{n}{k}$ is a integer.

[20] Of course, this does not apply to the "1" at the apex of Pascal's triangle (unless we extend the triangle further to the top by a (-1)-st row).

Exercise 2.17.1. Let $k \in \mathbb{N}$. Prove that the product of any k consecutive integers is divisible by $k!$.

Exercise 2.17.2. In this exercise, we shall use the *Iverson bracket notation*: If $\mathcal{A}$ is any statement, then $[\mathcal{A}]$ stands for the integer $\begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false} \end{cases}$ (which is also known as the *truth value* of $\mathcal{A}$). For instance, $[1+1=2] = 1$ and $[1+1=1] = 0$.

(a) Prove that $n//k = \sum_{i=1}^{n} [k \mid i]$ for any $n \in \mathbb{N}$ and any positive integer k.

(b) Prove that $v_p(n) = \sum_{i \geq 1} \left[p^i \mid n\right]$ for any prime p and any nonzero integer n.

Here, the sum $\sum_{i \geq 1} \left[p^i \mid n\right]$ is a sum over all positive integers; but it is well-defined, since it has only finitely many nonzero addends.

(c) Prove that $v_p(n!) = \sum_{i \geq 1} n//p^i$ for any prime p and any $n \in \mathbb{N}$. (Here, the expression "$\sum_{i \geq 1} n//p^i$" should be understood as $\sum_{i \geq 1} \left(n//p^i\right)$. Again, this sum $\sum_{i \geq 1} \left(n//p^i\right)$ is well-defined, since it has only finitely many nonzero addends.)

(d) Use part **(c)** to prove Corollary 2.17.11 again.

The claim of Exercise 2.17.2 **(c)** is usually rewritten in the form $v_p(n!) = \sum_{i \geq 1} \left\lfloor \dfrac{n}{p^i} \right\rfloor$ (which is equivalent, because of Proposition 2.8.3); in this form, it is known as Legendre's formula or as de Polignac's formula (see, e.g., [Grinbe16, Theorem 1.3.3]). It is often a helpful tool in proving divisibility properties of factorials and binomial coefficients. One application, for example, is to quickly compute how many zeroes the decimal expansion of $n!$ ends with. (Note that Exercise 2.17.2 **(b)** can be rewritten as $v_p(n) = \sum_{\substack{i \geq 1; \\ p^i \mid n}} 1$; in this form it appears in [Grinbe16, Lemma 1.3.4].)

2.17.3. Binomial formula and Vandermonde convolution

One of the staples of enumerative combinatorics are identities that involve binomial coefficients. Hundreds of such identities have been found (see, e.g., Henry W. Gould's website for a list of some of them; see also [GrKnPa94, Chapter 5] and [Grinbe15, Chapter 3] for introductions). At this point, let us only show two of the most important ones (not counting the ones we have already shown above). Probably the most famous one is the *binomial formula*:

Theorem 2.17.13. Let x, y be any numbers (e.g., rational or real or complex numbers). Let $n \in \mathbb{N}$. Then,

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}.$$

Theorem 2.17.13 is known as the *binomial formula* or the *binomial theorem*. It generalizes the well-known and beloved identities

$$(x+y)^2 = x^2 + 2xy + y^2;$$
$$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3;$$
$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

(as well as $(x+y)^1 = x^1 + y^1$ and $(x+y)^0 = 1$, of course).

The next identity we want to show is the *Vandermonde convolution identity*:

Theorem 2.17.14. Let $x, y \in \mathbb{Q}$ and $n \in \mathbb{N}$. Then,

$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k}.$$

For example, for $n = 2$, Theorem 2.17.14 says that

$$\binom{x+y}{2} = \underbrace{\binom{x}{0}}_{=1}\binom{y}{2} + \underbrace{\binom{x}{1}}_{=x}\underbrace{\binom{y}{1}}_{=y} + \binom{x}{2}\underbrace{\binom{y}{0}}_{=1} = \binom{y}{2} + xy + \binom{x}{2}.$$

The proof of Theorem 2.17.14 that we are soon going to sketch is similar to the one given in [Grinbe15, §3.3.3] (but, unlike the latter proof, we will use polynomials in 1 variable only). It will not be a complete proof, since it will rely on some properties of polynomials, and not only have we not proven these properties – we have actually not rigorously defined polynomials yet! (We will do so later, in Chapter 7.) See [Grinbe15, §3.3.2] for another (more boring and tedious, but conceptually simpler) proof of Theorem 2.17.14.

Our proof of Theorem 2.17.14 proceeds via several intermediate steps. The first one is to prove Theorem 2.17.14 in the particular case when $x, y \in \mathbb{N}$:

Lemma 2.17.15. Let $a, b \in \mathbb{N}$ and $n \in \mathbb{N}$. Then,

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k}\binom{b}{n-k}.$$

(We have renamed the variables x and y from Theorem 2.17.14 as a and b here, since we will soon use the letter "x" for something completely different.)

This shows that Theorem 2.17.14 holds for all $x \in \mathbb{N}$ and $y \in \mathbb{N}$. In order to extend its reach to arbitrary rational a and b, we shall use the "polynomial identity trick". First, let us briefly explain what polynomials are, without giving a formal definition.

Informally, a *polynomial* (in 1 variable x, with rational coefficients) is an "expression" of the form $a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$, where $a_k, a_{k-1}, \ldots, a_0$ are (fixed) rational numbers and where x is a (so far meaningless) symbol (called *indeterminate* or *variable*). For example, $4x^3 + 2x^2 - \frac{1}{3}x + \frac{2}{7}$ is a polynomial, and so is $0x^3 + x^2 - 0x + \frac{1}{3}$. We can omit terms of the form "$0x^i$" when writing down a polynomial and treat the result as being the same polynomial; thus, $0x^3 + x^2 - 0x + \frac{1}{3}$ can also be written as $x^2 - 0x + \frac{1}{3}$ and as $x^2 + \frac{1}{3}$. Likewise, we can treat the "+" signs as signifying addition and behaving like it, so, e.g., commutativity holds: $2x^3 + 5x$ and $5x + 2x^3$ are the same polynomial (but $2x + 5x^3$ is different). We also pretend that distributivity holds, so "like terms" can be combined: e.g., we have $4x^3 + 9x^3 = (4+9)\,x^3 = 13x^3$ or $4x^3 - 12x^3 = (4-12)\,x^3 = -8x^3$. Thus, we can add two polynomials: for example,

$$\left(3x^2 - 1x + \frac{1}{2}\right) + (6x - 7) = 3x^2 + \underbrace{(-1+6)}_{=5} x + \underbrace{\left(\frac{1}{2} - 7\right)}_{=\frac{-13}{2}} = 3x^2 + 5x + \frac{-13}{2}.$$

By pretending that the x^i (with $i \in \mathbb{N}$) are actual powers of the symbol x, and that multiplication obeys the associativity law (so that $\left(\lambda x^i\right) x^j = \lambda \left(x^i x^j\right) = \lambda x^{i+j}$ for rational λ and $i, j \in \mathbb{N}$), we can multiply polynomials as well (first use distributivity to expand the product):

$$\begin{aligned}(3x-5)\left(x^2+3x+2\right) &= 3x\left(x^2+3x+2\right) - 5\left(x^2+3x+2\right) \\ &= \left(3x^3+9x^2+6x\right) - \left(5x^2+15x+10\right) \\ &= 3x^3 + 4x^2 - 9x - 10.\end{aligned}$$

Most importantly, it is possible to *substitute* a number into a polynomial: If $u \in \mathbb{Q}$ and if $P = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ is a polynomial, then we define $P(u)$ (called the *evaluation* of P *at* u, or the *result of substituting* u *for* x *in* P) to be the number $a_k u^k + a_{k-1} u^{k-1} + \cdots + a_0$. More generally, if the polynomial P is given in any of its forms (e.g., as a product of other polynomials), then we can compute $P(u)$ by replacing each x appearing in this form by an u. For example, if $P = (2x+1)(3x+1) - (4x+1)(5x+1)$, then $P(u) = (2u+1)(3u+1) - (4u+1)(5u+1)$; thus, we do not need to expand P before substituting u into it.

Even more generally, u does not have to be a rational number in order to be substituted in a polynomial P – it can be (roughly speaking!) anything that can be taken to the i-th power for $i \in \mathbb{N}$ and that can be added and multiplied by a rational number. For example, u can be a real number or a square matrix or another

polynomial. (We will later learn the precise meaning of "anything" here[21].)

We have been vague in our definition of polynomials, since making it rigorous would take us a fair way afield. But we **will** eventually (in Chapter 7) define polynomials rigorously and prove that all of the above claims (e.g., about associativity and distributivity) actually hold. For now, we need a basic property of polynomials:

Proposition 2.17.16. Let P and Q be two polynomials in 1 variable x with rational coefficients. Assume that infinitely many $u \in \mathbb{Q}$ satisfy $P(u) = Q(u)$. Then, $P = Q$ (as polynomials).

We will prove Proposition 2.17.16 later (in Section 7.7).[22]

Note that polynomials are not functions – despite the fact that we can substitute numbers into them and obtain other numbers. However, in many regards, they behave like functions. For what we are going to do in this section, the difference does not matter; we can treat polynomials as functions here.

With Lemma 2.17.15, we have proven Theorem 2.17.14 in the case when x and y belong to $\mathbb{N}$. Our goal, however, is to prove it for arbitrary $x, y \in \mathbb{Q}$. Let us first lift it to an intermediate level of generality – allowing x to be arbitrary, but still requiring $y \in \mathbb{N}$. Thus, we want to prove the following lemma:

Lemma 2.17.17. Let $a \in \mathbb{Q}$, $b \in \mathbb{N}$ and $n \in \mathbb{N}$. Then,

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}.$$

Let us summarize the main idea of this proof: We replaced the rational number a by the indeterminate x, thus transforming the identity we were proving into an equality between two polynomials (namely, $P = Q$). But in order to prove an equality between polynomials, it suffices to prove that it holds at infinitely many numbers (by Proposition 2.17.16); thus, in particular, it suffices to check it at all nonnegative integers. But this is precisely what we did in Lemma 2.17.15 above. This kind of argument (with its use of Proposition 2.17.16) is known as the "polynomial identity trick".

Now, let us extend the reach of Lemma 2.17.17 further, allowing both a and b to be arbitrary (and thus obtaining the whole Theorem 2.17.14):

Lemma 2.17.18. Let $a, b \in \mathbb{Q}$ and $n \in \mathbb{N}$. Then,

$$\binom{a+b}{n} = \sum_{k=0}^{n} \binom{a}{k} \binom{b}{n-k}.$$

[21] Namely, "anything" will be concretized to mean "any element of a $\mathbb{Q}$-algebra". See Definition 7.6.1 for the details.

[22] Note that it is closely related to the Proposition 1.6.6 we used above.

Exercise 2.17.3. Let $a, b \in \mathbb{N}$ and $m \in \mathbb{Q}$. Let A be an a-element set. Let B be a b-element subset of A. Prove that

$$(\text{the number of } m\text{-element subsets } S \text{ of } A \text{ satisfying } B \subseteq S) = \binom{a-b}{m-b}.$$

2.17.4. Some divisibilities and congruences

So far we have been proving identities between binomial coefficients. Let us now step to divisibilities and congruences.

Proposition 2.17.12 shows that binomial coefficients $\binom{n}{k}$ are integers whenever n is an integer. This allows us to study divisibilities and congruences between binomial coefficients (and you have seen a few of them on homework set #1). One of the most important such divisibilities is the following fact:

Theorem 2.17.19. Let p be a prime. Let $k \in \{1, 2, \ldots, p-1\}$. Then, $p \mid \binom{p}{k}$.

We shall see a second, combinatorial proof of Theorem 2.17.19 further below; it will rely on the concept of group actions.

Let us state two congruences for binomial coefficients, which we will show later using tools from abstract algebra:

Theorem 2.17.20 (Lucas's congruence)**.** Let p be a prime. Let $a, b \in \mathbb{Z}$. Let $c, d \in \{0, 1, \ldots, p-1\}$. Then,

$$\binom{pa+c}{pb+d} \equiv \binom{a}{b}\binom{c}{d} \bmod p.$$

Theorem 2.17.21 (Babbage's congruence)**.** Let p be a prime. Let $a, b \in \mathbb{Z}$. Then,

$$\binom{pa}{pb} \equiv \binom{a}{b} \bmod p^2.$$

For the impatient: Elementary proofs of Theorem 2.17.20 and Theorem 2.17.21 can be found in [Grinbe17].

Remark 2.17.22. Lucas's congruence has the following consequence: Let p be a prime. Let $a, b \in \mathbb{N}$. Write a and b in base p as follows:

$$a = a_k p^k + a_{k-1} p^{k-1} + \cdots + a_0 p^0 \qquad \text{and}$$
$$b = b_k p^k + b_{k-1} p^{k-1} + \cdots + b_0 p^0$$

with $k \in \mathbb{N}$ and $a_k, a_{k-1}, \ldots, a_0, b_k, b_{k-1}, \ldots, b_0 \in \{0, 1, \ldots, p-1\}$. (Note that we allow "leading zeroes" – i.e., any of a_k and b_k can be 0.) Then,

$$\binom{a}{b} \equiv \binom{a_k}{b_k}\binom{a_{k-1}}{b_{k-1}} \cdots \binom{a_0}{b_0} \bmod p.$$

(This can be easily proven by induction on k, using Theorem 2.17.20 in the induction step.) This allows for quick computation of remainders of $\binom{a}{b}$ modulo prime numbers, and also explains (when applied to $p = 2$) why we can obtain (an approximation of) Sierpinski's triangle from Pascal's triangle by coloring all even numbers white and all odd numbers black.

See [Mestro14] and [Granvi05] for overviews of more complicated divisibilities and congruences for binomial coefficients.

Exercise 2.17.4. Let p be a prime.

(a) Prove that $\binom{2p}{p} \equiv 2 \bmod p$.

(b) Prove that $\binom{2p-1}{p} \equiv 1 \bmod p$.

(c) Prove that $\binom{p-1+k}{k} \equiv 0 \bmod p$ for each $k \in \{1, 2, \ldots, p-1\}$.

[**Hint:** This is very easy using Lucas's congruence, but you can also solve it without it.]

2.17.5. Integer-valued polynomials

Now that we have introduced polynomials (albeit informally and on somewhat shaky foundations) and binomial coefficients (albeit briefly), it would be a shame to leave unmentioned a subject that connects the two particularly closely: the *integer-valued polynomials*. We are going to state a few basic facts, but we will not prove them.

If $f = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ is a polynomial (in 1 variable x, with rational coefficients), then the rational numbers $a_k, a_{k-1}, \ldots, a_0$ are called the *coefficients* of f. The coefficients of a polynomial f are uniquely determined by f (except for the fact that we can always add terms of the form $0x^\ell$ and thus obtain extra coefficients that are equal to 0). (This fact is not obvious, given our "definition" of polynomials above[23]. We will later define polynomials more formally as sequences of coefficients; then this will become clear.)

[23] For example, why cannot we start with (say) $6x^2 + 5x + 4$, then rewrite it as $(2x+1)(3x+1) + 3$, then do some other transformations (using commutativity, associativity and other laws), and finally end up with a polynomial that has different coefficients (say, $3x^2 + 9x + 4$) ? We cannot, but it is not easy to prove with what we have.

If $f = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ is a polynomial (in 1 variable x, with rational coefficients) such that $a_k \neq 0$ (each polynomial that is not just 0 can be uniquely written in such a form), then the integer k is called the *degree* of f.

Definition 2.17.23. A polynomial P with rational coefficients is said to be *integer-valued* if ($P(n) \in \mathbb{Z}$ for all $n \in \mathbb{Z}$).

Of course, a polynomial with integer coefficients is always integer-valued. But there are other integer-valued polynomials, too:

Example 2.17.24. (a) The polynomial $\binom{x}{2} = \dfrac{x(x-1)}{2} = \dfrac{1}{2}x^2 - \dfrac{1}{2}x$ is integer-valued (since $\binom{n}{2} \in \mathbb{Z}$ for each $n \in \mathbb{Z}$), but its coefficients are $\dfrac{1}{2}, -\dfrac{1}{2}, 0$.

(b) More generally: If $k \in \mathbb{N}$ is arbitrary, then the polynomial $\binom{x}{k} = \dfrac{x(x-1)(x-2)\cdots(x-k+1)}{k!}$ is integer-valued (since $\binom{n}{k} \in \mathbb{Z}$ for each $n \in \mathbb{Z}$).

(c) If p is any prime, then the polynomial $\dfrac{x^p - x}{p}$ is integer-valued (since Theorem 2.15.1 **(b)** yields $a^p \equiv a \bmod p$ for each $a \in \mathbb{Z}$, which means that $\dfrac{a^p - a}{p} \in \mathbb{Z}$ for each $a \in \mathbb{Z}$). Its coefficients are not integers.

This suggests the following question**:** How can we describe the integer-valued polynomials? The following result of Pólya [Polya19] gives an answer:

Theorem 2.17.25. Let $k \in \mathbb{N}$.

(a) Any polynomial P (in 1 variable x, with rational coefficients) of degree k can be uniquely written in the form

$$P(x) = a_k \binom{x}{k} + a_{k-1} \binom{x}{k-1} + \cdots + a_0 \binom{x}{0}$$

with **rational** $a_k, a_{k-1}, \ldots, a_0$.

(b) The polynomial P is integer-valued if and only if these $a_k, a_{k-1}, \ldots, a_0$ are integers.

For example, the integer-valued polynomial $\dfrac{x^3 - x}{3}$ can be written as

$$\frac{x^3 - x}{3} = a_3 \binom{x}{3} + a_2 \binom{x}{2} + a_1 \binom{x}{1} + a_0 \binom{x}{0}$$

for

$$a_3 = 2, \qquad a_2 = 2, \qquad a_1 = 0, \qquad a_0 = 0.$$

These a_3, a_2, a_1, a_0 are integers – exactly as Theorem 2.17.25 **(b)** says.

I sketched a proof of Theorem 2.17.25 **(b)** in a talk in 2013 (`https://www.cip.ifi.lmu.de/~grinberg/storrs2013.pdf`)[24]. See also [daSilv12] for a self-contained proof.

2.18. Counting divisors

2.18.1. The number of divisors of n

Now that we have seen some combinatorial reasoning (e.g., in the proof of Theorem 2.17.14), let us solve a rather natural counting problem: Let us count the divisors of a nonzero integer n.

Proposition 2.18.1. Let $n \in \mathbb{Z}$ be nonzero. Then:

(a) The product $\prod_{p \text{ prime}} \left(v_p\left(n\right)+1\right)$ is well-defined, since all but finitely many of its factors are 1.

(b) We have

$$\left(\text{the number of positive divisors of } n\right) = \prod_{p \text{ prime}} \left(v_p\left(n\right)+1\right).$$

(c) We have

$$\left(\text{the number of divisors of } n\right) = 2 \prod_{p \text{ prime}} \left(v_p\left(n\right)+1\right).$$

Example 2.18.2. If $n = 12$, then

$$\left(\text{the number of positive divisors of } n\right) = 6$$

(since the positive divisors of $n = 12$ are $1, 2, 3, 4, 6, 12$) and

$$\begin{aligned}\prod_{p \text{ prime}} \left(v_p\left(n\right)+1\right) &= \left(\underbrace{v_2\left(n\right)}_{=2}+1\right)\left(\underbrace{v_3\left(n\right)}_{=1}+1\right) \prod_{\substack{p \text{ prime;} \\ p \notin \{2,3\}}} \left(\underbrace{v_p\left(n\right)}_{=0}+1\right) \\ &= \left(2+1\right)\left(1+1\right) \underbrace{\prod_{\substack{p \text{ prime;} \\ p \notin \{2,3\}}} 1}_{=1} = \left(2+1\right)\left(1+1\right) = 6.\end{aligned}$$

This confirms Proposition 2.18.1 **(b)** for $n = 12$. In order to confirm Proposition 2.18.1 **(c)** for $n = 12$ as well, we observe that $\left(\text{the number of divisors of } n\right) = 12$ (since the divisors of $n = 12$ are $-12, -6, -4, -3, -2, -1, 1, 2, 3, 4, 6, 12$).

[24] In this talk, I refer to integer-valued polynomials as "integral-valued polynomials".

The function

$$\{1,2,3,\ldots\} \to \mathbb{N},$$
$$n \mapsto (\text{the number of positive divisors of } n)$$

is known as the *divisor function* and is commonly denoted by τ. So Proposition 2.18.1 **(b)** gives a formula for $\tau(n)$. See [Grinbe16, Theorem 2.1.7 (proof sketched in §2.7)] for a different proof of this formula.

Our proof of Proposition 2.18.1 will rely on the following lemma, which classifies all divisors of a positive integer in terms of its prime factorization:

Lemma 2.18.3. Let $p_1, p_2, \ldots, p_u$ be finitely many distinct primes. For each $i \in \{1,2,\ldots,u\}$, let a_i be a nonnegative integer. Let $n = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}$.

Define a set T by

$$\begin{aligned} T &= \{0,1,\ldots,a_1\} \times \{0,1,\ldots,a_2\} \times \cdots \times \{0,1,\ldots,a_u\} \\ &= \{(b_1,b_2,\ldots,b_u) \mid b_i \in \{0,1,\ldots,a_i\} \text{ for each } i \in \{1,2,\ldots,u\}\} \\ &= \{(b_1,b_2,\ldots,b_u) \in \mathbb{N}^u \mid b_i \leq a_i \text{ for each } i \in \{1,2,\ldots,u\}\}. \end{aligned}$$

Then, the map

$$\begin{aligned} \Lambda : T &\to \{\text{positive divisors of } n\}, \\ (b_1,b_2,\ldots,b_u) &\mapsto p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u} \end{aligned}$$

is well-defined and bijective.

Example 2.18.4. For this example, let $u = 2$, $p_1 = 2$, $p_2 = 3$, $a_1 = 2$ and $a_2 = 1$. Define the integer n and the set T as in Lemma 2.18.3; then,

$$n = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u} = 2^2 \cdot 3^1 = 12$$

and

$$\begin{aligned} T &= \{0,1,\ldots,a_1\} \times \{0,1,\ldots,a_2\} \times \cdots \times \{0,1,\ldots,a_u\} = \{0,1,2\} \times \{0,1\} \\ &= \{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1)\}. \end{aligned}$$

Now, Lemma 2.18.3 says that the map

$$\begin{aligned} \Lambda : T &\to \{\text{positive divisors of } n\}, \\ (b_1,b_2,\ldots,b_u) &\mapsto p_1^{b_1} p_2^{b_2} \cdots p_u^{b_u} \end{aligned}$$

is well-defined and bijective. Here is a table of values of this map Λ:

$\mathbf{b}$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$
$\Lambda(\mathbf{b})$	1	3	2	6	4	12

.

Remark 2.18.5. Proposition 2.18.1 can be used to re-prove Proposition 2.14.7. We leave the details of this argument to the reader.

2.18.2. The sum of the divisors of n

The method by which we proved Proposition 2.18.1 can be used (with a minor modification) to not just count the positive divisors of a positive integer n, but also (for example) to compute their sum or the sum of their squares. This relies on the following basic property of $\sum$ and $\prod$ signs:

Lemma 2.18.6. Let $n \in \mathbb{N}$. For every $i \in \{1, 2, \ldots, n\}$, let Z_i be a finite set. For every $i \in \{1, 2, \ldots, n\}$ and every $k \in Z_i$, let $p_{i,k}$ be a number. Then,

$$\prod_{i=1}^{n} \sum_{k \in Z_i} p_{i,k} = \sum_{(k_1, k_2, \ldots, k_n) \in Z_1 \times Z_2 \times \cdots \times Z_n} \prod_{i=1}^{n} p_{i,k_i}.$$

(Note that if $n = 0$, then the Cartesian product $Z_1 \times Z_2 \times \cdots \times Z_n$ has no factors; it is what is called an *empty Cartesian product*. It is understood to be a 1-element set, and its single element is the 0-tuple $()$ (also known as the empty list).)

Lemma 2.18.6 is essentially a version of the distributivity law (or the FOIL method) for expanding a product of several sums, each of which has several factors. For example, if we take $n = 3$ and $Z_i = \{1, 2\}$ for each $i \in \{1, 2, 3\}$, then Lemma 2.18.6 says that

$$\begin{aligned}
&(p_{1,1} + p_{1,2})(p_{2,1} + p_{2,2})(p_{3,1} + p_{3,2}) \\
&= p_{1,1}p_{2,1}p_{3,1} + p_{1,1}p_{2,1}p_{3,2} + p_{1,1}p_{2,2}p_{3,1} + p_{1,1}p_{2,2}p_{3,2} \\
&\qquad + p_{1,2}p_{2,1}p_{3,1} + p_{1,2}p_{2,1}p_{3,2} + p_{1,2}p_{2,2}p_{3,1} + p_{1,2}p_{2,2}p_{3,2}
\end{aligned}$$

(which is precisely what you get if you expand the product $(p_{1,1} + p_{1,2})(p_{2,1} + p_{2,2})(p_{3,1} + p_{3,2})$ using the distributivity law). For another example, if we take $n = 2$ and $Z_i = \{1, 2, 3\}$ for each $i \in \{1, 2\}$, then Lemma 2.18.6 says that

$$\begin{aligned}
(p_{1,1} + p_{1,2} + p_{1,3})(p_{2,1} + p_{2,2} + p_{2,3}) = {} & p_{1,1}p_{2,1} + p_{1,1}p_{2,2} + p_{1,1}p_{2,3} \\
& + p_{1,2}p_{2,1} + p_{1,2}p_{2,2} + p_{1,2}p_{2,3} \\
& + p_{1,3}p_{2,1} + p_{1,3}p_{2,2} + p_{1,3}p_{2,3}
\end{aligned}$$

(which is, again, simply the result of expanding the left hand side). In the general

case, the idea behind Lemma 2.18.6 is that if you expand the product[25]

$$\begin{aligned}&\prod_{i=1}^{n}\sum_{k=1}^{m_i} p_{i,k}\\ &= \prod_{i=1}^{n}\left(p_{i,1}+p_{i,2}+\cdots+p_{i,m_i}\right)\\ &= \left(p_{1,1}+p_{1,2}+\cdots+p_{1,m_1}\right)\left(p_{2,1}+p_{2,2}+\cdots+p_{2,m_2}\right)\cdots\left(p_{n,1}+p_{n,2}+\cdots+p_{n,m_n}\right),\end{aligned}$$

then you get a sum of $m_1 m_2 \cdots m_n$ terms, each of which has the form

$$p_{1,k_1} p_{2,k_2} \cdots p_{n,k_n} = \prod_{i=1}^{n} p_{i,k_i}$$

for some $(k_1, k_2, \ldots, k_n) \in \{1,2,\ldots,m_1\} \times \{1,2,\ldots,m_2\} \times \cdots \times \{1,2,\ldots,m_n\}$. See [Grinbe15, proof of Lemma 7.160] for a rigorous proof of Lemma 2.18.6 (which uses induction and the distributivity law).

Now, we can state a formula for the sum of all positive divisors of a positive integer n, and more generally for the sum of the k-th powers of these positive divisors, where k is a fixed integer:

Exercise 2.18.1. Let n be a positive integer. Let $k \in \mathbb{Z}$. Prove that:

(a) The product $\prod_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(n)\cdot k}\right)$ is well-defined, since all but finitely many of its factors are 1.

(b) We have

$$\sum_{d \mid n} d^k = \prod_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(n)\cdot k}\right).$$

(Recall that the summation sign "$\sum_{d \mid n}$" means a sum over all **positive** divisors d of n.)

Example 2.18.7. If $n = 6$, then the positive divisors of n are $1, 2, 3, 6$. Thus, in this case, the claim of Exercise 2.18.1 **(b)** becomes

$$1^k + 2^k + 3^k + 6^k = \prod_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(6)\cdot k}\right).$$

[25] We are here assuming (for the sake of simplicity) that each set Z_i is $\{1,2,\ldots,m_i\}$ for some $m_i \in \mathbb{N}$. This does not weaken the reach of Lemma 2.18.6, since each finite set Z_i can be relabelled as $\{1,2,\ldots,m_i\}$ for $m_i = |Z_i|$.

This equality can easily be verified, since the right hand side is

$$\begin{aligned}
&\prod_{p \text{ prime}} \left(p^{0k} + p^{1k} + \cdots + p^{v_p(6)\cdot k}\right) \\
&= \underbrace{\left(2^{0k} + 2^{1k} + \cdots + 2^{v_2(6)\cdot k}\right)}_{\substack{=2^{0k}+2^{1k} \\ (\text{since } v_2(6)=1)}} \cdot \underbrace{\left(3^{0k} + 3^{1k} + \cdots + 3^{v_3(6)\cdot k}\right)}_{\substack{=3^{0k}+3^{1k} \\ (\text{since } v_3(6)=1)}} \\
&\quad \cdot \prod_{\substack{p \text{ prime}; \\ p \notin \{2,3\}}} \underbrace{\left(p^{0k} + p^{1k} + \cdots + p^{v_p(6)\cdot k}\right)}_{\substack{=p^{0k} \\ (\text{since } v_p(6)=0 \text{ (because } p \notin \{2,3\}))}} \\
&= \left(\underbrace{2^{0k}}_{=1} + \underbrace{2^{1k}}_{=2^k}\right) \cdot \left(\underbrace{3^{0k}}_{=1} + \underbrace{3^{1k}}_{=3^k}\right) \cdot \prod_{\substack{p \text{ prime}; \\ p \notin \{2,3\}}} \underbrace{p^{0k}}_{=1} \\
&= \left(1 + 2^k\right) \cdot \left(1 + 3^k\right) = \underbrace{1}_{=1^k} + 2^k + 3^k + \underbrace{2^k \cdot 3^k}_{=(2\cdot 3)^k = 6^k} = 1^k + 2^k + 3^k + 6^k.
\end{aligned}$$

Note that Proposition 2.18.1 **(b)** is the particular case of Exercise 2.18.1 **(b)** obtained when setting $k = 0$ (because each integer z satisfies $z^0 = 1$, and thus $\sum_{d|n} d^0$ is the number of positive divisors of n).

Exercise 2.18.2. Let n be a positive integer. Let

$$\begin{aligned}
z = &\left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 1 \mod 4\right) \\
&- \left(\text{the number of positive divisors } d \text{ of } n \text{ such that } d \equiv 3 \mod 4\right).
\end{aligned}$$

Prove the following:

(a) If there exists a prime p satisfying $p \equiv 3 \bmod 4$ and $v_p(n) \equiv 1 \bmod 2$, then $z = 0$.

(b) If there exists no prime p satisfying $p \equiv 3 \bmod 4$ and $v_p(n) \equiv 1 \bmod 2$, then

$$z = \prod_{\substack{p \text{ prime}; \\ p \equiv 1 \bmod 4}} \left(v_p(n) + 1\right).$$

[**Hint:** For every $u \in \mathbb{Z}$, set $L(u) = \begin{cases} 1, & \text{if } u\%4 = 1; \\ -1, & \text{if } u\%4 = 3; \\ 0, & \text{otherwise.} \end{cases}$ Prove that $L(uv) = L(u) \cdot L(v)$ for any integers u and v. Then, show that $z = \sum_{d|n} L(d)$. Exploit the similarity between the sum $\sum_{d|n} L(d)$ and the sum in Exercise 2.18.1 **(b)**.]

2.19. "Application": The Erdös–Ginzburg–Ziv theorem

In this section (which can be skipped at will), we shall apply some of what we learned above to prove a curious result found in 1961 by Erdős, Ginzburg and Ziv [ErGiZi61]:

Theorem 2.19.1. Let n be a positive integer. Let $a_1, a_2, \ldots, a_{2n-1}$ be any $2n-1$ integers (not necessarily distinct). Then, there exists an n-element subset S of $\{1, 2, \ldots, 2n-1\}$ such that $n \mid \sum_{s \in S} a_s$.

In other words, this theorem says that if you are given $2n-1$ integers, then you can pick n of them (without picking the same one twice[26]) such that the sum of your pick is divisible by n.

Example 2.19.2. In the case when $n = 2$, Theorem 2.19.1 can be restated as follows: If a, b, c are three integers, then at least one of the sums $b+c$, $c+a$ and $a+b$ is even. This is easy to prove by contradiction: Assume the contrary; thus, all three sums $b+c$, $c+a$ and $a+b$ are odd. Hence, $(b+c)+(c+a)+(a+b)$ is a sum of three odd numbers, and thus itself must be odd (since odd + odd is even, and odd + even is odd). But this contradicts the fact that $(b+c)+(c+a)+(a+b) = 2(a+b+c)$ is even. Thus, we have proven Theorem 2.19.1 in the case when $n = 2$.

Many proofs of Theorem 2.19.1 are known (see [AloDub93] for an exposition), but none of them is overly easy. We shall present one of these proofs (the one in [AloDub93, §2.3]) that uses prime factorization, Fermat's little theorem and binomial coefficients.

First of all, we need a combinatorial lemma, which easily follows from Lemma 2.18.6:

Lemma 2.19.3. Let S be a finite set. For each $s \in S$, let a_s be an integer. Let $n \in \mathbb{N}$. Then,

$$\left(\sum_{s \in S} a_s\right)^n = \sum_{(k_1, k_2, \ldots, k_n) \in S^n} \prod_{i=1}^{n} a_{k_i}.$$

(Note that if $n = 0$, then the Cartesian power S^n has no factors; it consists of a single element, namely the empty 0-tuple $()$.)

Exercise 2.19.1. Prove Lemma 2.19.3.

We shall first prove Theorem 2.19.1 in the case when n is prime; i.e., we shall prove the following result:

[26] But if two of the $2n-1$ integers are equal, then you can have them both in your pick.

Lemma 2.19.4. Let p be a prime. Let $a_1, a_2, \ldots, a_{2p-1}$ be any $2p-1$ integers (not necessarily distinct). Then, there exists a p-element subset S of $\{1, 2, \ldots, 2p-1\}$ such that $p \mid \sum_{s \in S} a_s$.

Having established Lemma 2.19.4, we shall next extend it to a larger list of numbers:

Lemma 2.19.5. Let p be a prime. Let u be a positive integer. Let $a_1, a_2, \ldots, a_{up-1}$ be any $up-1$ integers (not necessarily distinct). Then, there exist $u-1$ disjoint p-element subsets $S_1, S_2, \ldots, S_{u-1}$ of $\{1, 2, \ldots, up-1\}$ such that

$$p \mid \sum_{s \in S_i} a_s \qquad \text{for all } i \in \{1, 2, \ldots, u-1\}.$$

Exercise 2.19.2. Formalize the above proof of Lemma 2.19.5.

Now the hard part is done: It turns out that non-prime integers n in Theorem 2.19.1 can be dealt with by splitting out a prime factor p, and applying Lemma 2.19.5 to this p. Here is the argument in detail:

3. Equivalence relations and residue classes

3.1. Relations

Loosely speaking, a *relation* on a set S is a property that two elements a and b of S (or, more formally, a pair $(a, b) \in S \times S$ of two elements of S) can either have or not have. For example, equality (denoted $=$) is a relation, since two elements a and b of S are either equal (i.e., satisfy $a = b$) or not equal. Likewise, the divisibility relation (denoted $\mid$) is a relation on $\mathbb{Z}$, since two elements a and b of $\mathbb{Z}$ either satisfy $a \mid b$ or do not.

A formal definition of relations proceeds as follows:

Definition 3.1.1. Fix a set S. A *binary relation* on S is a subset of $S \times S$ (that is, a set of pairs of elements of S).

If R is a binary relation (on S), and if $a, b \in S$, then we write aRb for $(a, b) \in R$.

The word "*relation*" shall always mean "binary relation" unless we say otherwise.

So a relation on a set S is, formally speaking, a subset of $S \times S$ – but in practice, we think of it as a property that holds for some pairs $(a, b) \in S \times S$ (namely, for the ones that belong to this subset) and does not hold for some others (namely, for the ones that do not belong to this subset).[27] In order to define a relation R on a given

[27] Here, the word "some" can mean "none" or "all" or anything inbetween.

set S, it suffices to tell which pairs $(a,b) \in S \times S$ satisfy aRb (because then, R will simply be the set of all these pairs (a,b)). Let us define several relations on the set $\mathbb{Z}$ by this strategy:

Example 3.1.2. Let $S = \mathbb{Z}$.

(a) The relation $=$ is a binary relation on S. As a subset of $S \times S$, this relation is

$$\begin{aligned}&\{(a,b) \in S \times S \mid a = b\} \\ &= \{(c,c) \mid c \in S\} = \{\ldots, (-1,-1), (0,0), (1,1), \ldots\}.\end{aligned}$$

(b) The relation $<$ is a binary relation on S. As a subset of $S \times S$, this relation is

$$\{(a,b) \in S \times S \mid a < b\}.$$

(c) The relation $\leq$ is a binary relation on S. As a subset of $S \times S$, this relation is

$$\{(a,b) \in S \times S \mid a \leq b\}.$$

(d) The relation $\neq$ is also a binary relation on S.

(e) Fix $n \in \mathbb{Z}$. Define a relation $\underset{n}{\equiv}$ on $S = \mathbb{Z}$ by

$$\left(a \underset{n}{\equiv} b\right) \iff (a \equiv b \bmod n).$$

As a subset of $S \times S = \mathbb{Z} \times \mathbb{Z}$, this relation $\underset{n}{\equiv}$ is

$$\begin{aligned}&\{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid a \equiv b \bmod n\} \\ &= \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{there exists an integer } d \text{ such that } b = a + nd\} \\ &\qquad \text{(by Exercise 2.3.7)} \\ &= \{(a, a+nd) \mid a, d \in \mathbb{Z}\}.\end{aligned}$$

Note that the relation $\underset{0}{\equiv}$ is exactly the relation $=$ (by Example 2.3.2 **(c)**).

(f) Define a binary relation $\boxed{N}$ on S by

$$\left(a \boxed{N} b\right) \iff (\text{false})$$

(that is, $a \boxed{N} b$ never holds, no matter what a and b are). As a subset of $S \times S$, this relation $\boxed{N}$ is just the empty subset of $S \times S$.

(g) On the other extreme: Define a binary relation $\boxed{A}$ on S by

$$\left(a \boxed{A} b\right) \iff (\text{true})$$

(that is, $a \boxed{A} b$ holds for all a and b). As a subset of $S \times S$, this relation $\boxed{A}$ is the whole set $S \times S$. Note that the relation $\boxed{A}$ is exactly the relation $\underset{1}{\equiv}$ (by Example 2.3.2 **(d)**).

(h) The relation $\mid$ (divisibility) is also a relation on $S = \mathbb{Z}$.
(i) The relation $\perp$ (coprimality) is also a relation on $S = \mathbb{Z}$.
(j) We have defined several relations on the set $S = \mathbb{Z}$ now. The relations $=$, $\neq$, $\boxed{N}$ and $\boxed{A}$ (or, rather, relations analogous to them) can be defined on **any** set.

3.2. Equivalence relations

Relations occur frequently in mathematics, and there is a bunch of properties that a relation can have or not have. (See the Wikipedia article on binary relations for a long list of such properties.) We shall need only the following three:

Definition 3.2.1. Let R be a binary relation on a set S.
(a) We say that R is *reflexive* if every $a \in S$ satisfies aRa.
(b) We say that R is *symmetric* if every $a, b \in S$ satisfying aRb satisfy bRa.
(c) We say that R is *transitive* if every $a, b, c \in S$ satisfying aRb and bRc satisfy aRc.

(Here are mnemonics for the three words we just defined:

- "Reflexive" should make you think of R as a mirror through which a can see itself (that is, satisfy aRa).
- "Symmetric" means that the roles of a and b in aRb are interchangeable – a symmetry.
- "Transitive" means that you can "transit" an element b on your way from a to c (that is, if you treat aRb as the existence of a "path" from a to b, and bRc as the existence of a "path" from b to c, then you can combine a "path" from a to b with a "path" from b to c to get a "path" from a to c).)

Let us see some examples of these properties of relations[28]:

Example 3.2.2. Let S be the set $\mathbb{Z}$. Consider the relations on $\mathbb{Z}$ defined in Example 3.1.2.
(a) The relation $=$ is reflexive, symmetric and transitive.
(b) The relation $<$ is transitive, but neither reflexive nor symmetric.
(c) The relation $\leq$ is transitive and reflexive, but not symmetric.
(d) The relation $\neq$ is symmetric, but neither reflexive nor transitive.
(e) For each $n \in \mathbb{Z}$, the relation $\underset{n}{\equiv}$ is reflexive, symmetric and transitive.
(f) The relation $\boxed{N}$ is symmetric and transitive, but not reflexive.
(g) The relation $\boxed{A}$ is reflexive, symmetric and transitive.
(h) The divisibility relation $\mid$ is reflexive and transitive, but not symmetric.
(i) The coprimality relation $\perp$ is symmetric, but neither reflexive nor transitive.

[28]See further below for the proofs of the claims made in this example.

Definition 3.2.3. An *equivalence relation* on a set S means a relation on S that is reflexive, symmetric and transitive.

Example 3.2.4. Let S be any set. The relation $=$ on the set S is an equivalence relation, because it is reflexive, symmetric and transitive.

Example 3.2.5. Let $n \in \mathbb{Z}$. The relation $\underset{n}{\equiv}$ on $\mathbb{Z}$ (defined in Example 3.1.2 **(e)**) is an equivalence relation, because (as we saw in Example 3.2.2 **(e)**) it is reflexive, symmetric and transitive.

Example 3.2.6. Here are some examples from elementary plane geometry: Congruence (e.g., of triangles) is an equivalence relation. Similarity is also an equivalence relation. The same holds for direct similarity (i.e., orientation-preserving similarity). The same holds for parallelism of lines.

Example 3.2.7. Let S and T be two sets, and let $f : S \to T$ be a map. Define a relation $\underset{f}{\equiv}$ on S by

$$\left(a \underset{f}{\equiv} b\right) \iff \left(f(a) = f(b)\right).$$

This relation $\underset{f}{\equiv}$ is an equivalence relation.

We will soon learn that **every** equivalence relation on a set S is actually of the form $\underset{f}{\equiv}$ for some set T and some map $f : S \to T$. (Namely, this is proven in Exercise 3.3.3 below.)

Example 3.2.8. Let S be the set of all points on the landmass of the Earth, and let $\sim$ be the relation on S defined by

$$(a \sim b) \iff (\text{there is a land route from } a \text{ to } b).$$

This $\sim$ is an equivalence relation (with the caveat that S is not a mathematical object and thus not really well-defined).

Example 3.2.9. Let

$$S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) = \{(a_1, a_2) \mid a_1 \in \mathbb{Z} \text{ and } a_2 \in \mathbb{Z} \setminus \{0\}\}.$$

This is the set of all pairs whose first entry is an integer and whose second entry is a nonzero integer. We define a relation $\underset{*}{\sim}$ on S by

$$\left((a_1, a_2) \underset{*}{\sim} (b_1, b_2)\right) \iff (a_1 b_2 = a_2 b_1).$$

This relation $\underset{*}{\sim}$ is an equivalence relation.

The relation $\underset{*}{\sim}$ from Example 3.2.9 may appear familiar to you. In fact, its definition can be restated as follows:

$$\left((a_1, a_2) \underset{*}{\sim} (b_1, b_2)\right) \iff \left(\frac{a_1}{a_2} = \frac{b_1}{b_2}\right),$$

and this makes the claims of Example 3.2.9 a lot more obvious. However, this is (in a sense) circular reasoning: The statement "$\frac{a_1}{a_2} = \frac{b_1}{b_2}$" only makes sense if the rational numbers have been defined[29], but the definition of rational numbers (at least the usual definition, given in [Swanso18, §3.6] and in many other places) already relies on the claims of Example 3.2.9. (Namely, the rational numbers are defined as the equivalence classes of the relation $\underset{*}{\sim}$; this is explained in Example 3.3.6 below.) Thus, our above proof of Example 3.2.9 was not a waste of time, but rather an important prerequisite for the construction of rational numbers (one of the cornerstones of mathematics).

If you are familiar with basic linear algebra, you may notice that the relation $\underset{*}{\sim}$ from Example 3.2.9 can also be regarded as linear dependence. Namely, two pairs (a_1, a_2) and (b_1, b_2) in $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ satisfy $(a_1, a_2) \underset{*}{\sim} (b_1, b_2)$ if and only if the vectors (a_1, a_2) and (b_1, b_2) in $\mathbb{Q}^2$ are linearly dependent.[30]

One simple property of symmetric relations will come useful:

Proposition 3.2.10. Let $\sim$ be a symmetric relation on a set S. Let $a, b \in S$. Then, $a \sim b$ if and only if $b \sim a$.

3.3. Equivalence classes

3.3.1. Definition of equivalence classes

We can now state one of the most important definitions in mathematics:

Definition 3.3.1. Let $\sim$ be an equivalence relation on a set S.

(a) For each $a \in S$, we define a subset $[a]_\sim$ of S by

$$[a]_\sim = \{b \in S \mid b \sim a\}. \tag{30}$$

This subset $[a]_\sim$ is called the *equivalence class* of a, or the *$\sim$-equivalence class* of a.

(b) The *equivalence classes* of $\sim$ are defined to be the sets $[a]_\sim$ for $a \in S$. They are also known as the *$\sim$-equivalence classes*.

[29] since $\frac{a_1}{a_2}$ and $\frac{b_1}{b_2}$ are (in general) not integers but rational numbers

[30] Note, however, that linear dependence is no longer an equivalence relation if we allow the vector $(0, 0)$ in our set S, because then, it is no longer transitive (for example, $(1, 1)$ and $(0, 0)$ are linearly dependent, and $(0, 0)$ and $(1, 2)$ are linearly dependent, but $(1, 1)$ and $(1, 2)$ are not).

Example 3.3.2. Consider the relation $\underset{3}{\equiv}$ on $\mathbb{Z}$ (defined in Example 3.1.2 **(e)**). We have

$$\begin{aligned}[5]_{\underset{3}{\equiv}} &= \left\{ b \in \mathbb{Z} \mid b \underset{3}{\equiv} 5 \right\} = \{ b \in \mathbb{Z} \mid b \equiv 5 \bmod 3 \} \\ &= \{\ldots, -4, -1, 2, 5, 8, 11, 14, \ldots\}\end{aligned}$$

and

$$\begin{aligned}[3]_{\underset{3}{\equiv}} &= \left\{ b \in \mathbb{Z} \mid b \underset{3}{\equiv} 3 \right\} = \{ b \in \mathbb{Z} \mid b \equiv 3 \bmod 3 \} \\ &= \{\ldots, -6, -3, 0, 3, 6, 9, 12, \ldots\}\end{aligned}$$

and

$$\begin{aligned}[2]_{\underset{3}{\equiv}} &= \left\{ b \in \mathbb{Z} \mid b \underset{3}{\equiv} 2 \right\} = \{ b \in \mathbb{Z} \mid b \equiv 2 \bmod 3 \} \\ &= \{\ldots, -4, -1, 2, 5, 8, 11, 14, \ldots\}.\end{aligned}$$

Note that $[5]_{\underset{3}{\equiv}} = [2]_{\underset{3}{\equiv}}$, as you can easily see.

3.3.2. Basic properties

Proposition 3.3.3. Let $\sim$ be an equivalence relation on a set S. Let $a \in S$. Then,

$$[a]_{\sim} = \{ b \in S \mid a \sim b \}.$$

Proposition 3.3.3 shows that we can replace the condition "$b \sim a$" by "$a \sim b$" in Definition 3.3.1 **(a)** without changing the meaning of the definition. (Some authors, such as Swanson in [Swanso18, Definition 2.3.6], do exactly that.)

Proposition 3.3.4. Let $\sim$ be an equivalence relation on a set S. Let $a \in S$. Then, $a \in [a]_{\sim}$.

Proposition 3.3.4 shows that all equivalence classes of an equivalence relation are nonempty sets (because each equivalence class $[a]_{\sim}$ contains at least the element a).

Theorem 3.3.5. Let $\sim$ be an equivalence relation on a set S. Let $x, y \in S$.
(a) If $x \sim y$, then $[x]_{\sim} = [y]_{\sim}$.
(b) If not $x \sim y$, then the sets $[x]_{\sim}$ and $[y]_{\sim}$ are disjoint.
(c) We have $x \sim y$ if and only if $x \in [y]_{\sim}$.
(d) We have $x \sim y$ if and only if $y \in [x]_{\sim}$.
(e) We have $x \sim y$ if and only if $[x]_{\sim} = [y]_{\sim}$.

Theorem 3.3.5 yields an important property of equivalence classes:

Exercise 3.3.1. Let $\sim$ be an equivalence relation on a set S. Prove that any two equivalence classes of $\sim$ are either identical or disjoint.

In the following, we will try to use Greek letters for equivalence classes and Roman letters for their representatives. (See the solution to Exercise 3.3.1 for an example.)

3.3.3. More examples

Example 3.3.6. Consider the relation $\underset{*}{\sim}$ on $S = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ defined in Example 3.2.9. Its equivalence classes are the rational numbers. Indeed, the equivalence class $\left[(a_1, a_2)\right]_{\underset{*}{\sim}}$ of a pair $(a_1, a_2) \in S$ is commonly denoted by $\dfrac{a_1}{a_2}$ (or by a_1/a_2). This is how rational numbers are defined!

Equivalence classes appear in real life too, at least in the modern world. When you say that the sun rises approximately at 7 AM in February[31], what do "7 AM" and "February" mean? Clearly, "February" is not a specific month in history, since each year has its own February. Rather, it stands for an equivalence class of months, with respect to the relation of "being an integer number of years apart". Similarly, "7 AM" means an equivalence class of moments with respect to the relation of "being an integer number of days apart". Likewise, "the horse" in "the horse has a lifespan of 25 years" refers not to a specific horse, but to the whole species, which is an equivalence class of creatures with respect to a certain relation[32]. Finally, the equivalence classes of the relation $\sim$ in Example 3.2.8 are commonly referred to as "continents"[33] or "islands". Equivalence classes provide a way to refer to multiple objects (usually similar in some way) as if they were one.

3.3.4. The "is a permutation of" relation on tuples

Let us give a few more mathematical examples for equivalences and equivalence classes:

Definition 3.3.7. Let A be a set, and let $k \in \mathbb{N}$. As we know, A^k denotes the set of all k-tuples of elements of A.

The relation $\underset{\text{perm}}{\sim}$ on A^k is defined as follows:

$$\left(\mathbf{p} \underset{\text{perm}}{\sim} \mathbf{q}\right) \Longleftrightarrow \left(\mathbf{p} \text{ is a permutation of } \mathbf{q}\right).$$

[31] in Minneapolis

[32] According to Darwin, the relation is "being able to procreate" – although this is not per se an equivalence relation, so some tweaks need to be made ("reflexive-and-transitive closure") to turn it into one.

[33] at least if one considers Eurasia to be a single continent

(We are using Definition 2.13.16 here.) For example, $(3,8,8,2) \underset{\text{perm}}{\sim} (8,3,2,8)$.

Exercise 3.3.2. Prove that the relation $\underset{\text{perm}}{\sim}$ is an equivalence relation.

Definition 3.3.8. Let A be a set, and let $k \in \mathbb{N}$. The relation $\underset{\text{perm}}{\sim}$ on A^k is an equivalence relation (by Exercise 3.3.2). Its equivalence classes are called the *unordered k-tuples* of elements of A. For example, for $k = 2$ and $A = \mathbb{Z}$, the two 2-tuples $(6,8)$ and $(8,6)$ are permutations of each other, so $(6,8) \underset{\text{perm}}{\sim} (8,6)$ and thus $[(6,8)]_{\underset{\text{perm}}{\sim}} = [(8,6)]_{\underset{\text{perm}}{\sim}}$.

3.3.5. The "is a cyclic rotation of" relation on tuples

Another example of an equivalence relation is the following:

Definition 3.3.9. Again, let A be a set and $k \in \mathbb{N}$. If $\mathbf{a} = (a_1, a_2, \ldots, a_k) \in A^k$, then a *cyclic rotation* of $\mathbf{a}$ means a k-tuple of the form

$$(a_{i+1}, a_{i+2}, \ldots, a_k, a_1, a_2, \ldots, a_i) \in A^k$$

for some $i \in \{0, 1, \ldots, k\}$.

For example, the cyclic rotations of the 3-tuple $(1,4,5)$ are $(1,4,5)$, $(4,5,1)$ and $(5,1,4)$.

(Here is an equivalent description of cyclic rotations: Let C be the map $A^k \to A^k$ that sends each k-tuple $(a_1, a_2, \ldots, a_k)$ to $(a_2, a_3, \ldots, a_k, a_1)$. Then, it is easy to see that a cyclic rotation of $\mathbf{a}$ is the same as a k-tuple of the form $C^i(\mathbf{a})$ for some $i \in \{0, 1, \ldots, k\}$. But it is also easy to see that $C^k = \mathrm{id}$. Thus, the $C^i(\mathbf{a})$ for $i \in \{0, 1, \ldots, k\}$ are exactly the $C^i(\mathbf{a})$ for $i \in \mathbb{N}$.)

The relation $\underset{\text{cyc}}{\sim}$ on A^k is defined as follows:

$$\begin{aligned}\left(\mathbf{p} \underset{\text{cyc}}{\sim} \mathbf{q}\right) &\iff (\mathbf{p} \text{ is a cyclic rotation of } \mathbf{q}) \\ &\iff \left(\mathbf{p} = C^i(\mathbf{q}) \text{ for some } i \in \mathbb{N}\right).\end{aligned}$$

This relation $\underset{\text{cyc}}{\sim}$ is an equivalence relation. Its equivalence classes are called *necklaces* of length k over A.

We shall not prove the statements claimed in this definition, since they are particular cases of more general results that will be proven below (about groups acting on sets).

For example, the necklaces of length 3 over the set $A = \{1,2\}$ are

$$\begin{aligned}
[(1,1,1)]_{\underset{\text{cyc}}{\sim}} &= \{(1,1,1)\}, \\
[(1,1,2)]_{\underset{\text{cyc}}{\sim}} &= \{(1,1,2),(1,2,1),(2,1,1)\}, \\
[(1,2,2)]_{\underset{\text{cyc}}{\sim}} &= \{(1,2,2),(2,2,1),(2,1,2)\}, \\
[(2,2,2)]_{\underset{\text{cyc}}{\sim}} &= \{(2,2,2)\}.
\end{aligned}$$

This may suggest that a necklace $[(a_1,a_2,\ldots,a_k)]_{\underset{\text{cyc}}{\sim}}$ is uniquely determined by how often each element appears in the tuple $(a_1,a_2,\ldots,a_k)$. But this is not true in general; for example, if $A = \{1,2,3\}$, then

$$\begin{aligned}
[(1,2,3)]_{\underset{\text{cyc}}{\sim}} &= \{(1,2,3),(2,3,1),(3,1,2)\} \qquad \text{and} \\
[(1,3,2)]_{\underset{\text{cyc}}{\sim}} &= \{(1,3,2),(3,2,1),(2,1,3)\}
\end{aligned}$$

are two different necklaces of length 3 over the set $A = \{1,2,3\}$.

How many necklaces of length k over a q-element set A exist? It turns out that there is a nice formula for this, involving Euler's totient function ϕ:

Theorem 3.3.10. Let k be a positive integer. Let A be a q-element set (where $q \in \mathbb{N}$). Then, the number of necklaces of length k over the set A is

$$\frac{1}{k}\sum_{d|k}\phi(d)\,q^{k/d}.$$

Note that it is not (a priori) clear that $\frac{1}{k}\sum_{d|k}\phi(d)\,q^{k/d}$ is an integer! Actually, this holds even when q is a negative integer, even though there exist no q-element sets in that case. Thus, $\frac{1}{k}\sum_{d|k}\phi(d)\,x^{k/d}$ is another integer-valued polynomial for each positive integer k.

We will prove Theorem 3.3.10 using the concept of group actions further below.

3.3.6. Definition of the quotient set and the projection map

Definition 3.3.11. Let S be a set, and let $\sim$ be an equivalence relation on S.

(a) The set of equivalence classes of $\sim$ is denoted by $S/\sim$. It is called the *quotient* (or *quotient set*) of S by $\sim$.

(b) The map

$$\begin{aligned}
S &\to S/\sim, \\
s &\mapsto [s]_{\sim}
\end{aligned}$$

(which sends each element $s \in S$ to its equivalence class) is called the *canonical projection (onto the quotient)*, and we will denote it by $\pi_\sim$.

(c) An element of an equivalence class of $\sim$ is also called a *representative* of this class.

Exercise 3.3.3. Let S be a set.

Recall that if T is a further set, and if $f : S \to T$ is a map, then an equivalence relation $\underset{f}{\equiv}$ is defined on the set S. (See Example 3.2.7 for its definition.)

Now, let $\sim$ be **any** equivalence relation on S. Prove that $\sim$ has the form $\underset{f}{\equiv}$ for a properly chosen set T and a properly chosen $f : S \to T$.

More precisely, prove that $\sim$ equals $\underset{f}{\equiv}$, where T is the quotient set $S/\sim$ and where $f : S \to T$ is the canonical projection $\pi_\sim : S \to S/\sim$.

[**Hint:** To prove that two relations R_1 and R_2 on S are equal, you need to check that every pair (a, b) of elements of S satisfies the equivalence $(aR_1b) \iff (aR_2b)$.]

3.4. $\mathbb{Z}/n$ ("integers modulo n")

We now come to one of the most important example of equivalence classes: the residue classes of integers modulo a given positive integer n.

Convention 3.4.1. For the whole Section 3.4, we fix an integer n.

3.4.1. Definition of $\mathbb{Z}/n$

Definition 3.4.2. (a) Define a relation $\underset{n}{\equiv}$ on the set $\mathbb{Z}$ by

$$\left(a \underset{n}{\equiv} b\right) \iff (a \equiv b \bmod n).$$

(This is precisely the relation $\underset{n}{\equiv}$ from Example 3.1.2 **(e)**.)

Recall that $\underset{n}{\equiv}$ is an equivalence relation (by Example 3.2.5).

(b) A *residue class modulo n* means an equivalence class of the relation $\underset{n}{\equiv}$.

For example,

$$[0]_{\underset{5}{\equiv}} = \{\ldots, -15, -10, -5, 0, 5, 10, 15, 20, \ldots\},$$
$$[1]_{\underset{5}{\equiv}} = \{\ldots, -14, -9, -4, 1, 6, 11, 16, 21, \ldots\},$$
$$[2]_{\underset{5}{\equiv}} = \{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\},$$
$$[3]_{\underset{5}{\equiv}} = \{\ldots, -12, -7, -2, 3, 8, 13, 18, 23, \ldots\},$$
$$[4]_{\underset{5}{\equiv}} = \{\ldots, -11, -6, -1, 4, 9, 14, 19, 24, \ldots\}$$

are all the residue classes modulo 5. As you see, these classes are in 1-to-1 correspondence with the 5 possible remainders $0, 1, 2, 3, 4$ modulo 5. This generalizes (see Theorem 3.4.4 below). First, let us introduce a few notations:

Definition 3.4.3. (a) If i is an integer, then we denote the residue class $[i]_{\equiv n}$ by $[i]_n$. (Some authors denote this residue class by $\overline{i}_n$ or $i \bmod n$. Be careful with the notation $i \bmod n$, since other authors use it for the integer $i\%n$ when n is positive.)

(b) The set $\mathbb{Z}/\equiv n$ of all residue classes modulo n is called $\mathbb{Z}/n$. (Some authors call it $\mathbb{Z}/(n)$ or $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$. Be careful with the notation $\mathbb{Z}_n$, since it has a different meaning, too.)

3.4.2. What $\mathbb{Z}/n$ looks like

Let us now state and rigorously prove what we have just observed on the example of $n = 5$:

Theorem 3.4.4. Assume that the integer n is positive.

The set $\mathbb{Z}/n$ has exactly n elements, namely $[0]_n, [1]_n, \ldots, [n-1]_n$. (In particular, these elements $[0]_n, [1]_n, \ldots, [n-1]_n$ are distinct.)

Before we prove this, let us make a simple observation:

Proposition 3.4.5. (a) Each element of $\mathbb{Z}/n$ can be written in the form $[s]_n$ for some integer s.

(b) Let a and b be integers. Then, we have $[a]_n = [b]_n$ if and only if $a \equiv b \bmod n$.

Let us summarize some of the facts we have shown in the above proof as a separate proposition:

Proposition 3.4.6. Let n be a positive integer.

(a) The two maps

$$P : \{0, 1, \ldots, n-1\} \to \mathbb{Z}/n, \quad s \mapsto [s]_n$$

and

$$R : \mathbb{Z}/n \to \{0, 1, \ldots, n-1\}, \quad [s]_n \mapsto s\%n$$

are well-defined and mutually inverse, and thus are bijections.

(b) Let $\alpha \in \mathbb{Z}/n$. Then, there exists a unique $a \in \{0, 1, \ldots, n-1\}$ satisfying $\alpha = [a]_n$.

Proposition 3.4.6 **(b)** can be restated as follows: Each residue class $\alpha \in \mathbb{Z}/n$ has a unique representative in the set $\{0, 1, \ldots, n-1\}$.

3.4.3. Making choices that don't matter: The universal property of quotient sets

In the above proof of Theorem 3.4.4, we have witnessed an important issue in dealing with quotient sets: If you want to define a map f going **out** of a quotient set $S/\sim$ [34], then the easiest way to do so is often to specify $f([s]_\sim)$ for each $s \in S$; but in order to ensure that this definition is well-defined (i.e., that our map f actually exists), we need to verify that the value of $f([s]_\sim)$ we are specifying depends **only on the equivalence class** $[s]_\sim$ but not on the representative s. In other words, we need to verify that if s_1 and s_2 are two elements of S such that $[s_1]_\sim = [s_2]_\sim$, then our definition of f assigns the same value to $f([s_1]_\sim)$ as it does to $f([s_2]_\sim)$. This verification (which we did in our above proof by proving Claim 1) is often quite easy, but it is necessary.

Let us restate this strategy for defining maps out of a quotient set more rigorously:

Remark 3.4.7. Let S and T be two sets, and let $\sim$ be an equivalence relation on S. Assume that we want to define a map

$$\begin{aligned} f : S/\sim &\to T, \\ [s]_\sim &\mapsto F(s), \end{aligned}$$

where $F(s)$ is some element of T for each $s \in S$. (That is, we want to define a map $f : S \to T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$.)

In order to ensure that this f is well-defined, we need to verify that if s_1 and s_2 are two elements of S such that $[s_1]_\sim = [s_2]_\sim$, then $F(s_1) = F(s_2)$. If this verification has been done, the map f is well-defined.

Further examples of maps out of quotient sets defined in this way can be found in [ConradW][35].

Let us illustrate this method of defining maps on a few more examples:

Example 3.4.8. Let A be a set, and let $k \in \mathbb{N}$. Fix some $c \in A$. We can then define a map

$$\begin{aligned} \mathrm{mult}_c : A^k &\to \mathbb{N}, \\ (a_1, a_2, \ldots, a_k) &\mapsto (\text{the number of } i \in \{1, 2, \ldots, k\} \text{ such that } a_i = c). \end{aligned}$$

This map mult_c simply sends each k-tuple to the number of times that c appears in this k-tuple. For example, $\mathrm{mult}_5(1,5,2,4,7,5,5,6) = 3$, since 5 appears exactly 3 times in the 8-tuple $(1,5,2,4,7,5,5,6)$ (assuming that $k = 8$ and $A = \mathbb{Z}$). It is clear that this map

[34] In our case, the quotient set was $\mathbb{Z}/\underset{n}{\equiv}$ (also known as $\mathbb{Z}/n$), and the map we wanted to define was R.

[35] When reading [ConradW, Example 1.1], keep in mind that rational numbers are defined as equivalence classes of elements of $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, as we have seen in Example 3.3.6. Thus, $\mathbb{Q}$ is actually a quotient set: namely, $\mathbb{Q} = S/\underset{*}{\sim}$ using the notations of Example 3.3.6.

mult_c is well-defined. (The number $\mathrm{mult}_c\,\mathbf{a}$ for a k-tuple $\mathbf{a}$ is called the *multiplicity of c in* $\mathbf{a}$. Therefore the notation "mult_c".)

Now, it stands to reason that the same can be done with **unordered** k-tuples: After all, the number of times that c appears in a k-tuple should not depend on the order of the entries of the tuple. To formalize this, however, we need to deal with quotient sets. Indeed, recall that the "unordered k-tuples of elements of A" were defined (in Definition 3.3.8) as equivalence classes of the relation $\underset{\text{perm}}{\sim}$ on the set A^k. So $A^k/\underset{\text{perm}}{\sim}$ is the set of all unordered k-tuples of elements of A. The map that counts how often c appears in an unordered k-tuple should thus have the form

$$\begin{aligned}\mathrm{mult}'_c : A^k/\underset{\text{perm}}{\sim} &\to \mathbb{N},\\ [(a_1,a_2,\ldots,a_k)]_{\underset{\text{perm}}{\sim}} &\mapsto (\text{the number of } i\in\{1,2,\ldots,k\} \text{ such that } a_i = c)\,.\end{aligned}$$

Or, to put it more compactly (making use of the map mult_c for **ordered** k-tuples defined above), it should have the form

$$\begin{aligned}\mathrm{mult}'_c : A^k/\underset{\text{perm}}{\sim} &\to \mathbb{N},\\ [\mathbf{a}]_{\underset{\text{perm}}{\sim}} &\mapsto \mathrm{mult}_c\,\mathbf{a}.\end{aligned}$$

The question is: Why is this map mult'_c well-defined?

Remark 3.4.7 (applied to A^k, $\mathbb{N}$ and $\underset{\text{perm}}{\sim}$ instead of S, T and $\sim$) shows that in order to ensure that this map mult'_c is well-defined, we need to verify that if $\mathbf{a}_1$ and $\mathbf{a}_2$ are two elements of A^k (that is, two ordered k-tuples) such that $[\mathbf{a}_1]_{\underset{\text{perm}}{\sim}} = [\mathbf{a}_2]_{\underset{\text{perm}}{\sim}}$, then $\mathrm{mult}_c(\mathbf{a}_1) = \mathrm{mult}_c(\mathbf{a}_2)$. Let us do this: Let $\mathbf{a}_1$ and $\mathbf{a}_2$ be two elements of A^k (that is, two ordered k-tuples) such that $[\mathbf{a}_1]_{\underset{\text{perm}}{\sim}} = [\mathbf{a}_2]_{\underset{\text{perm}}{\sim}}$. Now, $[\mathbf{a}_1]_{\underset{\text{perm}}{\sim}} = [\mathbf{a}_2]_{\underset{\text{perm}}{\sim}}$ entails $\mathbf{a}_1 \underset{\text{perm}}{\sim} \mathbf{a}_2$ (indeed, Theorem 3.3.5 **(e)** shows that we have $\mathbf{a}_1 \underset{\text{perm}}{\sim} \mathbf{a}_2$ if and only if $[\mathbf{a}_1]_{\underset{\text{perm}}{\sim}} = [\mathbf{a}_2]_{\underset{\text{perm}}{\sim}}$). In other words, $\mathbf{a}_1$ is a permutation of $\mathbf{a}_2$ (by the definition of $\underset{\text{perm}}{\sim}$). In other words, the tuples $\mathbf{a}_1$ and $\mathbf{a}_2$ differ only in the order of their entries. Hence, Lemma 2.13.21 (applied to A, $\mathbf{a}_1$, $\mathbf{a}_2$ and c instead of P, $(a_1,a_2,\ldots,a_k)$, $(b_1,b_2,\ldots,b_\ell)$ and p) yields that

$$(\text{the number of times } c \text{ appears in } \mathbf{a}_1) = (\text{the number of times } c \text{ appears in } \mathbf{a}_2)\,.$$

This rewrites as $\mathrm{mult}_c(\mathbf{a}_1) = \mathrm{mult}_c(\mathbf{a}_2)$ (since (the number of times c appears in $\mathbf{a}_1$) $= \mathrm{mult}_c(\mathbf{a}_1)$ and (the number of times c appears in $\mathbf{a}_2$) $= \mathrm{mult}_c(\mathbf{a}_2)$). This is what we needed to prove. Thus, we have shown that mult'_c is well-defined.

On the other hand, if we tried to define a map

$$\begin{aligned}\mathrm{first} : A^k/\underset{\text{perm}}{\sim} &\to \mathbb{N},\\ [\mathbf{a}]_{\underset{\text{perm}}{\sim}} &\mapsto (\text{the first entry of } \mathbf{a})\end{aligned}$$

(assuming that $k > 0$, so that an ordered k-tuple does indeed have a first entry), then we would run into troubles, because it is **not** true that if $\mathbf{a}_1$ and $\mathbf{a}_2$ are two elements of A^k such that $[\mathbf{a}_1]_{\underset{\text{perm}}{\sim}} = [\mathbf{a}_2]_{\underset{\text{perm}}{\sim}}$, then (the first entry of $\mathbf{a}_1$) $=$ (the first entry of $\mathbf{a}_2$). And this is no surprise: There is no such thing as "the first entry" of an unordered k-tuple. The first entry of a k-tuple is sensitive to reordering of its entries.

We can restate this method of defining maps as a rigorous theorem:

Theorem 3.4.9. Let S and T be two sets, and let $\sim$ be an equivalence relation on S. For each $s \in S$, let $F(s)$ be an element of T. (In other words, let F be a map from S to T.) Assume that the following assumption holds:

> *Assumption 1:* If s_1 and s_2 are two elements of S satisfying $s_1 \sim s_2$, then $F(s_1) = F(s_2)$.

Then, there exists a unique map $f : S/\sim \to T$ such that every $s \in S$ satisfies $f([s]_\sim) = F(s)$.

Theorem 3.4.9 says that (under the assumption that Assumption 1 holds) we can define a map

$$\begin{aligned} f : S/\sim &\to T, \\ [s]_\sim &\mapsto F(s). \end{aligned}$$

For example, the map R defined in our proof of Theorem 3.4.4 was defined in this way (with $\mathbb{Z}$, $\mathbb{Z}$, $\underset{n}{\equiv}$ and $s\%n$ playing the roles of S, T, $\sim$ and $F(s)$), and our proof of Claim 1 was essentially us verifying that Assumption 1 of Theorem 3.4.9 is satisfied.

For the sake of completeness, let us give a formal proof for Theorem 3.4.9 as well:

Theorem 3.4.9 is known as the *universal property of the quotient set*.

3.4.4. Projecting from $\mathbb{Z}/n$ to $\mathbb{Z}/d$

As another example of a map from a quotient set, let us define certain maps from $\mathbb{Z}/n$ to $\mathbb{Z}/d$ that exist whenever two integers n and d satisfy $d \mid n$:

Proposition 3.4.10. Let n be an integer. Let d be a divisor of n. Then, there is a map

$$\begin{aligned} \pi_{n,d} : \mathbb{Z}/n &\to \mathbb{Z}/d, \\ [s]_n &\mapsto [s]_d. \end{aligned}$$

Example 3.4.11. (a) For example, for $n = 6$ and $d = 2$, Proposition 3.4.10 says that there is a map

$$\begin{aligned} \pi_{6,2} : \mathbb{Z}/6 &\to \mathbb{Z}/2, \\ [s]_6 &\mapsto [s]_2. \end{aligned}$$

This map sends the residue classes

$$\begin{aligned} &[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6 \\ \text{to } &[0]_2, [1]_2, [2]_2, [3]_2, [4]_2, [5]_2, \text{ respectively.} \end{aligned}$$

In other words, it sends the residue classes

$$\begin{aligned} &[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6 \\ \text{to } &[0]_2, [1]_2, [0]_2, [1]_2, [0]_2, [1]_2, \text{ respectively} \end{aligned}$$

(since $[2]_2 = [0]_2$ and $[3]_2 = [1]_2$ and $[4]_2 = [0]_2$ and $[5]_2 = [1]_2$). More generally, for arbitrary positive integers n and d satisfying $d \mid n$, the map $\pi_{n,d}$ sends the n residue classes $[0]_n, [1]_n, \ldots, [n-1]_n$ to

$$[0]_d, [1]_d, \ldots, [d-1]_d, [0]_d, [1]_d, \ldots, [d-1]_d, \ldots, [0]_d, [1]_d, \ldots, [d-1]_d$$

(that is, $[0]_d, [1]_d, \ldots, [d-1]_d$ in this order, repeated $\dfrac{n}{d}$ many times), respectively.

(b) For a non-example, set $n = 3$ and $d = 2$. Then, Proposition 3.4.10 does not apply, since 2 is not a divisor of 3. And for good reason: There is no map

$$\begin{aligned} \pi_{3,2} : \mathbb{Z}/3 &\to \mathbb{Z}/2, \\ [s]_3 &\mapsto [s]_2 . \end{aligned}$$

Indeed, this map would have to send $[0]_3$ and $[3]_3$ to $[0]_2$ and $[3]_2$, respectively; but this means sending two equal inputs to different outputs (since $[0]_3 = [3]_3$ but $[0]_2 \neq [3]_2$), which is impossible. More generally, if a positive integer d is **not** a divisor of a positive integer n, then there is no map

$$\begin{aligned} \pi_{n,d} : \mathbb{Z}/n &\to \mathbb{Z}/d, \\ [s]_n &\mapsto [s]_d . \end{aligned}$$

The next exercise is unrelated to $\mathbb{Z}/n$, but has been placed in this section because it relies on the same sort of "well-definedness" argument that we have seen in our proofs above:

Exercise 3.4.1. Fix a prime p. For each nonzero rational number r, define an integer $w_p(r)$ (called the *extended p-adic valuation* of r) as follows: We write r in the form $r = a/b$ for two nonzero integers a and b, and we set $w_p(r) = v_p(a) - v_p(b)$. (It also makes sense to set $w_p(0) = \infty$, but we shall not concern ourselves with this border case in this exercise.)

(a) Prove that this is well-defined – i.e., that $w_p(r)$ does not depend on the precise choice of a and b satisfying $r = a/b$.

(b) Prove that $w_p(n) = v_p(n)$ for each nonzero integer n.

(c) Prove that $w_p(ab) = w_p(a) + w_p(b)$ for any two nonzero rational numbers a and b.

(d) Prove that $w_p(a+b) \geq \min\{w_p(a), w_p(b)\}$ for any two nonzero rational numbers a and b if $a + b \neq 0$.

Exercise 3.4.2. Let r be a nonzero rational number. In Exercise 3.4.1, we have defined an integer $w_p(r)$ for each prime p. Prove the following:

(a) All but finitely many primes p satisfy $w_p(r) = 0$.

(b) We have $|r| = \prod_{p \text{ prime}} p^{w_p(r)}$ (and in particular, the product $\prod_{p \text{ prime}} p^{w_p(r)}$ is well-defined, i.e., has only finitely many factors different from 1).

(c) We have $r \in \mathbb{Z}$ if and only if each prime p satisfies $w_p(r) \geq 0$.

(d) We have the logical equivalence

$$\begin{aligned} &\Big(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k r \in \mathbb{Z}\Big) \\ &\iff \big(\text{every prime } p \text{ satisfying } w_p(r) < 0 \text{ satisfies } p \mid m\big). \end{aligned}$$

Note that Exercise 3.4.2 **(b)** can be regarded as a canonical factorization for rational numbers. (Unlike the canonical factorization for integers, it allows negative exponents on the primes.)

3.4.5. Addition, subtraction and multiplication in $\mathbb{Z}/n$

Let us recall the concept of a binary operation (defined in Definition 1.6.1). We shall now define several such operations on the set $\mathbb{Z}/n$ [36]:

Definition 3.4.12. (a) We define a binary operation $+$ on $\mathbb{Z}/n$ (called *addition*) by setting

$$[a]_n + [b]_n = [a+b]_n \qquad \text{for any integers } a \text{ and } b.$$

(In other words, we define a binary operation $+$ on $\mathbb{Z}/n$ as follows: For any $\alpha, \beta \in \mathbb{Z}/n$, we let $\alpha + \beta = [a+b]_n$, where a and b are two integers satisfying $\alpha = [a]_n$ and $\beta = [b]_n$.)

(b) We define a binary operation $-$ on $\mathbb{Z}/n$ (called *subtraction*) by setting

$$[a]_n - [b]_n = [a-b]_n \qquad \text{for any integers } a \text{ and } b.$$

(c) We define a binary operation $\cdot$ on $\mathbb{Z}/n$ (called *multiplication*) by setting

$$[a]_n \cdot [b]_n = [a \cdot b]_n \qquad \text{for any integers } a \text{ and } b.$$

We also write $[a]_n [b]_n$ for $[a]_n \cdot [b]_n$.

Theorem 3.4.13. Everything defined in Definition 3.4.12 is well-defined.

Recall that $\mathbb{Z}/n$ is a finite set (of size n) whenever n is a positive integer. Hence, for each given positive integer n, we can tabulate all the values of the operations

[36] We will check afterwards that these operations are indeed well-defined.

$+$, $-$ and $\cdot$; the resulting tables are called *addition tables*, *subtraction tables* and *multiplication tables* (like in high school, except that we are working with residue classes now).

Example 3.4.14. (a) If $n = 3$, then the addition, subtraction and multiplication tables for $\mathbb{Z}/n = \mathbb{Z}/3$ are

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

,

$-$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[2]_3$	$[1]_3$
$[1]_3$	$[1]_3$	$[0]_3$	$[2]_3$
$[2]_3$	$[2]_3$	$[1]_3$	$[0]_3$

,

$\cdot$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[1]_3$

.

(Here, the entry in the row corresponding to α and the column corresponding to β is $\alpha + \beta$, $\alpha - \beta$ and $\alpha \cdot \beta$, respectively.)

(b) If $n = 2$, then the addition, subtraction and multiplication tables for $\mathbb{Z}/n = \mathbb{Z}/2$ are

$+$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

,

$-$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

,

$\cdot$	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[0]_2$
$[1]_2$	$[0]_2$	$[1]_2$

.

(In particular, the addition table is the same as the subtraction table, because any $\alpha, \beta \in \mathbb{Z}/2$ satisfy $\alpha + \beta = \alpha - \beta$. This follows from Exercise 2.3.1.)

Remark 3.4.15. We **cannot** define a division operation on $\mathbb{Z}/n$ by setting

$$[a]_n \,/\, [b]_n := [a/b]_n \qquad \text{for any integers } a \text{ and } b.$$

Indeed, leaving aside the issues that b could be 0 or a/b could be non-integer, this would still not be well-defined, because the class $[a/b]_n$ depends not just on $[a]_n$ and $[b]_n$ but also on the concrete choices of a and b. For example, for $n = 4$, this ostensible "division operation" would have to satisfy

$$\text{“ } [6]_4 \,/\, [2]_4 \text{ ”} = [6/2]_4 = [3]_4$$

and

$$\text{“ } [2]_4 \,/\, [2]_4 \text{ ”} = [2/2]_4 = [1]_4,$$

but this is impossible (since $[6]_4 = [2]_4$ but $[3]_4 \neq [1]_4$).

For similar reasons, we cannot define $([a]_n)^{[b]_n}$.

For the outputs of our binary operations $+$, $-$ and $\cdot$ on $\mathbb{Z}/n$, we shall use the same terminology as with integers:

Definition 3.4.16. (a) If α and β are two elements of $\mathbb{Z}/n$, then we shall refer to $\alpha+\beta$ as the *sum* of α and β.

(b) If α and β are two elements of $\mathbb{Z}/n$, then we shall refer to $\alpha-\beta$ as the *difference* of α and β.

(c) If α and β are two elements of $\mathbb{Z}/n$, then we shall refer to $\alpha\cdot\beta$ (also known as $\alpha\beta$) as the *product* of α and β.

(d) If α is an element of $\mathbb{Z}/n$, then the difference $[0]_n-\alpha$ shall be denoted by $-\alpha$.

Caution: While the remainder $i\%n$ and the residue class $[i]_n$ encode the same information about an integer i (for a fixed positive integer n), they are not the same thing! For example, any two integers u and v satisfy $[u]_n+[v]_n=[u+v]_n$ but don't always satisfy $u\%n+v\%n=(u+v)\%n$ [37]. Thus, it is important to distinguish between $i\%n$ and $[i]_n$.

Remark 3.4.17. We can view the residue classes modulo 24 (that is, the elements of $\mathbb{Z}/24$) as the hours of the day. For example, the time "2 AM" can be viewed as the residue class $[2]_{24}$, whereas the time "3 PM" can be viewed as the residue class $[15]_{24}$. From this point of view, addition of residue classes is a rather familiar operation: For example, the statement that "10 hours from 3 PM is 1 AM" is saying $[15]_{24}+[10]_{24}=[1]_{24}$.

3.4.6. Scaling by $r\in\mathbb{Z}$

Let us define another operation – not binary this time – on $\mathbb{Z}/n$:

Definition 3.4.18. Fix $r\in\mathbb{Z}$.

For any $\alpha\in\mathbb{Z}/n$, we define a residue class $r\alpha\in\mathbb{Z}/n$ by setting

$$\left(r\left[a\right]_n=\left[ra\right]_n \qquad \text{for any } a\in\mathbb{Z}\right).$$

(In other words, for any $\alpha\in\mathbb{Z}/n$, we let $r\alpha=[ra]_n$, where a is an integer satisfying $\alpha=[a]_n$.) This is well-defined, because of Proposition 3.4.19 **(a)** below.

We also write $r\cdot[a]_n$ for $r\left[a\right]_n$.

Proposition 3.4.19. Fix $r\in\mathbb{Z}$.

(a) For any $\alpha\in\mathbb{Z}/n$, the residue class $r\alpha\in\mathbb{Z}/n$ in Definition 3.4.18 is well-defined.

(b) For any $\alpha\in\mathbb{Z}/n$, we have $r\alpha=[r]_n\cdot\alpha$.

[37] Here is a specific example:

$$[2]_5+[3]_5=[2+3]_5=[5]_5=[0]_5, \qquad \text{but}$$
$$2\%5+3\%5=2+3=5\neq 0\%5;$$

Exercise 2.6.3 **(a)** addresses how $u\%n+v\%n$ differs from $(u+v)\%n$.

For a fixed $r \in \mathbb{Z}$, we shall refer to the map

$$\begin{aligned} \mathbb{Z}/n &\to \mathbb{Z}/n, \\ \alpha &\mapsto r\alpha \end{aligned}$$

as *scaling by r*. This map is actually the same as multiplication by the residue class $[r]_n$ (by Proposition 3.4.19 **(b)**). So why did we define it "from scratch" rather than piggybacking on the already established definition of multiplication in $\mathbb{Z}/n$ (Definition 3.4.12 **(c)**)? The reason is that scaling operations appear much more frequently in algebra than multiplication operations. (For example, every vector space has a scaling operation, but usually there is no way of multiplying two vectors.) Thus, it is useful to have seen a scaling operation constructed independently.

3.4.7. k-th powers for $k \in \mathbb{N}$

Similarly to Definition 3.4.18, we can define what it means to take the k-th power of a residue class in $\mathbb{Z}/n$, when k is a nonnegative integer.

Definition 3.4.20. Fix $k \in \mathbb{N}$.

For any $\alpha \in \mathbb{Z}/n$, we define a residue class $\alpha^k \in \mathbb{Z}/n$ by setting

$$\left(\left([a]_n\right)^k = \left[a^k\right]_n \qquad \text{for any } a \in \mathbb{Z} \right).$$

(In other words, for any $\alpha \in \mathbb{Z}/n$, we let $\alpha^k = \left[a^k\right]_n$, where a is an integer satisfying $\alpha = [a]_n$.) This is well-defined, because of Proposition 3.4.21 below.

If $\alpha \in \mathbb{Z}/n$, then we shall refer to α^k as the *k-th power* of α.

Proposition 3.4.21. Fix $k \in \mathbb{N}$. For any $\alpha \in \mathbb{Z}/n$, the residue class $\alpha^k \in \mathbb{Z}/n$ in Definition 3.4.20 is well-defined.

3.4.8. Rules and properties for the operations

Convention 3.4.22. We shall follow the usual "PEMDAS" rules for the order of operations when interpreting expressions involving the operations defined in Definition 3.4.12, Definition 3.4.18 and Definition 3.4.20[38]. Thus, for example, the expression "$\alpha \cdot \beta + \gamma \cdot \delta$" means $(\alpha \cdot \beta) + (\gamma \cdot \delta)$ and not $\alpha \cdot (\beta + \gamma) \cdot \delta$. Likewise, the expression "$\alpha\beta^k + r\gamma$" (with $r \in \mathbb{Z}$) should be understood as "$\left(\alpha \left(\beta^k\right)\right) + (r\gamma)$" and not in any other way.

We shall now study some properties of the many "arithmetical" operations we have defined on $\mathbb{Z}/n$.

Theorem 3.4.23. The following rules for addition, subtraction, multiplication and scaling in $\mathbb{Z}/n$ hold:

(a) We have $\alpha + \beta = \beta + \alpha$ for any $\alpha, \beta \in \mathbb{Z}/n$.

(b) We have $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{Z}/n$.

(c) We have $\alpha + [0]_n = [0]_n + \alpha = \alpha$ for any $\alpha \in \mathbb{Z}/n$.

(d) We have $\alpha \cdot [1]_n = [1]_n \cdot \alpha = \alpha$ for any $\alpha \in \mathbb{Z}/n$.

(e) We have $\alpha \cdot \beta = \beta \cdot \alpha$ for any $\alpha, \beta \in \mathbb{Z}/n$.

(f) We have $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{Z}/n$.

(g) We have $\alpha \cdot (\beta + \gamma) = \alpha\beta + \alpha\gamma$ and $(\alpha + \beta) \cdot \gamma = \alpha\gamma + \beta\gamma$ for any $\alpha, \beta, \gamma \in \mathbb{Z}/n$.

(h) We have $\alpha \cdot [0]_n = [0]_n \cdot \alpha = [0]_n$ for any $\alpha \in \mathbb{Z}/n$.

(i) If $\alpha, \beta, \gamma \in \mathbb{Z}/n$, then we have the equivalence $(\alpha - \beta = \gamma) \iff (\alpha = \beta + \gamma)$.

(j) We have $r(\alpha + \beta) = r\alpha + r\beta$ for any $r \in \mathbb{Z}$ and $\alpha, \beta \in \mathbb{Z}/n$.

(k) We have $(r + s)\alpha = r\alpha + s\alpha$ for any $r, s \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}/n$.

(l) We have $r(s\alpha) = (rs)\alpha$ for any $r, s \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}/n$.

(m) We have $r(\alpha\beta) = (r\alpha)\beta = \alpha(r\beta)$ for any $r \in \mathbb{Z}$ and $\alpha, \beta \in \mathbb{Z}/n$.

(n) We have $-(r\alpha) = (-r)\alpha = r(-\alpha)$ for any $r \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}/n$.

(o) We have $1\alpha = \alpha$ for any $\alpha \in \mathbb{Z}/n$.

(p) We have $(-1)\alpha = -\alpha$ for any $\alpha \in \mathbb{Z}/n$.

(q) We have $-(\alpha + \beta) = (-\alpha) + (-\beta)$ for any $\alpha, \beta \in \mathbb{Z}/n$.

(r) We have $-[0]_n = [0]_n$.

(s) We have $-(-\alpha) = \alpha$ for any $\alpha \in \mathbb{Z}/n$.

(t) We have $-(\alpha\beta) = (-\alpha)\beta = \alpha(-\beta)$ for any $\alpha, \beta \in \mathbb{Z}/n$.

(u) We have $\alpha - \beta - \gamma = \alpha - (\beta + \gamma)$ for any $\alpha, \beta, \gamma \in \mathbb{Z}/n$. (Here and in the following, "$\alpha - \beta - \gamma$" should be read as "$(\alpha - \beta) - \gamma$".)

These properties should all look familiar, as they mirror the classical properties of the arithmetic operations on integers, rational numbers and real numbers (with the caveat that the residue classes $[0]_n$ and $[1]_n$ take on the roles of the numbers 0 and 1). For example, Theorem 3.4.23 **(g)** corresponds to the laws of distributivity for numbers. Parts **(a)**, **(b)**, **(c)**, **(i)**, **(j)**, **(k)**, **(l)** and **(o)** of Theorem 3.4.23 furthermore are reminiscent of the axioms for a vector space (with the caveat that scaling by r is only defined for integers r here, so $\mathbb{Z}/n$ is not precisely a vector space).

Recall the concept of a finite sum of integers (i.e., a sum of the form $\sum_{i \in I} a_i$, where I is a finite set and a_i is an integer for each $i \in I$), and the analogous concept of a finite product of integers (i.e., a product of the form $\prod_{i \in I} a_i$). These concepts are defined recursively[39] and satisfy various rules[40]. See [Grinbe15, §1.4] for a

[39] See [Grinbe15, §1.4.1 and §1.4.3] for their definitions, and [Grinbe15, §2.14] for a proof that these are well-defined.

[40] such as $\sum_{i \in I} (a_i + b_i) = \sum_{i \in I} a_i + \sum_{i \in I} b_i$ (where a_i and b_i are two integers for each $i \in I$) or $\sum_{i \in I} a_i = \sum_{i \in J} a_i + \sum_{i \in I \setminus J} a_i$ (where J is a subset of I)

comprehensive list of these rules and [Grinbe15, §2.14] for their proofs.

Definition 3.4.24. In the same vein, we define the concept of a finite sum of residue classes in $\mathbb{Z}/n$ (i.e., a sum of the form $\sum_{i\in I} \alpha_i$, where I is a finite set and $\alpha_i \in \mathbb{Z}/n$ for each $i \in I$), and the analogous concept of a finite product of residue classes in $\mathbb{Z}/n$ (i.e., a product of the form $\prod_{i\in I} \alpha_i$, where I is a finite set and $\alpha_i \in \mathbb{Z}/n$ for each $i \in I$).

More precisely, the concept of a finite sum $\sum_{i\in I} \alpha_i$ (with I being a finite set, and with $\alpha_i \in \mathbb{Z}/n$ for each $i \in I$) is defined recursively as follows:

- If the set I is empty (that is, $|I| = 0$), then $\sum_{i\in I} \alpha_i$ is defined to be $[0]_n \in \mathbb{Z}/n$ (and called an empty sum).
- Otherwise, we pick an arbitrary element $t \in I$, and set

$$\sum_{i\in I} \alpha_i = \alpha_t + \sum_{i\in I\setminus\{t\}} \alpha_i.$$

  (The sum $\sum_{i\in I\setminus\{t\}} \alpha_i$ on the right hand side is a sum over a smaller set than I, whence we can assume it to already be defined in this recursive definition.)

This definition is well-defined (i.e., the choice of element t does not influence the final value of the sum), by Proposition 3.4.25 **(a)** below.

The concept of a finite product $\prod_{i\in I} \alpha_i$ is defined similarly, except that we use multiplication instead of addition (and we define the empty product to be $[1]_n$ instead of $[0]_n$).

We will use the usual shorthands for special kinds of finite sums and products. For example, if I is an interval $\{p, p+1, \ldots, q\}$ of integers (and if $\alpha_i \in \mathbb{Z}/n$ for each $i \in I$), then the sum $\sum_{i\in I} \alpha_i$ will also be denoted by $\sum_{i=p}^{q} \alpha_i$ or $\alpha_p + \alpha_{p+1} + \cdots + \alpha_q$. Likewise for products. Thus, for example, $\alpha_1 + \alpha_2 + \cdots + \alpha_k$ and $\alpha_1\alpha_2\cdots\alpha_k$ are well-defined whenever $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{Z}/n$.

Proposition 3.4.25. **(a)** Definition 3.4.24 is well-defined.

(b) Finite sums ($\sum_{i\in I} \alpha_i$) and finite products ($\prod_{i\in I} \alpha_i$) of elements $\alpha_i \in \mathbb{Z}/n$ satisfy the same rules that finite sums and finite products of integers satisfy.

(c) If $a_1, a_2, \ldots, a_k$ are k integers, then

$$[a_1]_n + [a_2]_n + \cdots + [a_k]_n = [a_1 + a_2 + \cdots + a_k]_n \qquad \text{and}$$
$$[a_1]_n \cdot [a_2]_n \cdot \cdots \cdot [a_k]_n = [a_1 a_2 \cdots a_k]_n .$$

Also, the standard rules for exponents apply to residue classes:

Theorem 3.4.26. **(a)** We have $\alpha^0 = [1]_n$ for any $\alpha \in \mathbb{Z}/n$.
(b) We have $\alpha^1 = \alpha$ for any $\alpha \in \mathbb{Z}/n$.
(c) We have $\alpha^k = \underbrace{\alpha\alpha\cdots\alpha}_{k \text{ times}}$ for any $\alpha \in \mathbb{Z}/n$ and $k \in \mathbb{N}$.
(d) We have $\alpha^{u+v} = \alpha^u \alpha^v$ for any $\alpha \in \mathbb{Z}/n$ and any $u, v \in \mathbb{N}$.
(e) We have $(\alpha\beta)^k = \alpha^k \beta^k$ for any $\alpha, \beta \in \mathbb{Z}/n$ and $k \in \mathbb{N}$.
(f) We have $(\alpha^u)^v = \alpha^{uv}$ for any $\alpha \in \mathbb{Z}/n$ and any $u, v \in \mathbb{N}$.

Also, the binomial formula holds for residue classes:

Theorem 3.4.27. Let $\alpha, \beta \in \mathbb{Z}/n$ and $m \in \mathbb{N}$. Then,

$$(\alpha+\beta)^m = \sum_{k=0}^{m} \binom{m}{k} \alpha^k \beta^{m-k}.$$

3.5. Modular inverses revisited

Convention 3.5.1. For the whole Section 3.5, we fix a positive integer n.

In this section, we will see how modular inverses become actual inverses when we consider residue classes instead of numbers.

Recall that if a is an integer, then an *inverse of a in $\mathbb{Z}$* means an integer $a' \in \mathbb{Z}$ satisfying $aa' = 1$. The only two integers that have an inverse in $\mathbb{Z}$ are 1 and -1. The integer 1 has only one inverse (namely, itself). The integer -1 has only one inverse (namely, itself). Thus, "inverse in $\mathbb{Z}$" is not a very interesting notion.

Let us now define an analogous notion for $\mathbb{Z}/n$:

Definition 3.5.2. Let $\alpha \in \mathbb{Z}/n$. An *inverse* of α means an $\alpha' \in \mathbb{Z}/n$ such that $\alpha \cdot \alpha' = [1]_n$.

For example, $[2]_5$ is an inverse of $[3]_5$ for $n = 5$, since $[3]_5 \cdot [2]_5 = [3 \cdot 2]_5 = [6]_5 = [1]_5$.

It turns out that inverses of residue classes $\alpha \in \mathbb{Z}/n$ exist much more frequently than inverses of integers in $\mathbb{Z}$:

Proposition 3.5.3. Let $a \in \mathbb{Z}$.
(a) If $[a]_n \in \mathbb{Z}/n$ has an inverse, then $a \perp n$.
(b) If $a \perp n$, then $[a]_n \in \mathbb{Z}/n$ has a unique inverse.

As we will see in the proof of this proposition, the inverse of a residue class $[a]_n$ is simply the residue class $[a']_n$ of a modular inverse a' of a modulo n; thus, the

existence part of Proposition 3.5.3 **(b)** (i.e., the claim that $[a]_n$ has an inverse) is just Theorem 2.10.8 **(b)** in disguise. However, before we start proving Proposition 3.5.3, let us state the uniqueness part (i.e., the claim that the inverse of $[a]_n$ is unique) as a separate fact:

Proposition 3.5.4. Let $\alpha \in \mathbb{Z}/n$. Then, α has **at most one** inverse.

Note that in the above proof of Proposition 3.5.4, we have never had to pick a representative of the residue class α (nor of any other class). This is because this proof is actually an instance of a much more general argument. And indeed, you might recall that a very similar argument is used to prove the classical facts that

- a map has at most one inverse;
- a matrix has at most one inverse.

To be more precise, the proofs of these two facts differ slightly from our proof of Proposition 3.5.4, because the definitions of an inverse of a map and of an inverse of a matrix differ from Definition 3.5.2. Indeed, in Definition 3.5.2, we have only required the inverse α' of $\alpha \in \mathbb{Z}/n$ to satisfy the **single** equation $\alpha \cdot \alpha' = [1]_n$, whereas an inverse g of a map f is required to satisfy the **two** equations $f \circ g = \mathrm{id}$ and $g \circ f = \mathrm{id}$ (and likewise, an inverse B of a matrix A is required to satisfy the **two** equations $AB = I$ and $BA = I$ for the appropriate identity matrices I). But this difference is not substantial: The multiplication of residue classes in $\mathbb{Z}/n$ is commutative (by Theorem 3.4.23 **(e)**) (unlike the composition of maps or the multiplication of matrices); thus, the single equation $\alpha \cdot \alpha' = [1]_n$ automatically implies $\alpha' \cdot \alpha = [1]_n$. Hence, we could have as well required α' to satisfy both equations $\alpha \cdot \alpha' = [1]_n$ and $\alpha' \cdot \alpha = [1]_n$ in Definition 3.5.2, and nothing would change.

Let us now prove Proposition 3.5.3:

Corollary 3.5.5. Let U_n be the set of all residue classes $\alpha \in \mathbb{Z}/n$ that have an inverse. Then:
(a) For an integer a, we have the logical equivalence $([a]_n \in U_n) \iff (a \perp n)$.
(b) We have $|U_n| = \phi(n)$.

Definition 3.5.6. Let $\alpha \in \mathbb{Z}/n$ be a residue class that has an inverse. Then, Proposition 3.5.4 shows that α has **a unique** inverse. This inverse can thus be called "**the** *inverse*" of α; it will be denoted by α^{-1}.

For example, $([3]_5)^{-1} = [2]_5$ for $n = 5$, since $[2]_5$ is an inverse (and thus **the** inverse) of $[3]_5$.

Let us state a couple properties of inverses in $\mathbb{Z}/n$:

Exercise 3.5.1. (a) Let $\alpha \in \mathbb{Z}/n$ be a residue class that has an inverse. Prove that its inverse α^{-1} has an inverse as well, and this inverse is $\left(\alpha^{-1}\right)^{-1} = \alpha$.

(b) Let $\alpha, \beta \in \mathbb{Z}/n$ be two residue classes that have inverses. Prove that their product $\alpha\beta$ has an inverse as well, and this inverse is $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$.

The concept of inverses in $\mathbb{Z}/n$ lets us prove Theorem 2.15.7 (Wilson's theorem) again – or, rather, restate our previous proof of Theorem 2.15.7 in more natural terms:

3.6. The Chinese Remainder Theorem as a bijection between residue classes

Definition 3.6.1. Let n be a positive integer. Let d be a positive divisor of n. Then, define the map

$$\begin{aligned} \pi_{n,d} : \mathbb{Z}/n &\to \mathbb{Z}/d, \\ [s]_n &\mapsto [s]_d . \end{aligned}$$

(This is well-defined, according to Proposition 3.4.10.)

See Example 3.4.11 **(a)** for what this map looks like.

We can now state another version of the "Chinese Remainder Theorem", which claims the existence of a certain bijection. We have already seen such a version (Theorem 2.16.1), but that one claimed a bijection between two sets of **remainders**, whereas the following version claims a bijection between two sets of **residue classes**. Other than that, the two versions are rather similar.

Theorem 3.6.2. Let m and n be two coprime positive integers. Then, the map

$$\begin{aligned} S_{m,n} : \mathbb{Z}/(mn) &\to (\mathbb{Z}/m) \times (\mathbb{Z}/n), \\ \alpha &\mapsto (\pi_{mn,m}(\alpha), \pi_{mn,n}(\alpha)) \end{aligned}$$

is well-defined and is a bijection. It sends each $[s]_{mn}$ (with $s \in \mathbb{Z}$) to the pair $([s]_m, [s]_n)$.

Example 3.6.3. (a) Theorem 3.6.2 (applied to $m = 3$ and $n = 2$) says that the map

$$\begin{aligned} S_{3,2} : \mathbb{Z}/6 &\to (\mathbb{Z}/3) \times (\mathbb{Z}/2), \\ \alpha &\mapsto (\pi_{6,3}(\alpha), \pi_{6,2}(\alpha)) \end{aligned}$$

is a bijection. This map sends

$$\begin{array}{cccccc} [0]_6, & [1]_6, & [2]_6, & [3]_6, & [4]_6, & [5]_6 \\ ([0]_3, [0]_2), & ([1]_3, [1]_2), & ([2]_3, [2]_2), & ([3]_3, [3]_2), & ([4]_3, [4]_2), & ([5]_3, [5]_2), \end{array} \quad \text{to}$$

respectively. In other words, it sends

$$\begin{array}{cccccc} [0]_6, & [1]_6, & [2]_6, & [3]_6, & [4]_6, & [5]_6 \\ ([0]_3, [0]_2), & ([1]_3, [1]_2), & ([2]_3, [0]_2), & ([0]_3, [1]_2), & ([1]_3, [0]_2), & ([2]_3, [1]_2), \end{array} \quad \text{to}$$

respectively (since $[2]_2 = [0]_2$ and $[3]_3 = [0]_3$ and $[3]_2 = [1]_2$ and so on). This list of values shows that this map is bijective (since it takes on every possible value in $(\mathbb{Z}/3) \times (\mathbb{Z}/2)$ exactly once). Theorem 3.6.2 says that this holds for arbitrary coprime m and n.

(b) Let us see how Theorem 3.6.2 fails when m and n are **not** coprime. For example, take $m = 6$ and $n = 4$. Then, the map

$$\begin{aligned} S_{6,4} : \mathbb{Z}/24 &\to (\mathbb{Z}/6) \times (\mathbb{Z}/4), \\ \alpha &\mapsto (\pi_{24,6}(\alpha), \pi_{24,4}(\alpha)) \end{aligned}$$

is **not** a bijection. Indeed, it is neither injective (for example, it sends both $[0]_{24}$ and $[12]_{24}$ to the same pair $([0]_6, [0]_4)$) nor surjective (for example, it never takes the value $([1]_6, [2]_4)$).

The following proof of Theorem 3.6.2 has the same structure as our proof of Theorem 2.16.1 above, but is shorter since residue classes are easier to deal with than remainders.

We have already proven Theorem 2.14.4 using Theorem 2.16.1. Let us now reprove it using Theorem 3.6.2 instead (by a rather similar argument, but using residue classes instead of remainders):

3.7. Substitutivity and chains of congruences revisited

Proposition 3.4.5 **(b)** can be stated as follows: Given an integer n, two integers a and b are congruent to each other modulo n if and only if their residue classes $[a]_n$ and $[b]_n$ are equal. This lets us see congruences modulo n in a new light (namely, as equalities). In particular, some previous results about congruences now become trivial. For example, we can obtain a very short proof of Proposition 2.4.5 using residue classes:

We can also prove the Principle of substitutivity of congruences (which we informally stated in Section 2.5, and abbreviated as "PSC"):

3.8. A couple of applications of elementary number theory

In the following short section, we shall see two practical applications of the above number-theoretical studies. The first is a method for encrypting information (the RSA cryptosystem); the second is a trick by which computations with large integers can be split up into more manageable pieces (and distributed across several

computers, or parallelized across several cores). We shall be brief, since applications are not a focus of these notes; for further details, see [GalQua17] and the MathOverflow answer `https://mathoverflow.net/a/10022/` . If you are interested in further applications, you may also want to consult the other answers to `https://mathoverflow.net/questions/10014` (for a list of uses of the Chinese Remainder Theorem – mostly, but not entirely, inside mathematics), as well as [UspHea39, Appendix to Chapter VII] (for applications of modular arithmetic to calendar computations), and the Wikipedia page on "Universal hashing" (for an application of residue classes modulo primes).

3.8.1. The RSA cryptosystem

Let us present the *RSA cryptosystem*. This is one of the first modern methods for encrypting data. (The name "RSA" stands for the initials of its three authors: Rivest, Shamir and Adleman.)

This cryptosystem addresses a fairly standard situation: Albert and Julia are communicating over a channel (e.g., the Internet), but the channel may have eavesdroppers. Julia wants to send a secret message to Albert over this channel – i.e., a message that eavesdroppers should not be able to understand[41]. But Albert and Julia have not exchanged any keys with each other in advance; they can start exchanging keys now, but the eavesdropper will know all the keys they are sending each other. How can Albert and Julia start secretly communicating without giving eavesdroppers all the information they want to give each other?

The RSA cryptosystem allows Albert and Julia to solve this problem as follows:

Setup:

- Julia tells Albert (openly, over the channel) that she wants to communicate and thus he should start creating keys for that purpose.
- Albert generates two distinct large and sufficiently random primes p and q. (This involves a lot of technicalities like actually finding large primes. See Keith Conrad's note *The Solovay-Strassen test* [Conrad*] for an algorithm for generating large primes[42], and [GalQua17] for a more comprehensive treat-

[41] We assume that Julia is merely trying to keep the **content** of her message secret from the eavesdroppers; the eavesdroppers can still see **that she is sending something to Albert**. If Albert and Julia want to keep even this fact secret, they need a different branch of science – *steganography*, not cryptography. (For reasons that become obvious after a bit of thought, steganography is much less of an exact science than cryptography, and depends heavily on the real-life situation.)

[42] More precisely, the Solovay-Strassen test is an algorithm for checking (not with 100% surety, but with high probability, which suffices in practice) whether a given integer is prime. To make this into an algorithm for generating large primes, you can simply keep randomly picking large numbers until you hit one that is prime (which you can check using the Solovay–Strassen test). This doesn't take **too** long, because the prime number theorem says that (very roughly speaking!) the probability for a k-digit number to be prime is $\approx 1/k$. (A precise statement of this result would require us to introduce notions that have nothing to do with algebra; it is commonly done

ment. A brief discussion is also found in Garrett's slides [Garret03]. As to what "large" means, we refer to the Wikipedia article on "key size".)

- Albert computes the positive integer $m = pq$. This number m (called the *modulus*) he makes public (i.e., sends to Julia over the channel). (Note that factoring a number into a product of primes is computationally a lot harder than multiplying a bunch of primes[43]. Thus, eavesdroppers will not (likely) be able to reconstruct the primes p and q from their (public) product m.)

- Albert computes the positive integer $\ell = (p-1)(q-1)$, but keeps this number private.

- Albert randomly picks an $e \in \{2, 3, \ldots, \ell - 1\}$ such that $e \perp \ell$. (Again, we omit the details of how to pick such an e randomly[44].) This number e will be called the *encryption key*, and Albert keeps it private.

- Albert computes a positive modular inverse d of e modulo ℓ (that is, a positive integer d such that $ed \equiv 1 \bmod \ell$). This number d exists by Theorem 2.10.8 **(b)**; it will be called the *decryption key*.

- Albert publishes the pair (e, m) as his *public key*.

- We assume that the message that Julia wants to send to Albert is an element of $\{0, 1, \ldots, m-1\}$. This assumption is perfectly reasonable, because this message originally exists in **some** digital form (e.g., as a bitstring), and it is easy to translate it from this form into an element of $\{0, 1, \ldots, m-1\}$ by some universally agreed rule (e.g., if a bitstring $(a_1, a_2, \ldots, a_k)$ is short enough, then the integer $a_1 2^{k-1} + a_2 2^{k-2} + \cdots + a_k 2^{k-k}$ will belong to $\{0, 1, \ldots, m-1\}$, and thus we can translate this bitstring into this latter integer; otherwise, we break it up into shorter chunks and send those as separate messages).

Encrypting a message:
If Julia wants to send a message $a \in \{0, 1, \ldots, m-1\}$ to Albert, then she does the following:

- She computes the residue class $\alpha := [a]_m \in \mathbb{Z}/m$.

in courses on *analytic number theory*. Needless to say, it is perfectly possible to profit from this result in practice without proving it.)

[43] See the Wikipedia page on "Integer factorization" for details on what this means. Note that this is not a proven theorem; any day, someone could come up with a quick algorithm for factoring integers into products of primes. You would hear about it in the news, though.

[44] The rough idea is "pick $e \in \{2, 3, \ldots, \ell - 1\}$ randomly; check (using the Euclidean algorithm) whether $e \perp \ell$; if not, then pick another e, and keep repeating this until you hit an e such that $e \perp \ell$". In theory, you could be unlucky and keep picking bad e's forever; but in reality, you will soon hit an e that satisfies $e \perp \ell$.

- She computes α^e in $\mathbb{Z}/m$. (This can be computed quickly using *binary exponentiation (also known as exponentiation by squaring)*: If $\beta \in \mathbb{Z}/m$, then all powers of β can be computed recursively via the formulas $\beta^{2k} = \left(\beta^k\right)^2$ and $\beta^{2k+1} = \left(\beta^k\right)^2 \beta$. Note that we are working with residue classes in $\mathbb{Z}/m$ here, not with integers, so that the powers β^k of β will not grow forever as k gets large; they stay in the finite set $\mathbb{Z}/m$.)
- She sends the residue class α^e (or, more precisely, its unique representative in the set $\{0, 1, \ldots, m-1\}$ [45]) to Albert.

Decrypting a message:
Albert receives the residue class $\beta = \alpha^e$ (or, more precisely, a representative thereof, which he can easily turn into the residue class), and recovers the original message a as follows:

- He sets $\gamma = \beta^d$. This γ is the same α that Julia computed, as we shall see below.
- He recovers the original message $a \in \{0, 1, \ldots, m-1\}$ as the unique representative of the residue class $\gamma = \alpha$ in $\{0, 1, \ldots, m-1\}$ (since Julia defined α as the residue class of a).

This way, Julia can send a message to Albert that no eavesdropper can read – unless said eavesdropper knows d, or possesses an algorithm hitherto unknown to the world, or has an incredibly fast computer, or Albert's randomly picked numbers were not random enough[46], or one of myriad other practical mistakes has been made. The proper implementation of the RSA cryptosystem, and the real-life considerations needed to prevent "leakage" of sensitive data such as the decryption key d, are a subject in its own right, which we shall not discuss here.

[45] This unique representative exists by Proposition 3.4.6 **(b)** (and can be computed by picking an arbitrary representative b first, and then taking its remainder $b\%m$).

[46] Computers cannot generate "truly" random numbers (whatever this would even mean!); thus, you have to get by with number generators which try their best at being unpredictable. Lots of creativity has gone into finding ways to come up with numbers that are "as random as possible". Software alone is, per se, deterministic and thus can at most come up with numbers that "look random" ("pseudorandom number generators"). Nondeterministic input must come from the outside world. This is why certain programs that generate keys ask you to move your mouse around the screen – they are, in fact, using your mouse movements as a source of randomness. Better randomness comes from hardware random number generators, such as Geiger counters or lava lamps.

What happens if your randomly picked prime numbers are not random enough? In the worst case, you never find two distinct primes to begin with. In a more realistic case, your distinct primes will all belong to a small and predictable set, and an eavesdropper can easily find them simply by checking all possibilities. In less obvious cases, different keys you generate for different purposes will occasionally have some primes in common, in which case an easy application of the Chinese Remainder Theorem will allow an eavesdropper to reconstruct them and decrypt your messages. See `https://factorable.net` for a study of RSA keys in the wild, which found a lot of common primes.

Albert's method for recovering Julia's message relies on the following fact (which we shall prove a bit later):

Lemma 3.8.1. Let p and q be two distinct primes. Let N be a positive integer such that $N \equiv 1 \bmod (p-1)(q-1)$. Then:
(a) Each $a \in \mathbb{Z}$ satisfies $a^N \equiv a \bmod pq$.
(b) Each $\alpha \in \mathbb{Z}/(pq)$ satisfies $\alpha^N = \alpha$.

Now, when Albert receives $\beta = \alpha^e$ from Julia, we have

$$\beta^d = (\alpha^e)^d = \alpha^{ed}.$$

But d was a modular inverse of e modulo ℓ; thus, $ed \equiv 1 \bmod \ell$. Since $\ell = (p-1)(q-1)$, we thus have $ed \equiv 1 \bmod (p-1)(q-1)$. Hence, Lemma 3.8.1 **(b)** (applied to $N = ed$) yields $\alpha^{ed} = \alpha$ (since $\alpha \in \mathbb{Z}/\underbrace{m}_{=pq} = \mathbb{Z}/(pq)$). Thus, $\beta^d = \alpha^{ed} = \alpha$. Thus, the residue class $\gamma = \beta^d$ that Albert computes is exactly Julia's α; hence, Albert correctly recovers the message.

The RSA cryptosystem, as presented above, is more versatile than it may seem at first. Once Albert has generated his p, q, ℓ, m, d and e and sent (e, m) to Julia, Julia can send not just one but multiple messages to Albert using these keys. Albert can confidentially respond to these messages as well, by having Julia switch roles with him (i.e., Julia generates keys, Albert encrypts and Julia decrypts). Thus, a secure channel for communication can be established. Moreover, and less obviously, RSA can be used to digitally sign messages (i.e., convince the recipient that they really come from you – or at least from someone who possesses your private key); see, e.g., [Dummit16] or the Wikipedia.

3.8.2. Computing using the Chinese Remainder Theorem

Next, let us outline a simple yet unexpected application of the Chinese Remainder Theorem.

Assume that you have an expression a that is made of integers, addition, subtraction and multiplication. For example, say

$$a = 400 \cdot 405 \cdot 409 \cdot 413 - 401 \cdot 404 \cdot 408 \cdot 414. \tag{31}$$

Assume that computing a directly is too hard, because the intermediate results will be forbiddingly huge numbers, but you know (e.g., from some estimates) that the final result will be a fairly small number. Let's say (for simplicity) that you know that $0 \leq a < 500\,000$.

How can you use this information to compute a quickly?

One simple trick is to work with residue classes modulo 500 000 instead of working with integer. Thus, instead of computing the number a directly through the

equality (31), we can instead compute its residue class

$$\begin{aligned}[a]_{500\ 000} &= [400 \cdot 405 \cdot 409 \cdot 413 - 401 \cdot 404 \cdot 408 \cdot 414]_{500\ 000} \\ &= [400]_{500\ 000} \cdot [405]_{500\ 000} \cdot [409]_{500\ 000} \cdot [413]_{500\ 000} \\ &\qquad - [401]_{500\ 000} \cdot [404]_{500\ 000} \cdot [408]_{500\ 000} \cdot [414]_{500\ 000}\end{aligned}$$

(which is an easier task, because we can always reduce our intermediate results using the fact that every integer a satisfies $[a]_{500\ 000} = [a \ \%\ 500\ 000]_{500\ 000}$), and then recover a by observing that a must be the unique representative of its residue class $[a]_{500\ 000}$ that belongs to $\{0, 1, \ldots, 499\ 999\}$ (since $0 \leq a < 500\ 000$). This is actually how integer arithmetic works in most low-level programming languages; for example, the most popular integer type of the C++ language is "`int`", which stands not for integers but rather for residue classes modulo 2^{64} (when working on a 64-bit system). (This is where integer overflow comes from.)

Computing $[a]_{500\ 000}$ instead of computing a is already an improvement, but in practice, the "500 000" might actually be a significantly bigger number. Assume, for example, that instead of $0 \leq a < 500\ 000$, you merely know that $0 \leq a < N$ for some fixed number N which is small enough that computing in $\mathbb{Z}/N$ is possible, but large enough that doing the **whole** computation of $[a]_N$ in $\mathbb{Z}/N$ is unviable. What can we do then?

One thing we can do is to compute the residue classes $[a]_n$ for several coprime "small" integers n. For example, we can compute $[a]_2$ (by performing the whole computation of a using residue classes modulo 2 instead of integers) and similarly $[a]_3$ and $[a]_5$ and $[a]_7$ etc.. (We are using prime numbers for n here, which has certain advantages, but is not strictly necessary; all we need is that the values of n we are using are coprime.[47])

The Chinese Remainder Theorem (in the form of Theorem 3.6.2) shows that if m and n are two coprime positive integers, then the map $S_{m,n}$ from Theorem 3.6.2 (sending each $[s]_{mn}$ to the pair $([s]_m, [s]_n)$) is a bijection. In our proof of Theorem 3.6.2 (when proving the surjectivity of $S_{m,n}$), we gave an explicit way of constructing preimages under this map $S_{m,n}$ (using Bezout's theorem, which has a fast algorithm underlying it – the Extended Euclidean algorithm). Thus, we have an explicit way of recovering the residue class $[s]_{mn}$ from the pair $([s]_m, [s]_n)$ whenever s is an (unknown) integer (and m and n are two coprime positive integers). We shall now refer to this way as the "patching procedure" (since it lets us "patch" two residue classes $[s]_m$ and $[s]_n$ together to a residue class $[s]_{mn}$).

Now, having computed a bunch of residue classes $[a]_2, [a]_3, [a]_5, [a]_7$ of our unknown integer a modulo coprime small integers, we can "patch" these classes together:

- From $[a]_2$ and $[a]_3$, we get $[a]_{2\cdot 3}$ by the "patching procedure".
- From $[a]_{2\cdot 3}$ and $[a]_5$, we get $[a]_{2\cdot 3\cdot 5}$ by the "patching procedure".

[47] Note that the computations of $[a]_n$ for different values of n are independent of each other, which comes handy if you have several processors.

- From $[a]_{2\cdot 3\cdot 5}$ and $[a]_7$, we get $[a]_{2\cdot 3\cdot 5\cdot 7}$ by the "patching procedure".
- and so on.

We keep "patching" until the product $2 \cdot 3 \cdot 5 \cdot 7 \cdot \cdots$ becomes larger than our N (which will happen fairly soon, since this product grows super-exponentially with the number of "patching" steps). At that point, we have found the residue class $[a]_m$ of our unknown integer a modulo some integer $m > N$. Since $0 \leq a < N < m$, we can thus recover a itself (as the unique representative of the class $[a]_m$ that lies in the set $\{0, 1, \ldots, m-1\}$).

This technique is known as *Chinese Remaindering* (in its simplest form) and has been used a lot (for an example, see [Vogan07, pp. 1031–1033]). See [Knuth98, §4.3.2] for more details.

3.9. Primitive roots: an introduction

3.9.1. Definition and examples

Let us finally discuss a kind of residue classes that come very useful when they exist: the *primitive roots* (modulo a positive integer n). We are not yet able to ascertain when they exist and when they don't (this will require some more abstract algebra); but we can already see some examples of them:

Convention 3.9.1. For the whole Subsection 3.9.1, we fix a positive integer n.

Definition 3.9.2. Let $\alpha \in \mathbb{Z}/n$ be a residue class.
(a) We say that α is *invertible* if α has an inverse.
(b) A *power of* α means a residue class of the form α^m for some $m \in \mathbb{N}$.
(c) Assume that α is invertible. Then, α is said to be a *primitive root modulo* n if every invertible residue class $\beta \in \mathbb{Z}/n$ is a power of α.

Example 3.9.3. Let $n = 9$. The invertible residue classes in $\mathbb{Z}/9$ are $[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9$.

Clearly, the residue class $[1]_9$ is not a primitive root modulo 9, since all its powers equal $[1]_9$.

The powers of $[2]_9$ are

$$\begin{aligned}
([2]_9)^0 &= [1]_9, \\
([2]_9)^1 &= [2]_9, \\
([2]_9)^2 &= [4]_9, \\
([2]_9)^3 &= [8]_9, \\
([2]_9)^4 &= [7]_9, \\
([2]_9)^5 &= [5]_9, \\
&\ldots.
\end{aligned}$$

[48] Thus, they cover all the six invertible residue classes $[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9$. Hence, $[2]_9$ is a primitive root modulo 9.

It is easy to see that $[5]_9$ also is a primitive root modulo 9, and these two primitive roots are the only ones.

Note that Corollary 3.5.5 **(b)** shows that there are exactly $\phi(n)$ invertible residue classes in $\mathbb{Z}/n$. It is easy to see that any power of an invertible residue class is again invertible.

Euler's theorem (Theorem 2.15.3) yields that if $\alpha \in \mathbb{Z}/n$ is an invertible residue class, then $\alpha^{\phi(n)} = [1]_n$ (because Corollary 3.5.5 **(a)** shows that α can be written in the form $\alpha = [a]_n$ for some integer a satisfying $a \perp n$). Thus, it is easy to see that an invertible residue class $\alpha \in \mathbb{Z}/n$ has at most $\phi(n)$ distinct powers. When an invertible residue class $\alpha \in \mathbb{Z}/n$ has **exactly** $\phi(n)$ distinct powers, it is a primitive root (since there are exactly $\phi(n)$ invertible residue classes in $\mathbb{Z}/n$).

Example 3.9.4. Let $n = 8$. The invertible residue classes in $\mathbb{Z}/8$ are $[1]_8, [3]_8, [5]_8, [7]_8$.

Again, $[1]_8$ is certainly not a primitive root.

The powers of $[3]_8$ are

$$\begin{aligned} ([3]_8)^0 &= [1]_8, \\ ([3]_8)^1 &= [3]_8, \\ ([3]_8)^2 &= [9]_8 = [1]_8, \\ &\cdots \end{aligned}$$

[48] Here is a fast way to compute these powers:

$$\begin{aligned} ([2]_9)^0 &= [1]_9, \\ ([2]_9)^1 &= [2]_9, \\ ([2]_9)^2 &= \left[\underbrace{2^2}_{=4}\right]_9 = [4]_9, \\ ([2]_9)^3 &= \left[\underbrace{2^3}_{=8}\right]_9 = [8]_9, \\ ([2]_9)^4 &= \left[\underbrace{2^4}_{=16}\right]_9 = [16]_9 = [7]_9 \qquad (\text{since } 16 \equiv 7 \bmod 9), \\ ([2]_9)^5 &= [2]_9 \cdot \underbrace{([2]_9)^4}_{=[7]_9} = [2]_9 \cdot [7]_9 = \left[\underbrace{2 \cdot 7}_{=14}\right]_9 = [14]_9 = [5]_9 \qquad (\text{since } 14 \equiv 5 \bmod 9), \\ &\cdots. \end{aligned}$$

(so the even powers are $[1]_8$ and the odd powers are $[3]_8$). So $[3]_8$ is not a primitive root.

The same behavior prevents $[5]_8$ and $[7]_8$ from being primitive roots.

Thus, we see that there are no primitive roots modulo 8.

Examples 3.9.4 and 3.9.3 suggest the following questions: For what n does a primitive root modulo n exist, and when it does, how many of them are there? The following theorem – a result proven in 1801 by Gauss – answers both of these questions:

Theorem 3.9.5. **(a)** A primitive root modulo n exists if and only if n is

- either 1,
- or a prime p,
- or a power p^k of an odd prime[49] p (with k being a positive integer),
- or 4,
- or $2p^k$ for an odd prime p (with k being a positive integer).

(b) If a primitive root modulo n exists, then there are precisely $\phi(\phi(n))$ many of them.

This theorem would be fairly difficult to prove at this point, but will be doable with some abstract algebra (at least in the case $n = p$). See [GalQua17, Chapter 4] for a proof.

4. Complex numbers and Gaussian integers

4.1. Complex numbers

4.1.1. An informal introduction

We now leave (at least for the time being) the study of integers and proceed to consider a much larger "number system": the *complex numbers*.

Before we define these numbers rigorously, let me sketch the idea behind their construction. Please suspend your disbelief about the not-quite-kosher reasoning that will follow; we will return to rigorous mathematics in Definition 4.1.1 below.

We know that the number -1 (like any other negative number) has no square root in $\mathbb{R}$ (because the square of any real number is ≥ 0). But let us audaciously pretend that it does have a square root somewhere else. In other words, let us pretend that there exists a mythical "number" i such that $i^2 = -1$. Of course, such

[49] Recall: Odd primes are the same as primes $\neq 2$.

a "number" i will not be a real number, but let us assume (without real justification, for now) that it behaves like a usual number would (to some extent). In particular, let us assume that it can be added, subtracted and multiplied like the numbers that we know and love.

So we have extended the set $\mathbb{R}$ of real numbers by a new number i. Now, by applying addition, subtraction and multiplication to this new number (and our old numbers), we get a bunch of further new numbers – namely, all numbers of the form $a_0 + a_1 i + a_2 i^2 + \cdots + a_k i^k$, where $k \in \mathbb{N}$ and where $a_0, a_1, \ldots, a_k$ are real numbers. (These can be described as the polynomials in i with real coefficients.) However, some of these numbers will be equal; in fact, any number of this form can be reduced to a number of the form $a + bi$ (with $a, b \in \mathbb{R}$), because[50]

$$i^2 = -1, \qquad i^3 = i\underbrace{i^2}_{=-1} = -i, \qquad i^4 = i\underbrace{i^3}_{=-i} = -\underbrace{i^2}_{=-1} = -(-1) = 1,$$
$$i^5 = i\underbrace{i^4}_{=1} = i, \qquad \text{etc..}$$

For example, the number $3 + 5i + 9i^2 + 7i^3$ equals $3 + 5i + 9(-1) + 7(-i) = (3-9) + (5-7)i = -6 - 2i$.

So all our new numbers have the form $a + bi$ for two reals a and b. We call them "complex numbers". (As we have said, we will give a rigorous definition later.) Since we are assuming that the standard rules of arithmetic still hold for our new numbers, we can easily find formulas for computing the sum, the difference, the product and the quotient of two complex numbers written in the form $a + bi$: Namely, for any two complex numbers $a + bi$ and $c + di$ (with $a, b, c, d \in \mathbb{R}$), we have

$$(a+bi) + (c+di) = (a+c) + (b+d)i; \tag{32}$$
$$(a+bi) - (c+di) = (a-c) + (b-d)i; \tag{33}$$
$$\begin{aligned}(a+bi)(c+di) &= ac + adi + bci + bd\underbrace{i^2}_{=-1} = ac + adi + bci - bd \\ &= (ac-bd) + (ad+bc)i; \end{aligned} \tag{34}$$
$$\begin{aligned}\frac{a+bi}{c+di} &= \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac - adi + bci + bdi^2}{cc - cdi + dci - ddi^2} = \frac{ac - adi + bci + bd(-1)}{cc - cdi + dci - dd(-1)} \\ &= \frac{(ac+bd) + (bc-ad)i}{c^2+d^2} \qquad \text{(if } c, d \text{ are not both } 0\text{)}. \end{aligned} \tag{35}$$

(Note that the latter formula is an analogue of the standard procedure for rationalizing denominators that involve square roots:

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{\left(a+b\sqrt{2}\right)\left(c-d\sqrt{2}\right)}{\left(c+d\sqrt{2}\right)\left(c-d\sqrt{2}\right)} = \frac{(ac-2bd) + (bc-ad)\sqrt{2}}{c^2-2d^2},$$

[50] Of course, we are assuming that the standard rules – such as associativity of multiplication – apply to our "new" numbers.

except that the square root that we are trying to exorcise from the denominator is not $\sqrt{2}$ but $\sqrt{-1} = i$ now.)

However, not all features of real numbers carry over to complex numbers: Inequalities do not make sense for complex numbers. Indeed, if they would make sense, then we would get a contradiction as follows:

- If $i \geq 0$, then $i^2 \geq 0$, contradicting $i^2 = -1 < 0$.
- If $i < 0$, then $i^2 = (-i)^2 > 0$ (since $i < 0$ yields $-i > 0$), contradicting $i^2 = -1 < 0$.

Here, we have assumed two things about our relations: First, we have assumed that i is either ≥ 0 or < 0; and second, we have assumed that the square of a nonnegative complex number is nonnegative. Sure, we could avoid the contradiction by forfeiting one of these assumptions; but then, the $\geq$ and $<$ relations would not be worth their names any more.

So we appear to be able to extend the four operations $+, -, \cdot, /$ to our weird new numbers, but not the relations $<, \leq, >, \geq$ (at least not in any meaningful way). But how can we be sure that the four operations $+, -, \cdot, /$ don't already lead to some contradictions?

To answer this question, let us forget our daring postulation of the existence of i, and instead give a formal definition of complex numbers:

4.1.2. Rigorous definition of the complex numbers

Definition 4.1.1. (a) A *complex number* is defined as a pair (a, b) of two real numbers.

(b) We let $\mathbb{C}$ be the set of all complex numbers.

(c) For each real number r, we denote the complex number $(r, 0)$ by $r_{\mathbb{C}}$.

(d) We let i be the complex number $(0, 1)$. When the notation "i" is ambiguous, I will be calling it "$i_{\mathbb{C}}$" instead. (Some authors call it j or ι or $\sqrt{-1}$.)

(e) We define three binary operations $+$, $-$ and $\cdot$ on $\mathbb{C}$ by setting

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d), \\ (a,b) - (c,d) &= (a-c, b-d), \qquad \text{and} \\ (a,b) \cdot (c,d) &= (ac-bd, ad+bc) \end{aligned}$$

for all $(a, b) \in \mathbb{C}$ and $(c, d) \in \mathbb{C}$.

(f) If α and β are two complex numbers, then we write $\alpha\beta$ for $\alpha \cdot \beta$.

(g) If α is a complex number, then the complex number $0_{\mathbb{C}} - \alpha$ shall be denoted by $-\alpha$.

For example, the definition of the operation $\cdot$ on $\mathbb{C}$ yields

$$\underbrace{i}_{=(0,1)} \underbrace{i}_{=(0,1)} = (0,1)(0,1) = \left(\underbrace{0 \cdot 0 - 1 \cdot 1}_{=-1}, \underbrace{0 \cdot 1 + 1 \cdot 0}_{=0} \right) = (-1,0) = (-1)_{\mathbb{C}}.$$

We will later[51] equate the complex number $(-1)_{\mathbb{C}}$ with the real number -1; thus, this equation will simplify to $ii = -1$. So i "behaves like a square root of -1". But we also have $(-i)(-i) = (-1)_{\mathbb{C}}$, so $-i$ fits the same bill. Thus, we didn't have to postulate the existence of a mythical number i satisfying $i^2 = 1$; we simply found such a number in the set $\mathbb{C}$.

The definitions of the operations $+$, $-$ and $\cdot$ in Definition 4.1.1 are not chosen by accident. We shall later identify each complex number (a, b) with $a + bi$; then, these definitions will become exactly the equalities (32), (33) and (34) that we derived unrigorously.

We are leaving division of complex numbers undefined so far, because we will later get it more or less for free.

We shall follow the usual "PEMDAS" rules for the order of operations when interpreting expressions involving the operations $+$, $-$ and $\cdot$ on $\mathbb{C}$. Thus, for example, the expression "$\alpha + \beta \cdot \gamma$" shall mean $\alpha + (\beta \cdot \gamma)$ and not $(\alpha + \beta) \cdot \gamma$.

4.1.3. Rules for $+$, $-$ and $\cdot$

So we have defined complex numbers as pairs of real numbers, and we have defined three operations on them which we called $+$, $-$ and $\cdot$. But do these operations really deserve these names? Do they still behave as nicely as the corresponding operations on real numbers? Do they, in particular, satisfy the standard rules of arithmetic such as commutativity, associativity and distributivity? The next theorem shows that they indeed do:

Theorem 4.1.2. The following rules for addition, subtraction and multiplication in $\mathbb{C}$ hold:

(a) We have $\alpha + \beta = \beta + \alpha$ for any $\alpha, \beta \in \mathbb{C}$.

(b) We have $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{C}$.

(c) We have $\alpha + 0_{\mathbb{C}} = 0_{\mathbb{C}} + \alpha = \alpha$ for any $\alpha \in \mathbb{C}$.

(d) We have $\alpha \cdot 1_{\mathbb{C}} = 1_{\mathbb{C}} \cdot \alpha = \alpha$ for any $\alpha \in \mathbb{C}$.

(e) We have $\alpha \cdot \beta = \beta \cdot \alpha$ for any $\alpha, \beta \in \mathbb{C}$.

(f) We have $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$ for any $\alpha, \beta, \gamma \in \mathbb{C}$.

(g) We have $\alpha \cdot (\beta + \gamma) = \alpha\beta + \alpha\gamma$ and $(\alpha + \beta) \cdot \gamma = \alpha\gamma + \beta\gamma$ for any $\alpha, \beta, \gamma \in \mathbb{C}$.

(h) We have $\alpha \cdot 0_{\mathbb{C}} = 0_{\mathbb{C}} \cdot \alpha = 0_{\mathbb{C}}$ for any $\alpha \in \mathbb{C}$.

(i) If $\alpha, \beta, \gamma \in \mathbb{C}$, then we have the equivalence $(\alpha - \beta = \gamma) \iff (\alpha = \beta + \gamma)$.

(j) We have $-(\alpha + \beta) = (-\alpha) + (-\beta)$ for any $\alpha, \beta \in \mathbb{C}$.

(k) We have $-0_{\mathbb{C}} = 0_{\mathbb{C}}$.

(l) We have $-(-\alpha) = \alpha$ for any $\alpha \in \mathbb{C}$.

(m) We have $-(\alpha\beta) = (-\alpha)\beta = \alpha(-\beta)$ for any $\alpha, \beta \in \mathbb{C}$.

(n) We have $\alpha - \beta - \gamma = \alpha - (\beta + \gamma)$ for any $\alpha, \beta, \gamma \in \mathbb{C}$. (Here and in the following, "$\alpha - \beta - \gamma$" should be read as "$(\alpha - \beta) - \gamma$".)

[51] in Convention 4.1.7

4.1.4. Finite sums and finite products

Recall the concept of a finite sum of real numbers (i.e., a sum of the form $\sum_{i\in I} a_i$, where I is a finite set and a_i is a real number for each $i \in I$), and the analogous concept of a finite product of real numbers (i.e., a product of the form $\prod_{i\in I} a_i$).

Definition 4.1.3. In the same vein, we define the concept of a finite sum of complex numbers (i.e., a sum of the form $\sum_{i\in I} \alpha_i$, where I is a finite set and $\alpha_i \in \mathbb{C}$ for each $i \in I$), and the analogous concept of a finite product of complex numbers (i.e., a product of the form $\prod_{i\in I} \alpha_i$, where I is a finite set and $\alpha_i \in \mathbb{C}$ for each $i \in I$).

These concepts are well-defined, by Proposition 4.1.4 **(a)** below.

We will use the usual shorthands for special kinds of finite sums and products. For example, if I is an interval $\{p, p+1, \ldots, q\}$ of integers (and if $\alpha_i \in \mathbb{C}$ for each $i \in I$), then the sum $\sum_{i\in I} \alpha_i$ will also be denoted by $\sum_{i=p}^{q} \alpha_i$ or $\alpha_p + \alpha_{p+1} + \cdots + \alpha_q$. Likewise for products. Thus, for example, $\alpha_1 + \alpha_2 + \cdots + \alpha_k$ and $\alpha_1\alpha_2\cdots\alpha_k$ are well-defined whenever $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{C}$.

Proposition 4.1.4. **(a)** Definition 4.1.3 is well-defined.

(b) Finite sums ($\sum_{i\in I} \alpha_i$) and finite products ($\prod_{i\in I} \alpha_i$) of complex numbers $\alpha_i \in \mathbb{C}$ satisfy the same rules that finite sums and finite products of real numbers satisfy.

4.1.5. Embedding $\mathbb{R}$ into $\mathbb{C}$

Theorem 4.1.5. For any real numbers a and b, we have

$$(a+b)_{\mathbb{C}} = a_{\mathbb{C}} + b_{\mathbb{C}} \qquad \text{and} \tag{36}$$

$$(a-b)_{\mathbb{C}} = a_{\mathbb{C}} - b_{\mathbb{C}} \qquad \text{and} \tag{37}$$

$$(ab)_{\mathbb{C}} = a_{\mathbb{C}} b_{\mathbb{C}}. \tag{38}$$

Remark 4.1.6. If $a_1, a_2, \ldots, a_k$ are k reals, then

$$(a_1)_{\mathbb{C}} + (a_2)_{\mathbb{C}} + \cdots + (a_k)_{\mathbb{C}} = (a_1 + a_2 + \cdots + a_k)_{\mathbb{C}} \qquad \text{and}$$
$$(a_1)_{\mathbb{C}} \cdot (a_2)_{\mathbb{C}} \cdot \cdots \cdot (a_k)_{\mathbb{C}} = (a_1 a_2 \cdots a_k)_{\mathbb{C}}.$$

Convention 4.1.7. From now on, for each real number r, we shall identify the real number r with the complex number $r_{\mathbb{C}} = (r, 0)$.

Identifying different things is always risky in mathematics; for example, we have seen above why it would be a bad idea to identify residue classes $[a]_n$ of integers modulo a positive integer n with the corresponding remainders $a\%n$ (even though there is a 1-to-1 correspondence between the former and the latter). Nevertheless, the identification made in Convention 4.1.7 is harmless, due to Theorem 4.1.5[52] and because the map

$$\mathbb{R} \to \mathbb{C}, \qquad r \mapsto r_{\mathbb{C}}$$

is injective (so we are not identifying two different real numbers with one and the same complex numbers).

So we have identified each real number with a complex number. Thus, the complex numbers can be seen as an extension of the real numbers: $\mathbb{R} \subseteq \mathbb{C}$. (Of course, this is not **literally** true, since formally speaking $r_{\mathbb{C}}$ is a pair while r is a single real number. Nevertheless, we will work as if this was true, and hope that the reader can insert "$_{\mathbb{C}}$" subscripts wherever necessary in order to make our computations literally true.)

When we defined complex numbers as pairs of real numbers in Definition 4.1.1, we were intending that the pair (a, b) would correspond to the complex number $a + bi$ in our previous informal construction of the complex numbers. Convention 4.1.7 makes this actually hold:

Proposition 4.1.8. For any $(a, b) \in \mathbb{C}$, we have $(a, b) = a + bi$.

The next proposition shows that if we multiply a complex number (b, c) with a **real** number a (of course, understanding this real number a as the complex number $a_{\mathbb{C}} = (a, 0)$), then the result will simply be (ab, ac) (that is, multiplying a complex number by a merely multiplies both of its entries by a):

Proposition 4.1.9. For any $a \in \mathbb{R}$ and $(b, c) \in \mathbb{C}$, we have $a\,(b, c) = (ab, ac)$. (Here, of course, "$a\,(b, c)$" means the product $a_{\mathbb{C}}\,(b, c)$.)

4.1.6. Inverses and division of complex numbers

Definition 4.1.10. A complex number α is said to be *nonzero* if and only if it is distinct from the complex number $0_{\mathbb{C}} = (0, 0)$.

In other words, a complex number α is nonzero if and only if it is distinct from 0 (since we are identifying the real number 0 with $0_{\mathbb{C}}$). Equivalently, a complex

[52] Why does Theorem 4.1.5 matter here? Well, let us assume for a moment that Theorem 4.1.5 was false; specifically, let us assume that there are two real numbers a and b such that $(ab)_{\mathbb{C}} \neq a_{\mathbb{C}} b_{\mathbb{C}}$. Consider these a and b. Now, Convention 4.1.7 lets us identify the real numbers a, b and ab with the complex numbers $a_{\mathbb{C}}$, $b_{\mathbb{C}}$ and $(ab)_{\mathbb{C}}$. Thus, $ab = (ab)_{\mathbb{C}} \neq \underbrace{a_{\mathbb{C}}}_{=a} \underbrace{b_{\mathbb{C}}}_{=b} = ab$, which is nonsense.

To make sure that Convention 4.1.7 cannot spawn such absurdities, we had to prove Theorem 4.1.5.

number $\alpha = (a, b)$ is nonzero if and only if $(a, b) \neq (0, 0)$ as pairs (i.e., if and only if at least one of the real numbers a and b are nonzero).

We have so far been adding, subtracting and multiplying complex numbers, but never dividing them (except briefly, before we formally defined them). We could define division in the same way as we defined addition, subtraction and multiplication – namely, by an explicit formula for $\dfrac{(a, b)}{(c, d)}$ whenever (c, d) is nonzero[53]. However, it is more instructive to proceed differently, and construct the division from the multiplication that was already defined. After all, if our division is to deserve its name, it should undo multiplication; and this determines it uniquely. We will not define division right away; instead, we start out by defining an *inverse* of a complex number:

Definition 4.1.11. Let α be a complex number. An *inverse* of α means a complex number β such that $\alpha\beta = 1$. (Recall that $1 = 1_{\mathbb{C}}$ by Convention 4.1.7.)

The complex number 0 has no inverse (because $0\beta = 0 \neq 1$, no matter what β is). But it turns out that all the other complex numbers have one:

Theorem 4.1.12. Let α be a nonzero complex number. Then, α has a unique inverse.

Definition 4.1.13. Let α be a nonzero complex number. Theorem 4.1.12 shows that α has a unique inverse. This inverse is called α^{-1}, and will be referred to as *the inverse* of α.

Definition 4.1.14. (a) Let α and β be two complex numbers such that $\beta \neq 0$. Then, the quotient $\dfrac{\alpha}{\beta}$ is defined to be the complex number $\alpha \cdot \beta^{-1}$. It is sometimes also denoted by α/β.

(b) The operation that transforms a pair (α, β) of two complex numbers (with β nonzero) into α/β is called *division*.

It is easy to see that division undoes multiplication:

Proposition 4.1.15. Let α, β, γ be three complex numbers with $\beta \neq 0$. Then, we have the equivalence

$$\left(\gamma = \frac{\alpha}{\beta}\right) \iff (\alpha = \beta\gamma).$$

Inverses also have the following properties:

[53] This formula would be

$$\frac{(a, b)}{(c, d)} = \left(\frac{ac + bd}{c^2 + d^2}, \frac{bc - ad}{c^2 + d^2}\right).$$

Proposition 4.1.16. (a) Let $\alpha \in \mathbb{C}$ be a complex number that has an inverse (i.e., is nonzero). Then, its inverse α^{-1} has an inverse as well, and this inverse is $\left(\alpha^{-1}\right)^{-1} = \alpha$.

(b) Let $\alpha, \beta \in \mathbb{C}$ be two complex numbers that have inverses (i.e., are nonzero). Then, their product $\alpha\beta$ has an inverse as well, and this inverse is $(\alpha\beta)^{-1} = \alpha^{-1}\beta^{-1}$.

Corollary 4.1.17. Let $\alpha, \beta \in \mathbb{C}$ be two nonzero complex numbers. Then, the complex number $\alpha\beta$ is nonzero as well.

4.1.7. Powers of complex numbers

Let us now define powers of complex numbers, where the exponent is a nonnegative integer.

Definition 4.1.18. Let $\alpha \in \mathbb{C}$ and $n \in \mathbb{N}$. We define a complex number α^n (called the *n-th power of* α) by setting $\alpha^n = \underbrace{\alpha\alpha\cdots\alpha}_{n \text{ times}}$.

Definition 4.1.18 yields

$$i^2 = ii = (-1)_{\mathbb{C}} = -1.$$

Moreover, Definition 4.1.18 yields

$$\alpha^0 = \underbrace{\alpha\alpha\cdots\alpha}_{0 \text{ times}} = (\text{empty product}) = 1 \qquad \text{and}$$
$$\alpha^1 = \underbrace{\alpha\alpha\cdots\alpha}_{1 \text{ times}} = \alpha$$

for each $\alpha \in \mathbb{C}$.

For another example, Definition 4.1.18 yields

$$(1+i)^2 = (1+i)(1+i) = 1 + i + i + \underbrace{ii}_{=-1} = 1 + i + i + (-1) = i + i = 2i$$

and

$$(1+i)^4 = \underbrace{(1+i)(1+i)}_{=2i}\underbrace{(1+i)(1+i)}_{=2i} = 2i \cdot 2i = 4\underbrace{ii}_{=-1} = 4(-1) = -4.$$

We shall use the PEMDAS convention for the order of operations when powers are involved. For example, the expression "$\alpha\beta^k + \gamma$" means $\left(\alpha\left(\beta^k\right)\right) + \gamma$ rather than (say) $(\alpha\beta)^k + \gamma$.

Recall that any nonzero complex number α has an inverse α^{-1} (by Definition 4.1.13). This allows us to extend our definition of α^n to **negative** n as well:

Definition 4.1.19. Let $\alpha \in \mathbb{C}$ be nonzero. For any negative $n \in \mathbb{Z}$, we define a complex number α^n (called the *n-th power of* α) by $\alpha^n = \left(\alpha^{-1}\right)^{-n}$. (This is well-defined, since $\left(\alpha^{-1}\right)^{-n}$ is already defined by Definition 4.1.18 (because n is negative and thus $-n \in \mathbb{N}$).)

The attentive reader will have noticed that Definition 4.1.19 redefines α^{-1} when α is nonzero (indeed, -1 is a negative integer, and thus can be substituted for n in Definition 4.1.19). Fortunately, this new definition of α^{-1} does not clash with the original definition (Definition 4.1.13), because if we set $n = -1$ in Definition 4.1.19, then we get $\alpha^{-1} = \left(\alpha^{-1}\right)^1 = \alpha^{-1}$ (where the "α^{-1}" on the left hand side is the new meaning defined in Definition 4.1.19, whereas the "α^{-1}" on the right hand side is the old meaning defined in Definition 4.1.13).

If $\alpha = 0$ and if $n \in \mathbb{Z}$ is negative, then we leave α^n undefined.

Powers of complex numbers satisfy the usual rules for exponents:

Proposition 4.1.20. **(a)** We have $\alpha^{n+1} = \alpha\alpha^n$ for all $\alpha \in \mathbb{C}$ and $n \in \mathbb{N}$.
(b) We have $\alpha^{n+m} = \alpha^n\alpha^m$ for all $\alpha \in \mathbb{C}$ and $n, m \in \mathbb{N}$.
(c) We have $(\alpha\beta)^n = \alpha^n\beta^n$ for all $\alpha, \beta \in \mathbb{C}$ and $n \in \mathbb{N}$.
(d) We have $\left(\alpha^n\right)^m = \alpha^{nm}$ for all $\alpha \in \mathbb{C}$ and $n, m \in \mathbb{N}$.
(e) We have $1^n = 1$ for all $n \in \mathbb{N}$.
(f) We have $\alpha^{n+1} = \alpha\alpha^n$ for all nonzero $\alpha \in \mathbb{C}$ and all $n \in \mathbb{Z}$.
(g) We have $\alpha^{-n} = \left(\alpha^{-1}\right)^n$ for all nonzero $\alpha \in \mathbb{C}$ and all $n \in \mathbb{Z}$.
(h) We have $\alpha^{n+m} = \alpha^n\alpha^m$ for all nonzero $\alpha \in \mathbb{C}$ and all $n, m \in \mathbb{Z}$.
(i) We have $(\alpha\beta)^n = \alpha^n\beta^n$ for all nonzero $\alpha, \beta \in \mathbb{C}$ and all $n \in \mathbb{Z}$.
(j) We have $1^n = 1$ for all $n \in \mathbb{Z}$.
(k) We have $\left(\alpha^n\right)^{-1} = \alpha^{-n}$ for all nonzero $\alpha \in \mathbb{C}$ and all $n \in \mathbb{Z}$. (In particular, α^n is nonzero, so that $\left(\alpha^n\right)^{-1}$ is well-defined.)
(l) We have $\left(\alpha^n\right)^m = \alpha^{nm}$ for all nonzero $\alpha \in \mathbb{C}$ and all $n, m \in \mathbb{Z}$. (In particular, α^n is nonzero, so that $\left(\alpha^n\right)^m$ is well-defined for all $m \in \mathbb{Z}$.)
(m) Complex numbers satisfy the binomial formula: That is, if $\alpha, \beta \in \mathbb{C}$, then

$$(\alpha + \beta)^n = \sum_{k=0}^{n} \binom{n}{k} \alpha^k \beta^{n-k} \qquad \text{for } n \in \mathbb{N}.$$

Proposition 4.1.20 can be proven in the same way as the corresponding claims are proven for real (or rational) numbers:

Exercise 4.1.1. Prove Proposition 4.1.20.

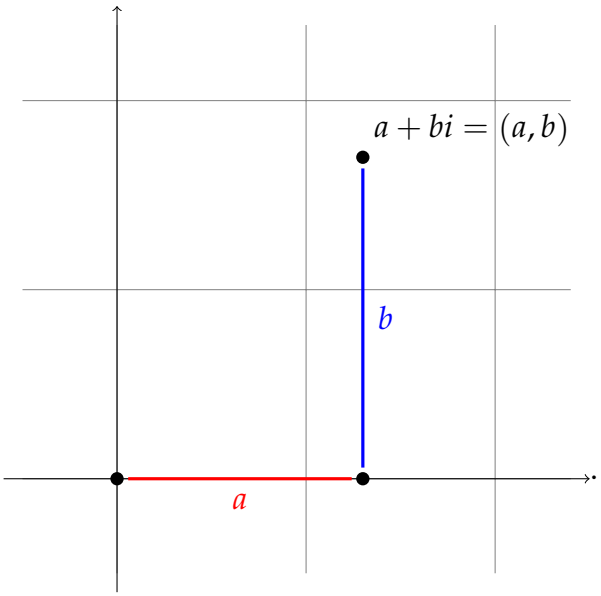
It may be tempting to try to extend Definition 4.1.19 further by defining fractional powers (such as $\alpha^{1/2}$). There is a way to do so, but such a definition would be of questionable use and somewhat fragile (in the sense that it would fail to satisfy the rules of exponents). For example, if you wanted to define $(-1)^{1/2}$, then the

only reasonable choices would be i and $-i$ (since these are the only two complex numbers whose squares are -1); but with either option, the equality $(\alpha\beta)^{1/2} = \alpha^{1/2}\beta^{1/2}$ would fail if we took $\alpha = -1$ and $\beta = -1$. Thus, we prefer to leave powers of the form α^n for $n \notin \mathbb{Z}$ undefined.

4.1.8. The Argand diagram

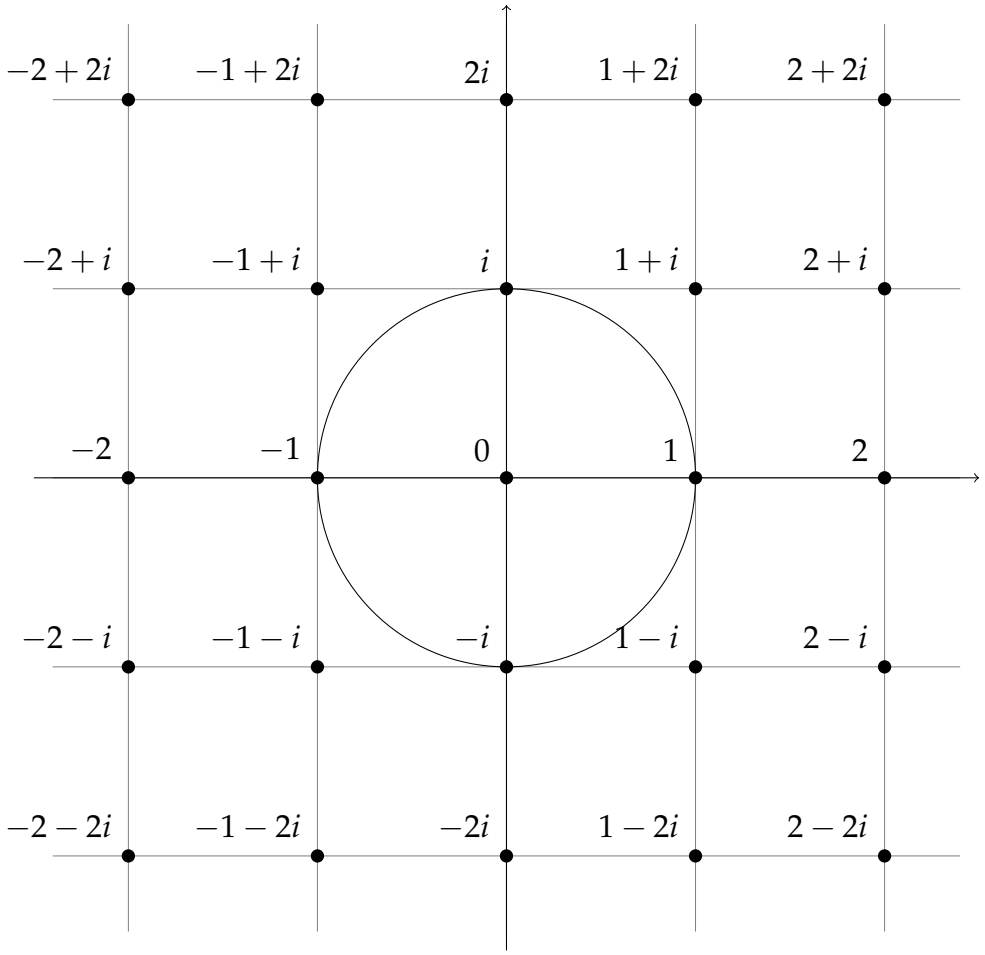
Let us next make a small detour to demonstrate a geometric representation of the complex numbers which, while not strictly necessary for what we intend to do with them, is conducive both to understanding them and to applying them.

Recall that a complex number was defined as a pair of real numbers. On the other hand, a point in the Cartesian plane is also defined as a pair of real numbers (its x-coordinate and its y-coordinate). Thus, it is natural to identify each complex number $(a, b) = a + bi$ with the point $(a, b) \in \mathbb{R}^2$ on the Cartesian plane (i.e., the point with x-coordinate a and y-coordinate b). This identification equates each complex number with a unique point in the Cartesian plane, and vice versa:



The picture below shows some of the points (specifically, all the 25 points $(a, b) \in \{-2, -1, 0, 1, 2\}^2$ whose both coordinates are integers between -2 and 2) labeled

with the corresponding complex numbers:



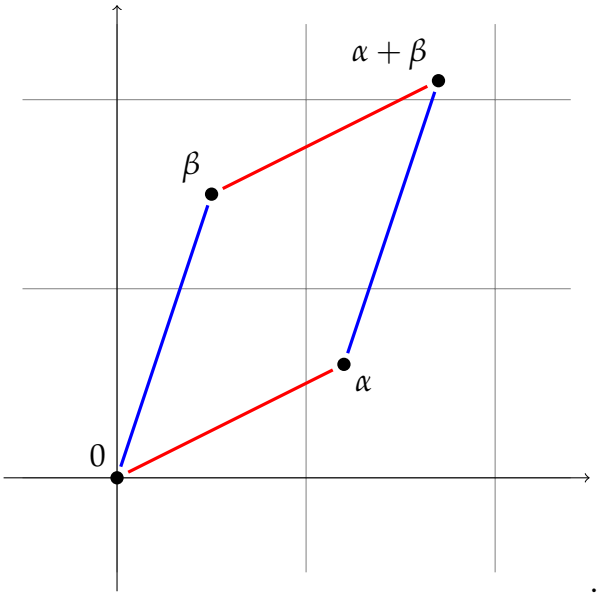
(39)

(as well as the unit circle, which passes through the four points labeled $1, i, -1, -i$; we will encounter these four points rather often in the following).

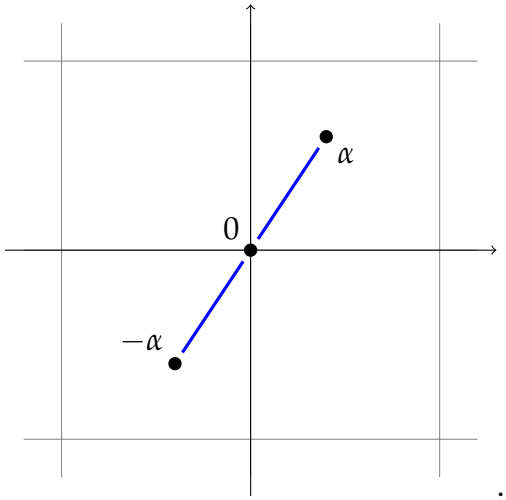
This identification of complex numbers with points is called the *Argand diagram* or the *complex plane* (although the latter word has yet another, different meaning). The complex number 0 corresponds to the origin $(0, 0)$ of the plane.

In Definition 4.1.1 **(e)**, we have introduced three operations on complex numbers; what do they mean geometrically for the corresponding points? The two operations $+$ and $-$ are easiest to understand: They are exactly the usual operations of addition and subtraction for vectors. Thus, if α and β are two complex numbers, then the points labeled by the four complex numbers 0, α, $\alpha + \beta$ and β

form a parallelogram:



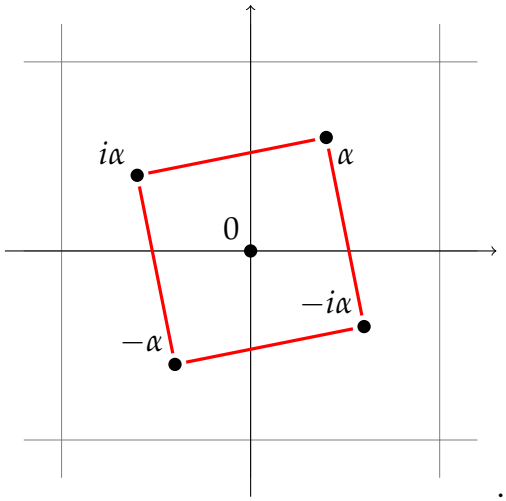
Likewise, the points labeled by the four complex numbers 0, α, β and $\beta - \alpha$ form a parallelogram. These parallelograms can be degenerate; in particular, the point $-\alpha$ is the reflection of the point α through the origin:[54]



Multiplication is less evident. The easiest case is multiplying by i: If α is a complex number, then the point $i\alpha$ is obtained from the point α by a 90° rotation (counterclockwise) around the origin. Thus, the four points α, $i\alpha$, $-\alpha$ and $-i\alpha$ are

[54] We no longer say "the point labeled by α", but simply equate α with that point now.

the vertices of a square centered at the origin:



.

More generally, if β is a complex number, then multiplication by β (that is, the map $\mathbb{C} \to \mathbb{C}$, $\alpha \mapsto \alpha\beta$) is a similitude transformation (so it preserves angles and ratios of lengths); more precisely it is a rotation around the origin composed with a homothety from the origin. Combined with the fact that it sends 1 to β, this uniquely determines it.

This is just the beginning of a rather helpful dictionary between elementary plane geometry and the algebra of complex numbers. See [AndAnd14] for many applications of this point of view, particularly to proving results in plane geometry.

4.1.9. Norms and conjugates

Let us now define some further features of complex numbers.

Definition 4.1.21. Let $\alpha = (a, b)$ be a complex number.

The *norm* of α is defined to be the real number $a^2 + b^2 \in \mathbb{R}$. This norm is called $\mathrm{N}(\alpha)$.

Proposition 4.1.22. Let α be a complex number.

(a) We have $\mathrm{N}(\alpha) \geq 0$.

(b) We have $\mathrm{N}(\alpha) = 0$ if and only if $\alpha = 0$.

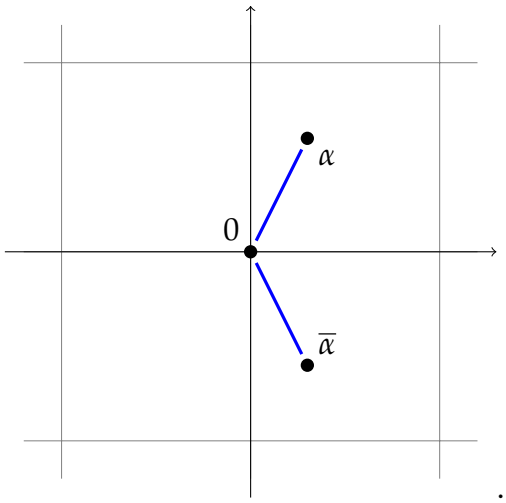
(c) If $\alpha \neq 0$, then $\mathrm{N}(\alpha) > 0$.

Proposition 4.1.23. Let $a \in \mathbb{R}$. Then, $\mathrm{N}(a_{\mathbb{C}}) = a^2$.

Definition 4.1.24. Let $\alpha = (a, b) \in \mathbb{C}$.

The *conjugate* $\overline{\alpha}$ of α is defined to be the complex number $(a, -b) \in \mathbb{C}$.

From the viewpoint of the Argand diagram, the conjugate $\overline{\alpha}$ of a complex number α is simply the result of reflecting α (or, to be pedantic, the point labeled by α) across the x-axis:



Thus, the following is completely self-evident:

Proposition 4.1.25. Let $\alpha \in \mathbb{C}$.

(a) We have $\alpha = \overline{\alpha}$ if and only if $\alpha \in \mathbb{R}$. (Keep in mind that we are following Convention 4.1.7, so that the statement "$\alpha \in \mathbb{R}$" (for a complex number α) actually means "$\alpha = r_{\mathbb{C}}$ for some $r \in \mathbb{R}$".)

(b) We always have $\overline{\overline{\alpha}} = \alpha$.

Since we don't want to depend on geometric reasoning, let us nevertheless prove this fact algebraically:

Proposition 4.1.26. Let $\alpha \in \mathbb{C}$.

(a) We have $\mathrm{N}(\alpha) = \alpha\overline{\alpha}$ (or, more formally: $(\mathrm{N}(\alpha))_{\mathbb{C}} = \alpha\overline{\alpha}$).

(b) We have $\mathrm{N}(\overline{\alpha}) = \mathrm{N}(\alpha)$.

Proposition 4.1.27. Let α and β be two complex numbers. Then:

(a) We have $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$.

(b) We have $\overline{\alpha - \beta} = \overline{\alpha} - \overline{\beta}$.

(c) We have $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$.

(d) We have $\mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta)$.

(e) If $\beta \neq 0$, then $\mathrm{N}\left(\dfrac{\alpha}{\beta}\right) = \dfrac{\mathrm{N}(\alpha)}{\mathrm{N}(\beta)}$.

The properties of the norm of a complex numbers let us see an old fact in new light: Remember the Brahmagupta–Fibonacci identity (1), which said that

$$\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (ad + bc)^2 + (ac - bd)^2$$

for $a, b, c, d \in \mathbb{R}$. This identity is equivalent to the identity

$$\mathrm{N}(\alpha) \cdot \mathrm{N}(\beta) = \mathrm{N}(\alpha\beta)$$

for the complex numbers $\alpha = (a, b) = a + bi$ and $\beta = (c, d) = c + di$. Thus, the identity (1) is just Proposition 4.1.27 **(d)**, restated without the use of complex numbers. This answers the question of how you could have come up with this identity – at least if you know complex numbers. (Brahmagupta must have found it in a different way, since complex numbers were not known to him.)

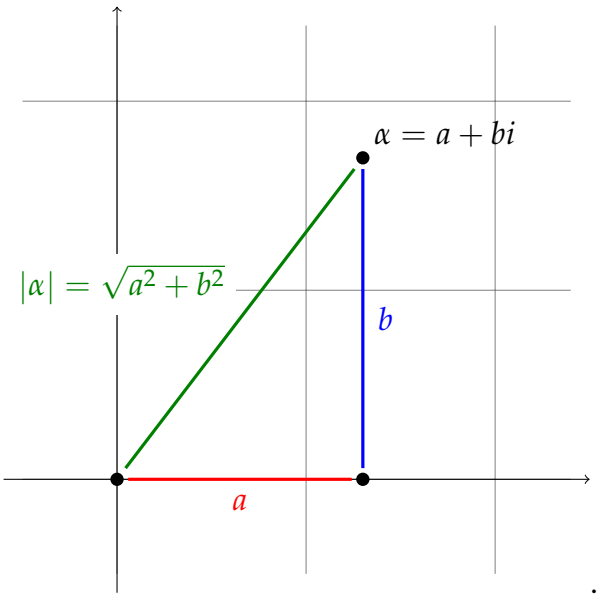
Corollary 4.1.28. Let $\alpha \in \mathbb{C}$ and $k \in \mathbb{N}$. Then:
(a) We have $\overline{\alpha^k} = \overline{\alpha}^k$.
(b) We have $\mathrm{N}\left(\alpha^k\right) = (\mathrm{N}(\alpha))^k$.

Using the norm of a complex number, we can define a notion of absolute value of a complex number:

Definition 4.1.29. Let $\alpha = (a, b)$ be a complex number. The *absolute value* (or *modulus* or *length*) of α is defined to be $\sqrt{\mathrm{N}(\alpha)} = \sqrt{a^2 + b^2} \in \mathbb{R}$. (This is well-defined, because Proposition 4.1.22 **(a)** shows that $\mathrm{N}(\alpha) \geq 0$.)

The absolute value of α is denoted by $|\alpha|$. (This notation does not conflict with the classical notation $|a|$ for the absolute value of a real number a, because if a is a real number, then Proposition 4.1.23 yields $\mathrm{N}(a_{\mathbb{C}}) = a^2$ and therefore $\sqrt{\mathrm{N}(a_{\mathbb{C}})} = \sqrt{a^2} = |a|$, where "$|a|$" means the classical concept of absolute value of a.)

In the Argand diagram, the absolute value $|\alpha|$ of a complex number α is simply the distance of α from the origin. The reason for this is the Pythagorean theorem:



Good references for the basic properties of complex numbers are [LaNaSc16] and [Swanso18, §3.9–§3.12]. The book [AndAnd14] is a treasure trove of applications and exercises.

4.1.10. Re, Im and the 2×2-matrix representation

We define some more attributes of a complex number.

Definition 4.1.30. Let $\alpha = (a, b)$ be a complex number (so that a and b are real numbers and $\alpha = a + bi$).

Then, a is called the *real part* of α and denoted $\operatorname{Re} \alpha$ (or $\mathfrak{R}\alpha$).

Also, b is called the *imaginary part* of α and denoted $\operatorname{Im} \alpha$ (or $\mathfrak{I}\alpha$).

The following proposition assigns a real 2×2-matrix to each complex number:

Proposition 4.1.31. Let $\mathbb{R}^{2\times 2}$ be the set of all 2×2-matrices with real entries.

Define a map $\mu : \mathbb{C} \to \mathbb{R}^{2\times 2}$ by setting

$$\mu(a, b) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \text{for each } (a, b) \in \mathbb{C}.$$

(a) We have $\mu(\alpha + \beta) = \mu(\alpha) + \mu(\beta)$ for all $\alpha, \beta \in \mathbb{C}$.
(b) We have $\mu(\alpha - \beta) = \mu(\alpha) - \mu(\beta)$ for all $\alpha, \beta \in \mathbb{C}$.
(c) We have $\mu(\alpha \cdot \beta) = \mu(\alpha) \cdot \mu(\beta)$ for all $\alpha, \beta \in \mathbb{C}$.
(d) The map μ is injective.

Proposition 4.1.31 really says that (instead of regarding complex numbers as pairs of real numbers) we can regard complex numbers as a specific kind of 2×2-matrices with real entries (by identifying each complex number α with the matrix $\mu(\alpha)$). This viewpoint has the advantage that multiplication of complex numbers becomes a particular case of matrix multiplication. (We could have saved ourselves the trouble of proving the associativity of multiplication for complex numbers if we had taken this viewpoint.)

4.1.11. The fundamental theorem of algebra

Finally, let me mention without proof the so-called *Fundamental Theorem of Algebra*:

Theorem 4.1.32. Let $p(x)$ be a polynomial of degree n with complex coefficients. Then, there exist complex numbers $\alpha_1, \alpha_2, \ldots, \alpha_n$ and β such that

$$p(x) = \beta(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

In other words, any polynomial with complex coefficients can be factored into linear factors. This is in contrast to real numbers, where polynomials can at best

be factored into linear and quadratic factors. (For example, the polynomial x^2+1 cannot be factored further over the real numbers, but factors as $(x+i)(x-i)$ over the complex numbers.)

The Fundamental Theorem of Algebra is not actually a theorem of algebra. It relies heavily on the concepts of real and complex numbers. So it is actually a theorem of analysis. For a proof, see [LaNaSc16, Theorem 3.2.2].

4.2. Gaussian integers

Inside the set $\mathbb{C}$ of all complex numbers (an uncountable set) lies a much smaller (countable) set of numbers, which are much closer to integers than to real numbers. We shall study them partly for their own sake, partly as an instructive example of what we will later call a commutative ring, and partly in order to answer the questions from Section 1.4 (although complex numbers were never mentioned in that section).

We shall follow Keith Conrad's notes [ConradG] for most of this section (but at the end we will go a bit further in order to answer Question 1.4.2 **(b)**).

4.2.1. Definitions and basics

We shall now define the *Gaussian integers*: a middle ground between integers and complex numbers.

Definition 4.2.1. A *Gaussian integer* is a complex number (a,b) with $a,b \in \mathbb{Z}$.

For example, $3+5i = (3,5)$ and $3-7i = (3,-7)$ are Gaussian integers. So are $0 = (0,0)$, $1 = (1,0)$ and $i = (0,1)$. Every integer is a Gaussian integer[55]. But $\frac{1}{2}+3i = \left(\frac{1}{2},3\right)$ and $\sqrt{2}+4i = \left(\sqrt{2},4\right)$ are not Gaussian integers.

Recall that in the Argand diagram, complex numbers correspond to points in the Cartesian plane. The Gaussian integers thus correspond to a special type of points – the ones whose both coordinates are integers. These points are called *lattice points*, as they form the nodes of a square lattice covering the plane. In the picture (39), the 25 marked points are precisely the lattice points (i.e., the Gaussian integers) that happen to fall inside the region drawn.

Remark 4.2.2. In Definition 4.2.1, we have defined Gaussian integers using complex numbers. This can be viewed as somewhat of an overkill, as the notion of complex numbers depends on the notion of real numbers, which are mostly useless for Gaussian integers. Thus, one might ask for a different definition of Gaussian integers – one which relies only on integers and not on real numbers.

[55] This relies on Convention 4.1.7, of course. If we avoid this convention, then we should instead say that for every integer r, the complex number $r_{\mathbb{C}} = (r,0)$ is a Gaussian integer.

Such a definition is easy to make: Just replace every appearance of real numbers in Definition 4.1.1 by integers! Thus, define the Gaussian integers as pairs of two integers; let $\mathbb{C}_{\mathbb{Z}}$ be the set of these pairs; denote the Gaussian integer $(r,0)$ by $r_{\mathbb{C}}$ whenever r is an integer; define the operations $+$, $-$ and $\cdot$ on the set $\mathbb{C}_{\mathbb{Z}}$ by the same formulas as in Definition 4.1.1 **(e)**; likewise, adapt the rest of Definition 4.1.1 to integers. Most of what we have done in Section 4.1 can be straightforwardly adapted to this notion of Gaussian integers (by making the obvious changes – i.e., mostly, replacing real numbers by integers); the main exceptions are the following:

- Not every nonzero Gaussian integer has an inverse (in the set of Gaussian integers). (In fact, as we will soon see, the only Gaussian integers that have inverses are $1, i, -1, -i$.) Thus, division and negative powers of Gaussian integers are usually not defined (without leaving the set of Gaussian integers).
- The absolute value $|\alpha|$ of a Gaussian integer α will usually not be an integer (since it is defined as a square root).

This alternative definition of Gaussian integers is equivalent to Definition 4.2.1; we are using the latter mainly because it is shorter.

Likewise, we could have defined "Gaussian rationals" by adapting Definition 4.1.1 to rational (instead of real) numbers. Unlike the Gaussian integers, these "Gaussian rationals" do have inverses (when they are nonzero), and thus division and negative powers are well-defined for them.

Definition 4.2.3. We let $\mathbb{Z}[i]$ be the set of all Gaussian integers.

Elementary number theory concerns itself with integers (mostly). Our goal in this section is to replicate as much as we can of this theory in the setting of Gaussian integers, and then see how it can be applied back to answer some questions about the usual integers.

We will try to use Greek letters for Gaussian integers and Roman letters for integers.

Proposition 4.2.4. **(a)** If α and β are two Gaussian integers, then $\alpha+\beta$, $\alpha-\beta$ and $\alpha\cdot\beta$ are Gaussian integers.

(b) If α is a Gaussian integer, then $-\alpha$ is a Gaussian integer.

(c) Sums and products of finitely many Gaussian integers are Gaussian integers.

Proposition 4.2.5. Let α be a Gaussian integer. Then, $\overline{\alpha}$ is a Gaussian integer.

Proposition 4.2.6. Let $\alpha \in \mathbb{Z}[i]$. Then, $\mathrm{N}(\alpha) \in \mathbb{N}$.

4.2.2. Units and unit-equivalence

Any nonzero Gaussian integer α has an inverse (by Theorem 4.1.12). But usually, this inverse is not a Gaussian integer, i.e., does not lie in $\mathbb{Z}[i]$. For example, $2^{-1} \notin \mathbb{Z}[i]$ and $(1+i)^{-1} = \dfrac{1-i}{2} \notin \mathbb{Z}[i]$. The Gaussian integers whose inverses do lie in $\mathbb{Z}[i]$ have a special name:

Definition 4.2.7. (a) A Gaussian integer $\alpha \in \mathbb{Z}[i]$ is said to be *invertible in* $\mathbb{Z}[i]$ if it has an inverse in $\mathbb{Z}[i]$.

A *unit* will mean a Gaussian integer that is invertible in $\mathbb{Z}[i]$.

(b) We define a relation $\sim$ on $\mathbb{Z}[i]$ by

$$(\alpha \sim \beta) \iff (\alpha = \gamma\beta \text{ for some unit } \gamma \in \mathbb{Z}[i]).$$

This relation will be called *unit-equivalence* (or *equality up to unit*). We say that two Gaussian integers α and β are *unit-equivalent* if $\alpha \sim \beta$.

For comparison, let us consider analogous concepts for integers instead of Gaussian integers. The units of $\mathbb{Z}$ (that is, the integers that are invertible in $\mathbb{Z}$) are 1 and -1. So if we defined a relation $\underset{\mathbb{Z}}{\sim}$ on $\mathbb{Z}$ in the same way as we defined the relation $\sim$ on $\mathbb{Z}[i]$ (but requiring $\gamma \in \mathbb{Z}$ instead of $\gamma \in \mathbb{Z}[i]$), then this relation would just be given by

$$\begin{aligned} \left(a \underset{\mathbb{Z}}{\sim} b\right) &\iff (a = cb \text{ for some } c \in \{1,-1\}) \\ &\iff (a = b \text{ or } a = -b) \iff (|a| = |b|). \end{aligned} \tag{40}$$

So the relation $\underset{\mathbb{Z}}{\sim}$ is not very exciting: it is simply "equality up to sign".[56] But the relation $\sim$ on $\mathbb{Z}[i]$ cannot be described as simply as this: It is easy to find two Gaussian integers α and β such that $|\alpha| = |\beta|$ holds but $\alpha \sim \beta$ does not (for example, the Gaussian integers $\alpha = 16 + 63i$ and $\beta = 33 + 56i$ both have absolute value 65 but are not unit-equivalent).

Proposition 4.2.8. The relation $\sim$ on $\mathbb{Z}[i]$ is an equivalence relation.

Proposition 4.2.9. Let α be a Gaussian integer.

(a) We have $\mathrm{N}(\alpha) = 0$ if and only if $\alpha = 0$.

(b) We have $\mathrm{N}(\alpha) = 1$ if and only if α is a unit.

(c) If α is nonzero and not a unit, then $\mathrm{N}(\alpha) > 1$.

[56] In other words, it is precisely the relation $\underset{\text{abs}}{\equiv}$, where $\text{abs} : \mathbb{Z} \to \mathbb{N}$ is the map sending each integer n to its absolute value $|n|$. (See Example 3.2.7 for how this relation $\underset{\text{abs}}{\equiv}$ is defined.)

Proposition 4.2.10. The units (in $\mathbb{Z}[i]$) are $1, -1, i, -i$.

As a consequence of Proposition 4.2.10, if we are given two Gaussian integers α and β, we can easily check whether $\alpha \sim \beta$ holds:

Proposition 4.2.11. Let α and β be two Gaussian integers. Then, we have $\alpha \sim \beta$ if and only if

$$(\alpha = \beta \text{ or } \alpha = -\beta \text{ or } \alpha = i\beta \text{ or } \alpha = -i\beta).$$

Definition 4.2.12. We know from Proposition 4.2.8 that the relation $\sim$ on $\mathbb{Z}[i]$ is an equivalence relation.

The equivalence classes of this relation $\sim$ shall be called the *unit-equivalence classes*. More specifically, for each $\alpha \in \mathbb{Z}[i]$, we shall denote the $\sim$-equivalence class of α as the *unit-equivalence class of* α.

Proposition 4.2.13. **(a)** For each $\alpha \in \mathbb{Z}[i]$, we have

$$(\text{the unit-equivalence class of } \alpha) = \{\alpha, i\alpha, -\alpha, -i\alpha\}.$$

(b) The unit-equivalence classes are the sets of the form $\{\alpha, i\alpha, -\alpha, -i\alpha\}$ for some $\alpha \in \mathbb{Z}[i]$.

Recall that (as we have seen in Subsection 4.1.8) if α is a complex number, then the four complex numbers α, $i\alpha$, $-\alpha$ and $-i\alpha$ (represented as points in the Argand diagram) are the vertices of a square centered at the origin. But when α is a Gaussian integer, these four complex numbers constitute the unit-equivalence class of α (by Proposition 4.2.13 **(a)**). Thus, geometrically speaking, the unit-equivalence class of a Gaussian integer α consists of the four vertices of a square centered at the origin. (When $\alpha = 0$, these four vertices coincide.)

Proposition 4.2.14. Let α be a Gaussian integer. Then, $\alpha \sim 1$ if and only if α is a unit.

Proposition 4.2.15. Let α and β be two unit-equivalent Gaussian integers. Then, $\mathrm{N}(\alpha) = \mathrm{N}(\beta)$.

The converse of Proposition 4.2.15 does not hold: There exist Gaussian integers α and β satisfying $\mathrm{N}(\alpha) = \mathrm{N}(\beta)$ that are not unit-equivalent.

At this point, let us briefly take a look at a seemingly random question: Which Gaussian integers α are unit-equivalent to their own conjugates (i.e., satisfy $\alpha \sim \overline{\alpha}$) ? Besides being an instructive exercise, answering this question will surprisingly aid us answer Question 1.4.2 later on!

Here are some examples:

- Every integer g satisfies $g \sim \overline{g}$, since an integer g always satisfies $\overline{g} = g$.

- Every integer g satisfies $gi \sim \overline{gi}$. Indeed, if g is an integer, then Proposition 4.1.27 **(c)** (applied to $\alpha = g$ and $\beta = i$) yields

$$\overline{gi} = \underbrace{\overline{g}}_{\substack{=g \\ \text{(since } g \in \mathbb{Z} \subseteq \mathbb{R}\text{)}}} \cdot \underbrace{\overline{i}}_{=-i} = g\left(-i\right) = -gi = \left(-1\right) \cdot \left(gi\right),$$

  and this leads to $\overline{gi} \sim gi$ (since -1 is a unit); but this, in turn, yields $gi \sim \overline{gi}$ (since Proposition 4.2.8 shows that $\sim$ is an equivalence relation).

- Every integer g satisfies $g\left(1+i\right) \sim \overline{g\left(1+i\right)}$. Indeed, if g is an integer, then Proposition 4.1.27 **(c)** (applied to $\alpha = g$ and $\beta = 1+i$) yields

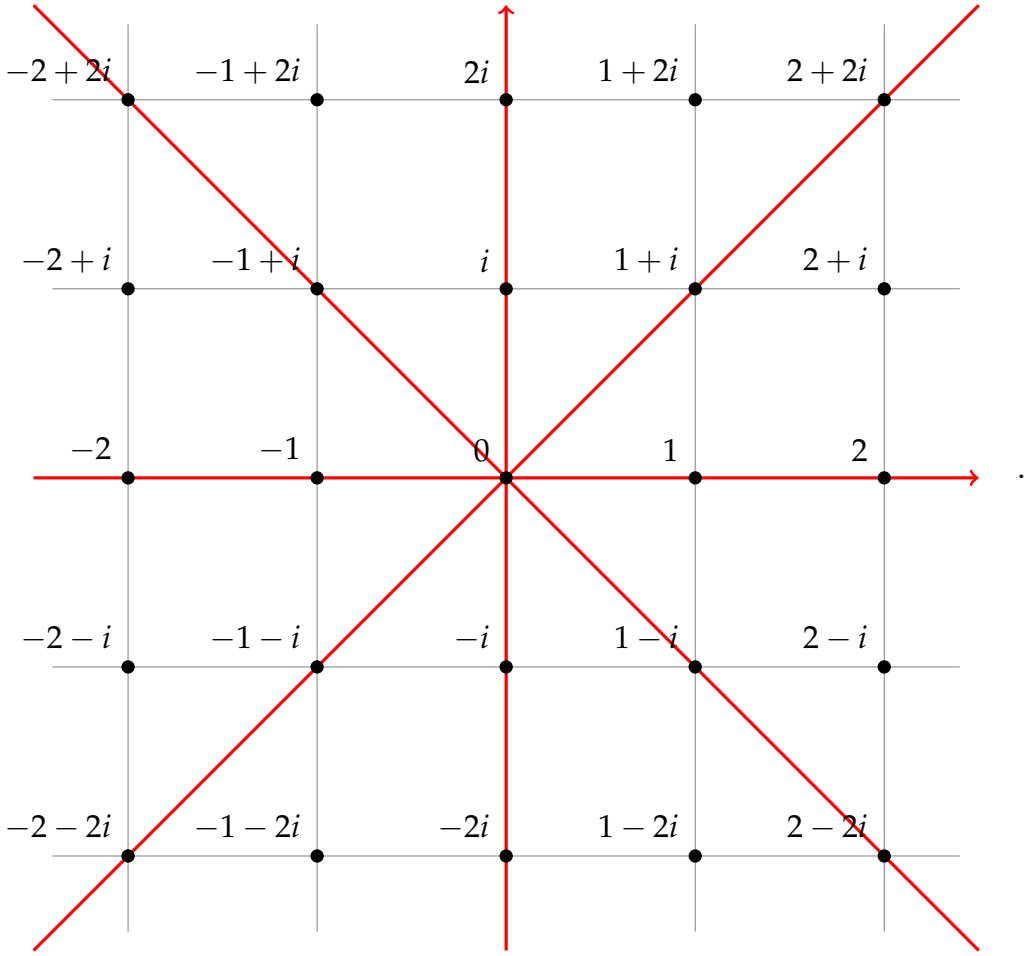
$$\overline{g\left(1+i\right)} = \underbrace{\overline{g}}_{\substack{=g \\ \text{(since } g \in \mathbb{Z} \subseteq \mathbb{R}\text{)}}} \cdot \underbrace{\overline{\left(1+i\right)}}_{\substack{=1-i \\ =(-i)(1+i) \\ \text{(check this!)}}} = g\left(-i\right)\left(1+i\right) = \left(-i\right) \cdot \left(g\left(1+i\right)\right),$$

  and this leads to $\overline{g\left(1+i\right)} \sim g\left(1+i\right)$ (since $-i$ is a unit); but this, in turn, yields $g\left(1+i\right) \sim \overline{g\left(1+i\right)}$ (since Proposition 4.2.8 shows that $\sim$ is an equivalence relation).

- Every integer g satisfies $g\left(1-i\right) \sim \overline{g\left(1-i\right)}$. This can be checked similarly to how we just checked $g\left(1+i\right) \sim \overline{g\left(1+i\right)}$.

Thus, in total, we have found four families of Gaussian integers α satisfying $\alpha \sim \overline{\alpha}$: namely, those of the form $g \in \mathbb{Z}$; those of the form gi with $g \in \mathbb{Z}$; those of the form $g\left(1+i\right)$ with $g \in \mathbb{Z}$; and those of the form $g\left(1-i\right)$ with $g \in \mathbb{Z}$. On the Argand diagram, these are precisely the lattice points on the four bold red lines on

the following picture:



Are there any other Gaussian integers α satisfying $\alpha \sim \overline{\alpha}$? As the following exercise (or, rather, its part **(a)**) shows, the answer is "no"; we have found all such α.

Exercise 4.2.1. Let α be a Gaussian integer satisfying $\alpha \sim \overline{\alpha}$. Prove the following:
(a) There exist some $g \in \mathbb{Z}$ and $\tau \in \{1, i, 1+i, 1-i\}$ such that $\alpha = g\tau$.
(b) These g and τ satisfy $\mathrm{N}(\alpha) \in \{g^2, 2g^2\}$.
(c) The norm $\mathrm{N}(\alpha)$ cannot be an odd prime.

(Part **(c)** of this exercise, strange as it sounds, is the one we will end up using later.)

For the sake of the next subsection, let us state a simple property of integers:

Lemma 4.2.16. Let a and b be two integers. Then, we have the logical equivalence

$$(a \mid b) \iff (\text{there exists a Gaussian integer } \gamma \text{ such that } b = a\gamma).$$

4.2.3. Divisibility and congruence

Now, let us begin to do proper number theory with Gaussian integers. The next definition is the straightforward analogue of Definition 2.2.1.

Definition 4.2.17. Let α and β be two Gaussian integers. We say that $\alpha \mid \beta$ (or "α *divides* β" or "β is *divisible by* α" or "β is a *multiple* of α") if there exists a Gaussian integer γ such that $\beta = \alpha\gamma$.

We furthermore say that $\alpha \nmid \beta$ if α does not divide β.

When making such a definition, we need to be careful: Potentially, it might create a clash of notations. In fact, if a and b are integers, then the statement "$a \mid b$" already has a meaning (explained in Definition 2.2.1). Definition 4.2.17 gives this statement a new meaning, because we can consider our integers a and b as Gaussian integers (since every integer is a Gaussian integer). If these two meanings are not equivalent, then the statement "$a \mid b$" becomes ambiguous (as it now has two different meanings) – so we have laid ourselves a landmine!

Fortunately, these two meanings **are** equivalent. That is: If a and b are two integers, then the statement "$a \mid b$" interpreted according to Definition 2.2.1 is equivalent to the statement "$a \mid b$" interpreted according to Definition 4.2.17. Indeed, if a and b are two integers, then we have the following chain of equivalences:

$$\begin{aligned}
&(a \mid b \text{ in the sense of Definition 2.2.1}) \\
&\iff (\text{there exists a Gaussian integer } \gamma \text{ such that } b = a\gamma) \qquad \text{(by Lemma 4.2.16)} \\
&\iff (a \mid b \text{ in the sense of Definition 4.2.17}) .
\end{aligned}$$

Thus, the two possible meanings of "$a \mid b$" are equivalent, and so we are spared of any ambiguity.

More generally, the following proposition holds:

Proposition 4.2.18. Let $a \in \mathbb{Z}$ and $\beta = (b, c) \in \mathbb{Z}[i]$. Then, $a \mid \beta$ if and only if a divides both b and c.

The next proposition is a (partial) analogue of Proposition 2.2.3:

Proposition 4.2.19. Let α and β be two Gaussian integers.

(a) If $\alpha \mid \beta$, then $\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$.

(b) If $\alpha \mid \beta$ and $\beta \neq 0$, then $\mathrm{N}(\alpha) \leq \mathrm{N}(\beta)$.

(c) Assume that $\alpha \neq 0$. Then, $\alpha \mid \beta$ if and only if $\dfrac{\beta}{\alpha} \in \mathbb{Z}[i]$.

Note that we are using the norms $\mathrm{N}(\alpha)$ and $\mathrm{N}(\beta)$ as analogues of $|a|$ and $|b|$ here, since the absolute values $|\alpha|$ and $|\beta|$ of Gaussian integers are often irrational and thus it makes no sense to talk of their divisibility. (At least, this prevents us from using the absolute values of α and β in Proposition 4.2.19 **(a)**. We could use them in Proposition 4.2.19 **(b)**.)

Note that the converse of Proposition 4.2.19 **(a)** does not hold. (That is, $\mathrm{N}(\alpha) \mid \mathrm{N}(\beta)$ does not yield $\alpha \mid \beta$.)

The next proposition is a straightforward analogue of Proposition 2.2.4:

Proposition 4.2.20. **(a)** We have $\alpha \mid \alpha$ for every $\alpha \in \mathbb{Z}[i]$. (This is called the *reflexivity of divisibility* for Gaussian integers.)

(b) If $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ satisfy $\alpha \mid \beta$ and $\beta \mid \gamma$, then $\alpha \mid \gamma$. (This is called the *transitivity of divisibility* for Gaussian integers.)

(c) If $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}[i]$ satisfy $\alpha_1 \mid \beta_1$ and $\alpha_2 \mid \beta_2$, then $\alpha_1\alpha_2 \mid \beta_1\beta_2$.

The next exercise is a Gaussian-integer analogue of Exercise 2.2.2:

Exercise 4.2.2. Let α and β be two Gaussian integers such that $\alpha \mid \beta$ and $\beta \mid \alpha$. Prove that $\alpha \sim \beta$.

Note that the conclusion "$\alpha \sim \beta$" in Exercise 4.2.2 is the proper Gaussian-integer analogue of the conclusion "$|a| = |b|$" in Exercise 2.2.2 (since (40) shows that unit-equivalence on $\mathbb{Z}[i]$ is an analogue of the "have the same absolute value" relation on $\mathbb{Z}$). (We could have stated the weaker conclusion $|\alpha| = |\beta|$ as well, but it would not be half as useful.)

A converse of Exercise 4.2.2 holds as well, so we have the following equivalent description of unit-equivalence:

Exercise 4.2.3. Let α and β be two Gaussian integers. Prove that we have the logical equivalence

$$(\alpha \sim \beta) \iff (\alpha \mid \beta \text{ and } \beta \mid \alpha).$$

The next exercise is an analogue of Exercise 2.2.3:

Exercise 4.2.4. Let α, β, γ be three Gaussian integers such that $\gamma \neq 0$. Prove that $\alpha \mid \beta$ holds if and only if $\alpha\gamma \mid \beta\gamma$.

The next exercise is an analogue of Exercise 2.2.4:

Exercise 4.2.5. Let $\nu \in \mathbb{Z}[i]$. Let $a, b \in \mathbb{N}$ be such that $a \leq b$. Prove that $\nu^a \mid \nu^b$.

Needless to say, the a and b in this exercise still have to be nonnegative integers, since Gaussian integers make no sense as exponents.

The next exercise is an analogue of Exercise 2.2.5:

Exercise 4.2.6. Let γ be a Gaussian integer such that $\gamma \mid 1$. Prove that $\gamma \sim 1$ (that is, γ is a unit, i.e., either 1 or -1 or i or $-i$).

Next come two more trivial facts:

Exercise 4.2.7. Let α and β be Gaussian integers such that $\alpha \mid \beta$. Prove that $\overline{\alpha} \mid \overline{\beta}$.

Exercise 4.2.8. Let α, β and γ be three Gaussian integers. Prove the following:
(a) If $\beta \sim \gamma$, then we have the logical equivalence $(\alpha \mid \beta) \iff (\alpha \mid \gamma)$.
(b) If $\alpha \sim \beta$, then we have the logical equivalence $(\alpha \mid \gamma) \iff (\beta \mid \gamma)$.
(c) Let δ be a further Gaussian integer. Assume that $\alpha \sim \beta$ and $\gamma \sim \delta$. Then, we have the logical equivalence $(\alpha \mid \gamma) \iff (\beta \mid \delta)$.

Another useful and easily proven fact is the following:

Exercise 4.2.9. Let α and β be Gaussian integers such that $\alpha \mid \beta$ and $\mathrm{N}(\alpha) = \mathrm{N}(\beta)$. Prove that $\alpha \sim \beta$.

We have defined congruence for integers in Definition 2.3.1. We can repeat the same definition for Gaussian integers:

Definition 4.2.21. Let $\nu, \alpha, \beta \in \mathbb{Z}[i]$. We say that α *is congruent to* β *modulo* ν if and only if $\nu \mid \alpha - \beta$. We shall use the notation "$\alpha \equiv \beta \bmod \nu$" for "$\alpha$ is congruent to β modulo ν".

We furthermore shall use the notation "$\alpha \not\equiv \beta \bmod \nu$" for "$\alpha$ is not congruent to β modulo ν".

Once again, such a definition risks sneaking in ambiguity, but fortunately this one does not: If $n, a, b \in \mathbb{Z}$, then the statement "$a \equiv b \bmod n$" interpreted according to Definition 2.3.1 is equivalent to the statement "$a \equiv b \bmod n$" interpreted according to Definition 4.2.21 (by treating n, a, b as Gaussian integers). To see why, recall that both statements are defined to mean "$n \mid a - b$", and the meaning of the latter statement does not depend on whether we interpret n, a, b as integers or as Gaussian integers[57].

The next proposition is a straightforward analogue of Proposition 2.3.3:

Proposition 4.2.22. Let $\nu \in \mathbb{Z}[i]$ and $\alpha \in \mathbb{Z}[i]$. Then, $\alpha \equiv 0 \bmod \nu$ if and only if $\nu \mid \alpha$.

The next proposition is a straightforward analogue of Proposition 2.3.4:

Proposition 4.2.23. Let $\nu \in \mathbb{Z}[i]$.
(a) We have $\alpha \equiv \alpha \bmod \nu$ for every $\alpha \in \mathbb{Z}[i]$.
(b) If $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ satisfy $\alpha \equiv \beta \bmod \nu$ and $\beta \equiv \gamma \bmod \nu$, then $\alpha \equiv \gamma \bmod \nu$.
(c) If $\alpha, \beta \in \mathbb{Z}[i]$ satisfy $\alpha \equiv \beta \bmod \nu$, then $\beta \equiv \alpha \bmod \nu$.
(d) If $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}[i]$ satisfy $\alpha_1 \equiv \beta_1 \bmod \nu$ and $\alpha_2 \equiv \beta_2 \bmod \nu$, then

$$\alpha_1 + \alpha_2 \equiv \beta_1 + \beta_2 \bmod \nu; \tag{41}$$
$$\alpha_1 - \alpha_2 \equiv \beta_1 - \beta_2 \bmod \nu; \tag{42}$$
$$\alpha_1 \alpha_2 \equiv \beta_1 \beta_2 \bmod \nu. \tag{43}$$

[57] We have proven this latter fact shortly after Definition 4.2.17.

(e) Let $\mu \in \mathbb{Z}[i]$ be such that $\mu \mid \nu$. If $\alpha, \beta \in \mathbb{Z}[i]$ satisfy $\alpha \equiv \beta \bmod \nu$, then $\alpha \equiv \beta \bmod \mu$.

Exercise 4.2.10. Let n be an integer. Let (a,b) and (c,d) be two Gaussian integers. Prove that we have the following logical equivalence:

$$((a,b) \equiv (c,d) \bmod n) \iff (a \equiv c \bmod n \text{ and } b \equiv d \bmod n).$$

(Of course, the statement "$(a,b) \equiv (c,d) \bmod n$" is to be understood by treating the integer n as a Gaussian integer.)

Exercise 4.2.11. For any Gaussian integer τ, we let $\underset{\tau}{\equiv}$ be the binary relation on $\mathbb{Z}[i]$ defined by

$$\left(\alpha \underset{\tau}{\equiv} \beta\right) \iff (\alpha \equiv \beta \bmod \tau).$$

(a) Prove that the relation $\underset{\tau}{\equiv}$ is an equivalence relation whenever $\tau \in \mathbb{Z}[i]$.

We shall refer to the equivalence classes of this relation $\underset{\tau}{\equiv}$ as the *Gaussian residue classes modulo* τ; let $\mathbb{Z}[i]/\tau$ be the set of all these classes.

(b) Let n be a positive integer. Thus, a relation $\underset{n}{\equiv}$ on $\mathbb{Z}[i]$ is defined (by treating the integer n as a Gaussian integer). Exercise 4.2.11 **(a)** (applied to $\tau = n$) shows that this relation $\underset{n}{\equiv}$ is an equivalence relation.

Prove that the equivalence classes of the relation $\underset{n}{\equiv}$ (on $\mathbb{Z}[i]$) are the n^2 classes $[a+bi]_{\underset{n}{\equiv}}$ for $(a,b) \in \{0,1,\ldots,n-1\}^2$, and that these n^2 classes are all distinct.

Example 4.2.24. For $n = 3$, Exercise 4.2.11 **(b)** is saying that the equivalence classes of the relation $\underset{3}{\equiv}$ (on $\mathbb{Z}[i]$) are the 3^2 classes

$$\begin{array}{lll} [0+0i]_{\underset{3}{\equiv}}, & [0+1i]_{\underset{3}{\equiv}}, & [0+2i]_{\underset{3}{\equiv}}, \\ [1+0i]_{\underset{3}{\equiv}}, & [1+1i]_{\underset{3}{\equiv}}, & [1+2i]_{\underset{3}{\equiv}}, \\ [2+0i]_{\underset{3}{\equiv}}, & [2+1i]_{\underset{3}{\equiv}}, & [2+2i]_{\underset{3}{\equiv}}, \end{array}$$

and that these 3^2 classes are distinct. In contrast, the equivalence classes of the analogous relation $\underset{3}{\equiv}$ on $\mathbb{Z}$ are merely the 3 classes $[0]_{\underset{3}{\equiv}}, [1]_{\underset{3}{\equiv}}, [2]_{\underset{3}{\equiv}}$ (by Theorem 3.4.4).

Remark 4.2.25. Exercise 4.2.11 **(b)** yields $|\mathbb{Z}[i]/n| = n^2 = \mathrm{N}(n)$ for any positive integer n. This is essentially [ConradG, Lemma 7.15]. (Conrad proves this "by example"; you can follow the argument but you should write it up in full generality.)

More generally, $|\mathbb{Z}[i]/\tau| = \mathrm{N}(\tau)$ for any nonzero Gaussian integer τ. This is proven in [ConradG, Theorem 7.14] (using Exercise 4.2.11 as a stepping stone).

4.2.4. Division with remainder

Now, let us try to make division with remainder work for Gaussian integers. This turns out to be tricky: There is no straightforward analogue of Theorem 2.6.1 for Gaussian integers. (In fact, it is not clear what $\{0, 1, \ldots, b-1\}$ would mean if we let b be a Gaussian integer.) The best thing we can get for Gaussian integers is an analogue of Exercise 2.6.2 **(a)**:

Theorem 4.2.26. Let α and $\beta \neq 0$ be Gaussian integers. There exist Gaussian integers γ and ρ such that $\alpha = \gamma\beta + \rho$ and $\mathrm{N}(\rho) \leq \mathrm{N}(\beta)/2$.

Note that the pair (γ, ρ) in this theorem is not unique. As we have said, Theorem 4.2.26 is an analogue of Exercise 2.6.2 **(a)** (with α, β, γ and ρ taking the roles of u, n, q and r), not an analogue of Theorem 2.6.1; nevertheless, it is the closest we can get to Theorem 2.6.1 in $\mathbb{Z}[i]$, and can often be substituted in places where one would usually want to apply Theorem 2.6.1 (as long as one does not try to use uniqueness of quotient and remainder).

Theorem 4.2.26 can be visualized geometrically (similarly to the visualizations shown in Remark 2.6.8 and Remark 2.6.10, but using the Argand diagram). See [ConradG, §7] for the details.

The following proof of Theorem 4.2.26 follows [ConradG, proof of Theorem 3.1].

Note that we cannot define $\alpha//\beta$ or $\alpha\%\beta$ for Gaussian integers α and β, since there is no uniqueness statement in Theorem 4.2.26.

4.2.5. Common divisors

Next, we define the Gaussian divisors of a Gaussian integer (in analogy to Definition 2.9.1):

Definition 4.2.27. Let $\beta \in \mathbb{Z}[i]$. The *Gaussian divisors* of β are defined as the Gaussian integers that divide β.

Note that we are calling them "Gaussian divisors" and not "divisors", because when β is an actual integer, there are (usually) Gaussian divisors of β that are not divisors of β (in the sense of Definition 2.9.1). For example, $1+i$ is a Gaussian divisor of 2 (since $2 = (1+i)(1-i)$), but the only divisors of 2 (in the sense of Definition 2.9.1) are $-2, -1, 1, 2$. This is one of those situations where using the same name for a concept and its Gaussian-integer analogue would lead to ambiguities.

The following is an analogue of Proposition 2.9.2:

Proposition 4.2.28. **(a)** If $\beta \in \mathbb{Z}[i]$, then 1 and β are Gaussian divisors of β.
(b) The Gaussian divisors of 0 are all the Gaussian integers.
(c) Let $\beta \in \mathbb{Z}[i]$ be nonzero. Then, all Gaussian divisors of β belong to the set

$$\left\{ x+yi \mid x,y \in \mathbb{Z} \text{ satisfying } x^2 \leq \mathrm{N}(\beta) \text{ and } y^2 \leq \mathrm{N}(\beta) \right\}.$$

Thus, again, finding all Gaussian divisors of a Gaussian integer β is a problem solvable in finite time. (Indeed, if $\beta = 0$, then Proposition 4.2.28 **(b)** answers this question; but otherwise, the set in Proposition 4.2.28 **(c)** is clearly finite.)

The following is a straightforward analogue of Definition 2.9.3:

Definition 4.2.29. Let $\beta_1, \beta_2, \ldots, \beta_k$ be Gaussian integers. Then, the *common Gaussian divisors* of $\beta_1, \beta_2, \ldots, \beta_k$ are defined to be the Gaussian integers α that satisfy

$$(\alpha \mid \beta_i \text{ for all } i \in \{1,2,\ldots,k\}) \tag{44}$$

(in other words, that divide all of the Gaussian integers $\beta_1, \beta_2, \ldots, \beta_k$). We let $\mathrm{Div}_{\mathbb{Z}[i]}(\beta_1, \beta_2, \ldots, \beta_k)$ denote the set of these common Gaussian divisors.

The reason why I chose the notation $\mathrm{Div}_{\mathbb{Z}[i]}(\beta_1, \beta_2, \ldots, \beta_k)$ rather than the simpler notation $\mathrm{Div}(\beta_1, \beta_2, \ldots, \beta_k)$ is that the latter would be ambiguous. In fact, when $\beta_1, \beta_2, \ldots, \beta_k$ are integers, the set $\mathrm{Div}(\beta_1, \beta_2, \ldots, \beta_k)$ of common divisors of $\beta_1, \beta_2, \ldots, \beta_k$ is **not** the set $\mathrm{Div}_{\mathbb{Z}[i]}(\beta_1, \beta_2, \ldots, \beta_k)$ of common Gaussian divisors of $\beta_1, \beta_2, \ldots, \beta_k$. (For example, the former set does not contain i, while the latter does.)

We cannot directly define a "greatest common Gaussian divisor of $\beta_1, \beta_2, \ldots, \beta_k$" to be the greatest element of $\mathrm{Div}_{\mathbb{Z}[i]}(\beta_1, \beta_2, \ldots, \beta_k)$, since "greatest" does not make sense for complex numbers. (Even if we wanted "greatest in norm", it would not a-priori be obvious that there are no ties, i.e., that such a greatest common Gaussian divisor is unique.)

However, it turns out that a "greatest common Gaussian divisor" $\gcd_{\mathbb{Z}[i]}(\beta_1, \beta_2, \ldots, \beta_k)$ actually can be defined reasonably (although only up to multiplication by units). Before we can do so, let us state some basic properties of common Gaussian divisors:[58]

Proposition 4.2.30. **(a)** We have $\mathrm{Div}_{\mathbb{Z}[i]}(\alpha, 0) = \mathrm{Div}_{\mathbb{Z}[i]}(\alpha)$ for all $\alpha \in \mathbb{Z}[i]$.
(b) We have $\mathrm{Div}_{\mathbb{Z}[i]}(\alpha, \beta) = \mathrm{Div}_{\mathbb{Z}[i]}(\beta, \alpha)$ for all $\alpha, \beta \in \mathbb{Z}[i]$.
(c) We have $\mathrm{Div}_{\mathbb{Z}[i]}(\alpha, \eta\alpha + \beta) = \mathrm{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ for all $\alpha, \beta, \eta \in \mathbb{Z}[i]$.
(d) If $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ satisfy $\beta \equiv \gamma \bmod \alpha$, then $\mathrm{Div}_{\mathbb{Z}[i]}(\alpha, \beta) = \mathrm{Div}_{\mathbb{Z}[i]}(\alpha, \gamma)$.

[58] Proposition 4.2.30 is an analogue of part of Lemma 2.9.10. Thus, we have chosen to label its claims in a way that matches the corresponding claims in Lemma 2.9.10. This forced us to skip claim **(e)**, since there is no analogue of Lemma 2.9.10 **(e)** for Gaussian integers (because $\beta \% \alpha$ is not defined when β and α are Gaussian integers).

(f) We have $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) \subseteq \operatorname{Div}_{\mathbb{Z}[i]}(\alpha)$ and $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) \subseteq \operatorname{Div}_{\mathbb{Z}[i]}(\beta)$ for all $\alpha,\beta \in \mathbb{Z}[i]$.

(g) We have $\operatorname{Div}_{\mathbb{Z}[i]}(\eta\alpha,\beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta)$ for all $\alpha,\beta \in \mathbb{Z}[i]$ and every unit $\eta \in \mathbb{Z}[i]$.

(h) We have $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\eta\beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta)$ for all $\alpha,\beta \in \mathbb{Z}[i]$ and every unit $\eta \in \mathbb{Z}[i]$.

(i) If $\alpha,\beta \in \mathbb{Z}[i]$ satisfy $\alpha \mid \beta$, then $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha)$.

(j) The common Gaussian divisors of the empty list of Gaussian integers are $\operatorname{Div}_{\mathbb{Z}[i]}() = \mathbb{Z}[i]$.

You have reached the end of the finished part.
TODO: Write on from here.

Recall that Proposition 2.9.7 gave us a quick way to compute $\gcd(a,b)$ for two nonnegative integers a and b; this is called the Euclidean algorithm. Likewise, we can use Proposition 4.2.30 to compute $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta)$ for two Gaussian integers α and β (or, more precisely, to rewrite $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta)$ in the form $\operatorname{Div}_{\mathbb{Z}[i]}(\gamma)$ for a single Gaussian integer γ). For example, we can compute $\operatorname{Div}_{\mathbb{Z}[i]}(32+9i, 4+11i)$ as follows:[59]

$$
\begin{aligned}
&\operatorname{Div}_{\mathbb{Z}[i]}(32+9i, 4+11i) \\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(4+11i, \underbrace{32+9i}_{=(2-2i)(4+11i)+(2-5i)}\right) && \text{(by Proposition 4.2.30 \textbf{(b)})} \\
&= \operatorname{Div}_{\mathbb{Z}[i]}(4+11i, (2-2i)(4+11i)+(2-5i)) \\
&= \operatorname{Div}_{\mathbb{Z}[i]}(4+11i, 2-5i) && \text{(by Proposition 4.2.30 \textbf{(c)})} \\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(2-5i, \underbrace{4+11i}_{=(-2+i)(2-5i)+(3-i)}\right) && \text{(by Proposition 4.2.30 \textbf{(b)})} \\
&= \operatorname{Div}_{\mathbb{Z}[i]}(2-5i, (-2+i)(2-5i)+(3-i)) \\
&= \operatorname{Div}_{\mathbb{Z}[i]}(2-5i, 3-i) && \text{(by Proposition 4.2.30 \textbf{(c)})} \\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(3-i, \underbrace{2-5i}_{=(1-i)(3-i)-i}\right) && \text{(by Proposition 4.2.30 \textbf{(b)})}
\end{aligned}
$$

[59] This is [ConradG, Example 4.4].

$$
\begin{aligned}
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(3-i,(1-i)(3-i)-i\right) \\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(3-i,-i\right) \qquad \text{(by Proposition 4.2.30 \textbf{(c)})} \\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(-i, \underbrace{3-i}_{=(1+3i)(-i)+0}\right) \qquad \text{(by Proposition 4.2.30 \textbf{(b)})} \\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(-i,(1+3i)(-i)+0\right) \\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(-i,0\right) \qquad \text{(by Proposition 4.2.30 \textbf{(c)})} \\
&= \operatorname{Div}_{\mathbb{Z}[i]}\left(-i\right) \qquad \text{(by Proposition 4.2.30 \textbf{(a)})} \\
&= \{1,i,-1,-i\}.
\end{aligned}
$$

In the same way, for **any** two Gaussian integers α and β we can find a Gaussian integer γ such that $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\gamma)$. This resulting γ will actually be unique up to multiplication by units (i.e., its unit-equivalence class will be unique). Better yet, we have the following analogue of Bezout's theorem for Gaussian integers:

Theorem 4.2.31. Let $\alpha,\beta \in \mathbb{Z}[i]$. Then:

(a) There exists a $\mathbb{Z}[i]$-linear combination γ of α and β that is a common Gaussian divisor of α and β. (Note: A $\mathbb{Z}[i]$-*linear combination of* α *and* β means a Gaussian integer of the form $\lambda\alpha+\mu\beta$ with $\lambda,\mu \in \mathbb{Z}[i]$.)

(b) Any such γ satisfies $\operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta) = \operatorname{Div}_{\mathbb{Z}[i]}(\gamma)$.

(c) The unit-equivalence class of this γ is uniquely determined.

This theorem is, in a sense, a generalization of Theorem 2.9.12, even though (unlike the latter theorem) it does not rely on an already existing concept of "greatest common divisor" but rather builds the foundation for such a concept. With Theorem 4.2.31 in hand, it makes sense to call γ the "greatest common Gaussian divisor" of α and β, but rigorously speaking this name should be reserved for the unit-equivalence class of γ since γ itself is not unique.

Definition 4.2.32. The *greatest common Gaussian divisor* (or, short, *gcd*) of two Gaussian integers α and β is defined to be the γ from Theorem 4.2.31 **(a)**. It is called $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$.

So it is a common Gaussian divisor of α and β and also a $\mathbb{Z}[i]$-linear combination of α and β and satisfies

$$\operatorname{Div}_{\mathbb{Z}[i]}\left(\gcd_{\mathbb{Z}[i]}(\alpha,\beta)\right) = \operatorname{Div}_{\mathbb{Z}[i]}(\alpha,\beta). \tag{45}$$

However, it is only well-defined up to unit-equivalence. Thus, if you have $\gamma_1 = \gcd_{\mathbb{Z}[i]}(\alpha,\beta)$ and $\gamma_2 = \gcd_{\mathbb{Z}[i]}(\alpha,\beta)$, then you cannot conclude that $\gamma_1 = \gamma_2$ (you can only conclude $\gamma_1 \sim \gamma_2$). So, strictly speaking, we should have defined $\gcd_{\mathbb{Z}[i]}(\alpha,\beta)$ as a unit-equivalence class, not as a concrete Gaussian integer. But we will allow ourselves this abuse of notation. We shall not write equality

signs like the one in "$\gamma_1 = \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$", however; we instead prefer to write "$\gamma_1 \sim \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$". Generally, whenever you see $\gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ in a statement, you should be understanding the statement to hold for **every** possible choice of $\gcd_{\mathbb{Z}[i]}(\alpha, \beta)$.

Proposition 4.2.33. Let a and b be two integers. Then,

$$\gcd(a, b) \sim \gcd_{\mathbb{Z}[i]}(a, b).$$

(Of course, the gcd on the left hand side is the gcd of the two integers a and b as defined in Definition 2.9.6, whereas the $\gcd_{\mathbb{Z}[i]}$ on the right hand side is the greatest common Gaussian divisor of the Gaussian integers a and b.)

This proposition allows us to write "gcd" for both concepts of gcd without having to disambiguate the meaning. (We shall not do so, however.)

Proposition 4.2.34. Let α and β be two Gaussian integers, not both equal to 0. Then, the possible values of $\gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ (that is, strictly speaking, all four elements of the unit-equivalence class $\gcd_{\mathbb{Z}[i]}(\alpha, \beta)$) are exactly the elements of $\mathrm{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$ having the largest norm.

Proposition 4.2.34 shows that $\gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ is uniquely determined by the set $\mathrm{Div}_{\mathbb{Z}[i]}(\alpha, \beta)$. (Yes, you have to consider the case $\alpha = \beta = 0$ separately in proving this.) Hence, Proposition 4.2.30 yields:

Proposition 4.2.35. **(a)** We have $\gcd_{\mathbb{Z}[i]}(\alpha, 0) \sim \gcd_{\mathbb{Z}[i]}(\alpha)$ for all $\alpha \in \mathbb{Z}[i]$.
(b) We have $\gcd_{\mathbb{Z}[i]}(\alpha, \beta) \sim \gcd_{\mathbb{Z}[i]}(\beta, \alpha)$ for all $\alpha, \beta \in \mathbb{Z}[i]$.
(c) We have $\gcd_{\mathbb{Z}[i]}(\alpha, \eta\alpha + \beta) \sim \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ for all $\alpha, \beta, \eta \in \mathbb{Z}[i]$.
(d) If $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ satisfy $\beta \equiv \gamma \bmod \alpha$, then $\gcd_{\mathbb{Z}[i]}(\alpha, \beta) \sim \gcd_{\mathbb{Z}[i]}(\alpha, \gamma)$.
(g) We have $\gcd_{\mathbb{Z}[i]}(\eta\alpha, \beta) \sim \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$ and every unit $\eta \in \mathbb{Z}[i]$.
(h) We have $\gcd_{\mathbb{Z}[i]}(\alpha, \eta\beta) \sim \gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ for all $\alpha, \beta \in \mathbb{Z}[i]$ and every unit $\eta \in \mathbb{Z}[i]$.
(i) If $\alpha, \beta \in \mathbb{Z}[i]$ satisfy $\alpha \mid \beta$, then $\gcd_{\mathbb{Z}[i]}(\alpha, \beta) \sim \gcd_{\mathbb{Z}[i]}(\alpha)$.
(j) The greatest common Gaussian divisor of the empty list of Gaussian integers is $\gcd_{\mathbb{Z}[i]}() = 0$.

Theorem 2.9.15 still holds for Gaussian integers.
Theorem 2.9.17 still holds for Gaussian integers.
Theorem 2.9.19 still holds for Gaussian integers.
Theorem 2.9.20 has to be modified as follows:

Corollary 4.2.36. Let $\sigma, \alpha, \beta \in \mathbb{Z}[i]$. Then,

$$\gcd_{\mathbb{Z}[i]}(\sigma\alpha, \sigma\beta) \sim \sigma \gcd_{\mathbb{Z}[i]}(\alpha, \beta).$$

Exercise 2.9.4 still holds for Gaussian integers.

Exercise 2.9.5 becomes the claim that if $\alpha_1 \sim \alpha_2$ and $\beta_1 \sim \beta_2$, then $\gcd_{\mathbb{Z}[i]}(\alpha_1, \beta_1) \sim \gcd_{\mathbb{Z}[i]}(\alpha_2, \beta_2)$. The solution does not carry over, but you can easily prove this new claim by hand.

Greatest common Gaussian divisors of k Gaussian integers can also be defined.

The next definition is an analogue of Definition 2.10.1:

Definition 4.2.37. Let α and β be two Gaussian integers. We say that α is *coprime* to β if and only if $\gcd_{\mathbb{Z}[i]}(\alpha, \beta) \sim 1$ (that is, $\gcd_{\mathbb{Z}[i]}(\alpha, \beta)$ is a unit).

Thus, any two coprime integers are also two coprime Gaussian integers (because of Proposition 4.2.33), and vice versa (for the same reason). This is why we can afford speaking of "coprime Gaussian integers" and not just "Gaussian-coprime Gaussian integers".

Everything we said about coprimality of integers still holds for Gaussian integers. In particular, Proposition 2.10.4, Theorem 2.10.6, Theorem 2.10.7, Theorem 2.10.8 and Theorem 2.10.9 still hold if all integers are replaced by Gaussian integers (with the caveat that the gcd is no longer unique, so for example "$ab \equiv \gcd(a, n) \bmod n$" must be interpreted as "ab is congruent to **some** of the possible values of $\gcd_{\mathbb{Z}[i]}(a, n)$ modulo n").

We could define *Gaussian rationals* (their set is called $\mathbb{Q}[i]$) as complex numbers $a + bi$ with $a, b \in \mathbb{Q}$. These are exactly the quotients of Gaussian integers.

Lowest common multiples of Gaussian integers still exist, but their definition has to be modified. For example, we can define $\operatorname{lcm}_{\mathbb{Z}[i]}(\alpha, \beta)$ as the (unique up to unit-equivalence) Gaussian integer γ such that the Gaussian common multiples of α and β are the Gaussian multiples of γ. (We would have to prove that it actually is unique and exists.) Theorem 2.11.6 still holds, in the sense that $\gcd_{\mathbb{Z}[i]}(\alpha, \beta) \cdot \operatorname{lcm}_{\mathbb{Z}[i]}(\alpha, \beta) \sim \alpha\beta$. Many other properties of lowest common multiples extend to Gaussian integers.

The Chinese remainder theorem (Theorem 2.12.1) still holds for coprime Gaussian integers μ and ν. A similar fact holds for k mutually coprime Gaussian integers.

4.2.6. Gaussian primes

The next definition is an analogue of Definition 2.13.1:

Definition 4.2.38. Let π be a nonzero Gaussian integer that is not a unit. We say that π is a *Gaussian prime* if each Gaussian divisor of π is either a unit or unit-equivalent to π.

The letter "π" in this definition is unrelated to the irrational number $\pi = 3.14159\ldots$. It just happens to be the Greek letter corresponding to the Roman "p".

The Gaussian primes are **not** a superset of the primes. For example:

Example 4.2.39. The Gaussian integer 2 is not a Gaussian prime.

So don't forget the word "Gaussian" when you mean it!

Let us search for Gaussian primes. So we know that 2 is not a Gaussian prime. What about 3?

Example 4.2.40. The Gaussian integer 3 is a Gaussian prime.

So we know that 3 is a Gaussian prime, but 2 is not. Is there a way to tell which integers are Gaussian primes, without checking all Gaussian divisors?

Let us first state a positive criterion, which generalizes Example 4.2.40:

Lemma 4.2.41. Let p be a prime such that $p \equiv 3 \bmod 4$. Then, p is a Gaussian prime.

It is clear that no prime is divisible by 4. Thus, there are three types of primes:

- *Type 1:* Primes that are $\equiv 1 \bmod 4$: these are $5, 13, 17, 29, \ldots$.
- *Type 2:* Primes that are even: there is only one of these, namely 2.
- *Type 3:* Primes that are $\equiv 3 \bmod 4$: these are $3, 7, 11, 19, 23, \ldots$.

(One can show that there are infinitely many primes of Type 1 and infinitely many primes of Type 3. It can also be shown that there are "roughly the same amount" of Type-1 primes and of Type-3 primes "in theory", but "in practice" the Type-3 primes are more frequent. For the concrete meaning of this weird paradoxical claim, google for "Chebyshev's bias".)

Lemma 4.2.41 says that all Type-3 primes are Gaussian primes. What about the other primes – are they Gaussian primes? We already know that 2 is not, since $2 = (1+i)(1-i)$. Likewise, 5 is not, since $5 = (1+2i)(1-2i)$. Likewise, 13 is not, since $13 = (2+3i)(2-3i)$.

This may suggest that primes p satisfying $p = 2$ or $p \equiv 1 \bmod 4$ (that is, primes of Type 1 or Type 2) not only factor nontrivially, but actually factor as

$$p = (x+yi)(x-yi) \qquad \text{for some integers } x \text{ and } y.$$

Of course, this equation rewrites as $p = x^2 + y^2$. Thus, we are back to asking Question 1.4.1, at least for primes.

We shall now answer this question, and actually prove a bit more:

Theorem 4.2.42. Let p be a prime such that either $p = 2$ or $p \equiv 1 \bmod 4$.

(a) There exist integers x and y such that $p = x^2 + y^2$.

(b) If $p \equiv 1 \bmod 4$, then there exist exactly 8 pairs (x, y) of integers such that $p = x^2 + y^2$. (For example, if $p = 5$, then these 8 pairs are $(1, 2)$, $(2, 1)$, $(1, -2)$, $(-2, 1)$, $(-1, 2)$, $(2, -1)$, $(-1, -2)$ and $(-2, -1)$.)

(c) There exists a Gaussian prime π such that $p = \pi\overline{\pi}$.

(d) The Gaussian integer p itself is not a Gaussian prime.

(e) Assume that $p \equiv 1 \bmod 4$. Consider the Gaussian prime π from Theorem 4.2.42 **(c)**. Then, $\overline{\pi}$ is also a Gaussian prime, and we do not have $\pi \sim \overline{\pi}$.

For example, the Type-1 prime 17 satisfies

$$\begin{aligned} 17 &= 1^2 + 4^2 = (1 + 4i)(1 - 4i) = (1 + 4i)\left(\overline{1 + 4i}\right) \\ &= (1 - 4i)\left(\overline{1 - 4i}\right) = (4 + i)\left(\overline{4 + i}\right). \end{aligned}$$

Note that the claim of Theorem 4.2.42 **(a)** (at least for $p \neq 2$) also appears in [AigZie18, Proposition in Chapter 4], with a very different proof.

Before we can prove Theorem 4.2.42, we will have to build up the theory of Gaussian primes a bit more. We first state the Gaussian-integer analogue of Proposition 2.13.5:

Proposition 4.2.43. Let π be a Gaussian prime. Let $\alpha \in \mathbb{Z}[i]$. Then, either $\pi \mid \alpha$ or $\pi \perp \alpha$.

Next, we state the analogue to Theorem 2.13.6:

Theorem 4.2.44. Let π be a Gaussian prime. Let $\alpha, \beta \in \mathbb{Z}[i]$ such that $\pi \mid \alpha\beta$. Then, $\pi \mid \alpha$ or $\pi \mid \beta$.

We also need the following simple fact:

Lemma 4.2.45. Let α be a Gaussian integer. If $\mathrm{N}(\alpha)$ is prime, then α is a Gaussian prime.

This shows, for example, that $1 + i$ and $1 + 2i$ are Gaussian primes. The converse of Lemma 4.2.45 does not hold (e.g., since 3 is a Gaussian prime, but $\mathrm{N}(3) = 9$ is not prime).

Next, let us show that conjugation does not change Gaussian primeness:

Lemma 4.2.46. Let π be a Gaussian prime. Then, $\overline{\pi}$ is a Gaussian prime, too.

Now, we can prove Theorem 4.2.42:

We have thus answered Question 1.4.2 **(b)** in the case when n is a prime: We have shown that a prime p is a sum of two perfect squares if and only if either $p = 2$ or $p \equiv 1 \bmod 4$; and we have shown that the number of pairs $(x, y) \in \mathbb{Z}^2$ satisfying

$p = x^2 + y^2$ is 8 when $p \equiv 1 \bmod 4$ and is 4 when $p = 2$ (the latter claim is easy to check).

What about the case of arbitrary n?

For $n = 21$, we have $n \equiv 1 \bmod 4$, but n is not a sum of two perfect squares. So the answer we gave for the case of prime n does not generalize to arbitrary n.

It turns out that the right answer for arbitrary n will come from the analogue of prime factorization in $\mathbb{Z}[i]$.

Proposition 4.2.47. Let ν be a nonzero Gaussian integer that is not a unit. Then, there exists at least one Gaussian prime π such that $\pi \mid \nu$.

Proposition 4.2.48. Let ν be a nonzero Gaussian integer. Then, ν is unit-equivalent to a certain product of finitely many Gaussian primes.

Definition 4.2.49. Let ν be a nonzero Gaussian integer. A *Gaussian prime factorization* of ν means a tuple $(\pi_1, \pi_2, \ldots, \pi_k)$ of Gaussian primes such that $\nu \sim \pi_1 \pi_2 \cdots \pi_k$.

Why did we require only $\nu \sim \pi_1 \pi_2 \cdots \pi_k$ and not $\nu = \pi_1 \pi_2 \cdots \pi_k$? Because we want -1 to have a Gaussian prime factorization, but there is no way to literally write -1 as a product of Gaussian primes.

Exercise 4.2.12. Let π and κ be two Gaussian primes that do not satisfy $\pi \sim \kappa$. Prove that $\pi \perp \kappa$.

Lemma 4.2.50. Let π be a Gaussian prime. Let α be a nonzero Gaussian integer. Then, there exists a largest $m \in \mathbb{N}$ such that $\pi^m \mid \alpha$.

Similarly to Definition 2.13.23, we can define π-adic valuations:

Definition 4.2.51. Let π be a Gaussian prime.

(a) Let α be a nonzero Gaussian integer. Then, $v_\pi(\alpha)$ shall denote the largest $m \in \mathbb{N}$ such that $\pi^m \mid \alpha$. This is well-defined (by Lemma 4.2.50). This nonnegative integer $v_\pi(\alpha)$ will be called the *π-valuation* (or the *π-adic valuation*) of α.

(b) We extend this definition of $v_\pi(\alpha)$ to the case of $\alpha = 0$ as follows: Set $v_\pi(0) = \infty$.

Definition 4.2.51 does not conflict with Definition 2.13.23. Indeed, if a prime p happens to also be a Gaussian prime, and if n is an integer, then both definitions yield the same value of $v_p(n)$ (since $p^m \mid a$ means the same thing whether we treat p and a as integers or as Gaussian integers).

Theorem 4.2.52. Let π be a Gaussian prime.

(a) We have $v_\pi(\alpha\beta) = v_\pi(\alpha) + v_\pi(\beta)$ for any two Gaussian integers α and β.

(b) We have $v_\pi(\alpha+\beta) \geq \min\{v_\pi(\alpha), v_\pi(\beta)\}$ for any two Gaussian integers α and β.

(c) We have $v_\pi(1) = 0$. More generally, $v_\pi(\alpha) = 0$ for any unit $\alpha \in \mathbb{Z}[i]$.

(d) We have $v_\pi(\kappa) = \begin{cases} 1, & \text{if } \kappa \sim \pi; \\ 0, & \text{otherwise} \end{cases}$ for any Gaussian prime κ.

Proposition 4.2.53. Let ν be a nonzero Gaussian integer. Let $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ be a Gaussian prime factorization of ν. Let π be a Gaussian prime. Then,

$$\begin{aligned}
&(\text{the number of times a Gaussian integer unit-equivalent to } \pi \\
&\qquad \text{appears in the tuple } (\alpha_1, \alpha_2, \ldots, \alpha_k)) \\
&= (\text{the number of times } [\pi]_\sim \text{ appears in the tuple } ([\alpha_1]_\sim, [\alpha_2]_\sim, \ldots, [\alpha_k]_\sim)) \\
&= (\text{the number of } i \in \{1,2,\ldots,k\} \text{ such that } \alpha_i \sim \pi) \\
&= (\text{the number of } i \in \{1,2,\ldots,k\} \text{ such that } [\alpha_i]_\sim = [\pi]_\sim) \\
&= v_\pi(\nu).
\end{aligned}$$

Theorem 4.2.54. Let ν be a nonzero Gaussian integer.

(a) There exists a Gaussian prime factorization of ν.

(b) Any two such factorizations differ only by reordering their entries and multiplying them by units. More precisely: If $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ and $(\beta_1, \beta_2, \ldots, \beta_\ell)$ are two Gaussian prime factorizations of ν, then $([\alpha_1]_\sim, [\alpha_2]_\sim, \ldots, [\alpha_k]_\sim)$ is a permutation of $([\beta_1]_\sim, [\beta_2]_\sim, \ldots, [\beta_\ell]_\sim)$.

Example 4.2.55. We have

$$5 = (1+2i)(1-2i) = (2+i)(2-i).$$

Thus, both $(1+2i, 1-2i)$ and $(2+i, 2-i)$ are Gaussian prime factorizations of 5. They may look different, but actually you get the second one from the first by swapping the two entries and multiplying the first entry by the unit i and multiplying the second entry by the unit $-i$. This perfectly agrees with Theorem 4.2.54.

In analogy to Exercise 2.13.5 (and with the same proof), we have:

Exercise 4.2.13. Let π be a Gaussian prime. Let $\alpha, \beta \in \mathbb{Z}[i]$ be such that $\alpha \sim \beta$. Prove that $v_\pi(\alpha) = v_\pi(\beta)$.

We also have the following:

Exercise 4.2.14. Let π be a Gaussian prime. Let $\alpha \in \mathbb{Z}[i]$. Then, $\overline{\pi}$ is a Gaussian prime as well, and satisfies

$$v_{\overline{\pi}}(\overline{\alpha}) = v_{\pi}(\alpha).$$

Definition 4.2.56. For the rest of this section, let GP be the set of all Gaussian primes of the form $x + yi$ with $x \in \{1, 2, 3, \ldots\}$ and $y \in \{0, 1, 2, \ldots\}$.

The following is easy to see:

Lemma 4.2.57. Let π be a Gaussian prime. Then, there exists **exactly one** $\sigma \in \mathrm{GP}$ such that $\pi \sim \sigma$.

In other words, each Gaussian prime is unit-equivalent to exactly one $\sigma \in \mathrm{GP}$. Thus, the set GP contains exactly one element of each unit-equivalence class of Gaussian primes. (Thus, GP is what is called a "system of distinct representatives" for the unit-equivalence classes of all Gaussian primes.)

In analogy to Corollary 2.13.34, we have:

Corollary 4.2.58. Let α be a nonzero Gaussian integer. Then,

$$\alpha \sim \prod_{\pi \in \mathrm{GP}} \pi^{v_{\pi}(\alpha)}.$$

Here, the infinite product $\prod_{\pi \in \mathrm{GP}} \pi^{v_{\pi}(\alpha)}$ is well-defined (according to the Gaussian-integer analogue of Lemma 2.13.32 **(b)**).

In analogy to Proposition 2.13.35, we have the following:

Proposition 4.2.59. Let α and β be Gaussian integers. Then, $\alpha \mid \beta$ if and only if each Gaussian prime π satisfies $v_{\pi}(\alpha) \leq v_{\pi}(\beta)$.

If α is a Gaussian integer, and c is a unit-equivalence class of Gaussian integers, then either all elements of c divide α or none of them does.[60] Thus, we can talk of *unit-equivalence classes of Gaussian divisors of* α (by which we mean unit-equivalence classes of Gaussian integers whose elements all divide α).

Here is an analogue of Proposition 2.18.1 for Gaussian integers:

Proposition 4.2.60. Let $\alpha \in \mathbb{Z}[i]$ be a nonzero Gaussian integer. Then:

(a) The product $\prod_{\pi \in \mathrm{GP}} (v_{\pi}(\alpha) + 1)$ is well-defined, since all but finitely many of its factors are 1.

[60] This is easy to check. Indeed, it boils down to the fact that any two elements of c divide each other (because they are unit-equivalent).

(b) We have

$$\begin{aligned}&\left(\text{the number of unit-equivalence classes of Gaussian divisors of } \alpha\right)\\ &= \prod_{\pi \in \mathrm{GP}} \left(v_\pi\left(\alpha\right)+1\right).\end{aligned}$$

(c) We have

$$\left(\text{the number of Gaussian divisors of } \alpha\right) = 4 \cdot \prod_{\pi \in \mathrm{GP}} \left(v_\pi\left(\alpha\right)+1\right).$$

Lemma 4.2.61. Let $\pi_1, \pi_2, \ldots, \pi_u$ be finitely many Gaussian primes, no two of which are unit-equivalent. For each $i \in \{1,2,\ldots,u\}$, let a_i be a nonnegative integer. Let $\alpha = \pi_1^{a_1}\pi_2^{a_2}\cdots\pi_u^{a_u}$.

Define a set T by

$$\begin{aligned}T &= \{0,1,\ldots,a_1\} \times \{0,1,\ldots,a_2\} \times \cdots \times \{0,1,\ldots,a_u\}\\ &= \{(b_1,b_2,\ldots,b_u) \mid b_i \in \{0,1,\ldots,a_i\} \text{ for each } i \in \{1,2,\ldots,u\}\}\\ &= \{(b_1,b_2,\ldots,b_u) \in \mathbb{N}^u \mid b_i \leq a_i \text{ for each } i \in \{1,2,\ldots,u\}\}.\end{aligned}$$

Then, the map

$$\begin{aligned}\Lambda : T &\to \{\text{unit-equivalence classes of Gaussian divisors of } \alpha\},\\ (b_1,b_2,\ldots,b_u) &\mapsto \left[\pi_1^{b_1}\pi_2^{b_2}\cdots\pi_u^{b_u}\right]_\sim\end{aligned}$$

is well-defined and bijective.

Now, we can finally answer Question 1.4.2 **(b)** (following [DumFoo04, §8.3, Corollary 19]):

Theorem 4.2.62. Let n be a positive integer.

(a) If there is at least one prime $p \equiv 3 \bmod 4$ such that $v_p\left(n\right)$ is odd, then there is **no** pair $(x,y) \in \mathbb{Z}^2$ such that $n = x^2+y^2$.

(b) Assume that for each prime $p \equiv 3 \bmod 4$, the number $v_p\left(n\right)$ is even. Then,

$$\begin{aligned}&\left(\text{the number of pairs } (x,y) \in \mathbb{Z}^2 \text{ such that } n = x^2+y^2\right)\\ &= 4 \cdot \prod_{\substack{p \text{ prime};\\ p \equiv 1 \bmod 4}} \left(v_p\left(n\right)+1\right).\end{aligned}$$

Example 4.2.63. **(a)** Let $n = 35$. Then, Theorem 4.2.62 **(a)** yields that there are **no** integers x and y such that $n = x^2 + y^2$. In fact, the prime $7 \equiv 3 \bmod 4$ satisfies $v_7(n) = 1$.

(b) Let $n = 45$. Then, for each prime $p \equiv 3 \bmod 4$, the number $v_p(n)$ is even. Indeed, $n = 45 = 3^2 \cdot 5$, so $v_3(n) = 2$ is even and $v_p(n) = 0$ for all other primes p of Type 3. Hence, Theorem 4.2.62 **(b)** yields

$$\begin{aligned}&\left(\text{the number of pairs } (x,y) \in \mathbb{Z}^2 \text{ such that } n = x^2 + y^2\right) \\ &= 4 \cdot \underbrace{\prod_{\substack{p \text{ prime;} \\ p \equiv 1 \bmod 4}} \left(v_p(n) + 1\right)}_{\substack{= v_5(n)+1 \\ = 1+1 = 2}} = 4 \cdot 2 = 8.\end{aligned}$$

One consequence of Theorem 4.2.62 is that a positive integer n can be written in the form $x^2 + y^2$ with $x, y \in \mathbb{Z}$ if and only if it has the property that for each prime $p \equiv 3 \bmod 4$, the number $v_p(n)$ is even. A different proof of this fact appears in [AigZie18, Theorem in Chapter 4].

4.2.7. What are the Gaussian primes?

We have so far seen the following Gaussian primes:

- Each prime of Type 3 is a Gaussian prime.
- $1 + i$ is a Gaussian prime.
- For each prime p of Type 1, we have a Gaussian prime π such that $p = \pi\overline{\pi}$, and then $\overline{\pi}$ is also a Gaussian prime.

Theorem 4.2.64. Each Gaussian prime is unit-equivalent to one of the Gaussian primes in this list.

4.3. Brief survey of similar number systems

- Let us now see when a prime p can be written as $x^2 + 2y^2$ with $x, y \in \mathbb{Z}$.

  The set
  $$\mathbb{Z}\left[\sqrt{-2}\right] = \mathbb{Z}\left[\sqrt{2}i\right]$$
  is defined as the set of all complex numbers of the form $a + b\sqrt{2}i$ with $a, b \in \mathbb{Z}$. It is perhaps easier to regard it as its own variant of Gaussian

integers, which I will call the "2-Gaussian integers". These "2-Gaussian integers" can be defined as pairs $(a,b) \in \mathbb{Z}^2$ with addition and subtraction defined entrywise and multiplication defined by

$$(a,b)(c,d) = (ac - 2bd, ad + bc).$$

[61] You can then write such pairs (a,b) as $a + b\sqrt{2}i$, where $\sqrt{2}i$ is simply a symbol for the 2-Gaussian integer $(0,1)$. Each 2-Gaussian integer (a,b) has a norm, defined by $\mathrm{N}((a,b)) = a^2 + 2b^2$.

Much of the theory of Gaussian integers still applies verbatim to 2-Gaussian integers. In particular, division with remainder still works for 2-Gaussian integers (like it does for Gaussian integers, i.e., non-uniquely), and the proof uses the same argument, but this time we have $\mathrm{N}(\rho) \leq 3\,\mathrm{N}(\beta)/4$ instead of $\mathrm{N}(\rho) \leq \mathrm{N}(\beta)/2$. Hence, 2-Gaussian integers have unique factorizations into "2-Gaussian primes".

This can be used to show that a prime p can be written as $x^2 + 2y^2$ if and only if there is an integer u satisfying $u^2 \equiv -2 \bmod p$. It can furthermore be shown that such an integer u exists if and only if $p = 2$ or $p \equiv 1, 3 \bmod 8$ (where "$p \equiv 1, 3 \bmod 8$" is shorthand for "$p \equiv 1 \bmod 8$ or $p \equiv 3 \bmod 8$"). The proof uses a fact called *quadratic reciprocity*, which we **may** see later in this course.

- When can a prime p be written as $x^2 + 3y^2$ with $x, y \in \mathbb{Z}$?

  The logical continuation of the above pattern would be "when $p = 3$ or $p \equiv 1 \bmod 3$", since these are the cases when there is an integer u satisfying $u^2 \equiv -3 \bmod p$. And that is indeed true, but the proof is more complicated. Indeed, the "3-Gaussian integers" no longer have division with remainder, as $\mathrm{N}(\rho) \leq \mathrm{N}(\beta)/2$ turns into $\mathrm{N}(\rho) \leq \mathrm{N}(\beta)$ which is not a strict inequality. Nevertheless we can prove our guess with more complicated reasoning: We need to use not $\mathbb{Z}\left[\sqrt{-3}\right]$ but rather the *Eisenstein integers* $a + b\omega$ with $a, b \in \mathbb{Z}$ and $\omega = \dfrac{-1 + i\sqrt{3}}{2}$. These are best understood as pairs $(a,b) \in \mathbb{Z}^2$ with addition and subtraction defined entrywise and multiplication defined by

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

  Their norm is $\mathrm{N}((a,b)) = a^2 - ab + b^2$. They form a triangular lattice, not a rectangular one, and they do have division with remainder. Note that $\mathrm{N}(a + b\omega) = a^2 - ab + b^2$, so some more work is needed to turn them into $x^2 + 3y^2$ solutions, but it's doable.

[61] Be careful, however: This definition of 2-Gaussian integers as pairs of integers conflicts with the definition of complex numbers as pairs of reals; the 2-Gaussian integer (a,b) and the complex number (a,b) are two different numbers (unless $b = 0$).

- When can a prime p be written as $x^2 + 4y^2$ with $x, y \in \mathbb{Z}$?

  This is easy: $4y^2 = (2y)^2$, so we are looking for a way of writing p as $x^2 + y^2$ with y even.

  I claim that the answer is "when $p \equiv 1 \bmod 4$". Do you see why?

- When can a prime p be written as $x^2 + 5y^2$ with $x, y \in \mathbb{Z}$?

  Our guess, by following the above pattern, would be "when $p = 2$ or $p = 5$ or $p \equiv 1, 3, 7, 9 \bmod 20$", since these are the cases when there is an integer u satisfying $u^2 \equiv -5 \bmod p$. But this is not true anymore. The right answer is "when $p = 2$ or $p = 5$ or $p \equiv 1, 9 \bmod 20$". And unsurprisingly, $\mathbb{Z}\left[\sqrt{-5}\right]$ does not have division with remainder.

- More generally, you can fix $n \in \mathbb{N}$ and ask when a prime can be written in the form $x^2 + ny^2$. There is a whole book [Cox13] devoted to this question! The answer becomes more complicated with n getting large, and touches on a surprising number of different fields of mathematics (geometry, complex analysis, elliptic functions and elliptic curves).

- We can also ask when a prime p can be written as $x^2 - ny^2$. The appropriate analogue of $\mathbb{Z}[i]$ tailored to this question is $\mathbb{Z}\left[\sqrt{n}\right]$, which however behaves much differently, since $\sqrt{n}$ is real. For example, as you saw on homework set #4 (in the Remark after Exercise 4), there are infinitely many units in $\mathbb{Z}\left[\sqrt{2}\right]$; the same is true for each $\mathbb{Z}\left[\sqrt{n}\right]$ with $n > 1$ and n not being a perfect square (but this is much harder to prove).

- When can an $n \in \mathbb{N}$ be written as a sum of three squares? Legendre's three-squares theorem says that the answer is "if and only if n is not of the form $n = 4^a (8b + 7)$ for $a, b \in \mathbb{N}$". This is very hard to prove ([UspHea39, Chapter XIII] might have the only elementary proof).

- When can an $n \in \mathbb{N}$ be written as a sum of four squares? Lagrange's four-squares theorem reveals that the answer to this question is "always"![62] This is easier to show, and there is even a formula for the number of representations: it is $8 \sum\limits_{\substack{d \mid n; \\ 4 \nmid d}} d$. The existence part can be proven using "Hurwitz integers", which are certain quaternions.

[62] An application (fortunately, no longer relevant):

"`Warning: Due to a known bug, the default Linux document viewer evince prints N*N copies of a PDF file when N copies requested. As a workaround, use Adobe Reader acroread for printing multiple copies of PDF documents, or use the fact that every natural number is a sum of at most four squares.`"

5. Rings and fields

5.1. Definition of a ring

We have seen several "number systems" in the above chapters:

- $\mathbb{N}$ (the nonnegative integers);
- $\mathbb{Z}$ (the integers);
- $\mathbb{R}$ (the real numbers);
- $\mathbb{Z}/n$ (the residue classes modulo n) for an integer n;
- $\mathbb{C}$ (the complex numbers);
- $\mathbb{Z}[i]$ (the Gaussian integers);
- $\mathbb{D}$ (the dual numbers – see homework set #4 exercise 3);
- $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$ (see homework set #4 exercise 4);
- $\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ (the Eisenstein integers);
- $\mathbb{Z}\left[\sqrt{-3}\right]$ (see homework set #5 exercise 6).

It may be a stretch to refer to the elements of some of these systems as "numbers", but it is not taboo (the word "number" has no precise meaning in mathematics), and these sets have a lot in common: We can add, subtract and multiply their elements (except for $\mathbb{N}$, which does not allow subtraction); these operations satisfy the usual rules (e.g., associativity of multiplication, distributivity, etc.); these sets contain some element "behaving like 0" (that is, an element $\mathbf{0}$ such that $a + \mathbf{0} = \mathbf{0} + a = a$ and $a \cdot \mathbf{0} = \mathbf{0} \cdot a = \mathbf{0}$ for all a) and some element "behaving like 1" (that is, an element $\mathbf{1}$ such that $a \cdot \mathbf{1} = \mathbf{1} \cdot a = a$ for all a). It turns out that just a few of these rules are sufficient to make "all the other rules" (in a certain appropriate sense) follow from them. Thus, it is reasonable to crystallize these few rules into a common, general notion (of which the above examples – excluding $\mathbb{N}$ – will be particular cases); this notion will be called a "**ring**". Hence, we shall define a **ring** to be (roughly speaking) a set with operations $+$ and $\cdot$ and elements 0 and 1 that satisfy these few rules. Let us be specific about what these rules are:[63]

Definition 5.1.1. (a) A *ring* means a set $\mathbb{K}$ endowed with

- two binary operations called "*addition*" and "*multiplication*", and denoted by $+_{\mathbb{K}}$ and $\cdot_{\mathbb{K}}$, respectively, and

[63] Recall the definition of a "binary operation" (Definition 1.6.1). In particular, a binary operation on a set S must have all its values in S.

- two elements called "*zero*" (or "*origin*") and "*unity*" (or "*one*"), and denoted by $0_{\mathbb{K}}$ and $1_{\mathbb{K}}$, respectively

such that the following axioms are satisfied:

- **Commutativity of addition:** We have $a +_{\mathbb{K}} b = b +_{\mathbb{K}} a$ for all $a, b \in \mathbb{K}$.
- **Associativity of addition:** We have $a +_{\mathbb{K}} (b +_{\mathbb{K}} c) = (a +_{\mathbb{K}} b) +_{\mathbb{K}} c$ for all $a, b, c \in \mathbb{K}$.
- **Neutrality of zero:** We have $a +_{\mathbb{K}} 0_{\mathbb{K}} = 0_{\mathbb{K}} +_{\mathbb{K}} a = a$ for all $a \in \mathbb{K}$.
- **Existence of additive inverses:** For any $a \in \mathbb{K}$, there exists an element $a' \in \mathbb{K}$ such that $a +_{\mathbb{K}} a' = a' +_{\mathbb{K}} a = 0_{\mathbb{K}}$. (It is not **immediately** obvious, but will be shown later, that such an a' is unique. Thus, a' is called the *additive inverse* of a, and is denoted by $-a$.)
- **Associativity of multiplication:** We have $a(bc) = (ab)c$ for all $a, b, c \in \mathbb{K}$. Here and in the following, we use "xy" as an abbreviation for "$x \cdot_{\mathbb{K}} y$".
- **Neutrality of one:** We have $a1_{\mathbb{K}} = 1_{\mathbb{K}}a = a$ for all $a \in \mathbb{K}$.
- **Annihilation:** We have $a0_{\mathbb{K}} = 0_{\mathbb{K}}a = 0_{\mathbb{K}}$ for all $a \in \mathbb{K}$.
- **Distributivity:** We have

  $$a(b +_{\mathbb{K}} c) = ab +_{\mathbb{K}} ac \qquad \text{and} \qquad (a +_{\mathbb{K}} b)c = ac +_{\mathbb{K}} bc$$

  for all $a, b, c \in \mathbb{K}$. Here and in the following, we are using the PEMDAS convention for order of operations; thus, for example, "$ab +_{\mathbb{K}} ac$" must be understood as "$(ab) +_{\mathbb{K}} (ac)$".

These eight axioms will be called the *ring axioms*.

(Note that we do not require the existence of a "subtraction" operation $-_{\mathbb{K}}$. But we will later construct such an operation out of the existing operations and axioms; it is thus unnecessary to require it. We also do not require the existence of multiplicative inverses; nor do we require commutativity of multiplication yet.)

(b) A ring $\mathbb{K}$ (with operations $+_{\mathbb{K}}$ and $\cdot_{\mathbb{K}}$) is called *commutative* if it satisfies the following extra axiom:

- **Commutativity of multiplication:** We have $ab = ba$ for all $a, b \in \mathbb{K}$.

Note a few things:

- We shall abbreviate $+_{\mathbb{K}}$, $\cdot_{\mathbb{K}}$, $0_{\mathbb{K}}$ and $1_{\mathbb{K}}$ as $+$, $\cdot$, 0 and 1 unless there is a chance of confusion with the "usual" notions of addition, multiplication, zero

and one. (The example of the ring $\mathbb{Z}'$ shown below is a case where such confusion is possible; but most of the time, it is not.)

- We have not required our rings to be endowed with a "subtraction" operation. Nevertheless, each ring $\mathbb{K}$ automatically has a subtraction operation: Namely, for any $a, b \in \mathbb{K}$, we can define $a - b$ to be $a + b'$, where b' is the additive inverse of b. (We will later see that this operation is well-defined (Definition 5.4.4) and satisfies the rules you would expect (Definition 5.4.5).)

- Some of the ring axioms we required in Definition 5.1.1 are redundant, i.e., they follow from other ring axioms. (For example, Annihilation follows from the other axioms.) We don't mind this, as long as these axioms are natural and easy to check in real examples.

- We have required commutativity of addition to hold for all rings, but commutativity of multiplication only to hold for commutative rings. You may wonder what happens if we also omit the commutativity of addition. The answer is "nothing new": Commutativity of addition follows from the other axioms! (Proving this is a fun, although inconsequential, puzzle.)

- By our definition, a ring consists of a set $\mathbb{K}$, two operations $+$ and $\cdot$ and two elements 0 and 1. Thus, strictly speaking, a ring is a 5-tuple $(\mathbb{K}, +, \cdot, 0, 1)$. In reality, we will often just speak of the "ring $\mathbb{K}$" (so we will mention only the set and not the other four pieces of data) and assume that the reader can figure out the rest of the 5-tuple. This is okay as long as the rest of the 5-tuple can be inferred from the context. For example, when we say "the ring $\mathbb{Z}$", it is clear that we mean the ring $(\mathbb{Z}, +, \cdot, 0, 1)$ with the usual addition and multiplication operations and the usual numbers 0 and 1. The same applies when we speak of "the ring $\mathbb{R}$" or "the ring $\mathbb{C}$" or "the ring $\mathbb{Z}[i]$". In general, whenever a set S is equipped with two operations that are called $+$ and $\cdot$ and two elements that are called 0 and 1 (even if these elements are not literally the numbers 0 and 1), we automatically understand "the ring S" to be the ring $(S, +, \cdot, 0, 1)$ that is defined using these operations and elements. If we want to make a different ring out of the set S, then we have to say this explicitly.

- Some authors do not require the element 1 as part of what it means to be a ring. But we do. Be careful when reading the literature, as the truth or falsehood of many results depends on whether the 1 is included in the definition of a ring or not. (When authors do not require the element 1 in the definition of a ring, they reserve the notion of a "unital ring" for a ring that does come equipped with a 1 that satisfies the "Neutrality of one" axiom; i.e., they call "unital ring" what we call "ring".)

  The variant of the notion of rings in which the element 1 is not required is most commonly called a *nonunital ring*; it appears in Exercises 1 and 2 of midterm #3.

5.2. Examples of rings

Many of the "number systems" seen above, and several others, are examples of rings:

- The sets $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$ (each endowed with the usual addition, multiplication, 0 and 1) are commutative rings. In each case, the additive inverse of an element a is what we know as $-a$ from high school. (Rigorous proofs of the ring axioms, as well as rigorous definitions of $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$, can be found in textbooks and lecture notes on the construction of the number system – such as [Swanso18, Chapter 3].)

- The set $\mathbb{N}$ (again endowed with the usual addition, multiplication, 0 and 1) is not a ring. Indeed, the "existence of additive inverses" axiom fails for $a = 1$, because the element 1 has no additive inverse in $\mathbb{N}$ (that is, there is no $1' \in \mathbb{N}$ such that $1 + 1' = 1' + 1 = 0$).

- The sets $\mathbb{C}$, $\mathbb{Z}[i]$, $\mathbb{D}$, $\mathbb{Z}\left[\sqrt{2}\right]$, $\mathbb{Z}[\omega]$ and $\mathbb{Z}\left[\sqrt{-3}\right]$ (from Chapter 4 and from the homework sets) are commutative rings. All of the axioms are easy to check, and some of them we have checked. (For example, the ring axioms for $\mathbb{C}$ follow easily from Theorem 4.1.2.) In each case, the element a' in the "existence of additive inverses" axiom is $-a$.

- If you have seen polynomials: The set $\mathbb{Z}[x]$ of all polynomials in a single variable x with integer coefficients is a commutative ring. Similarly for other kinds of coefficients, and several variables. We will come back to this once we have rigorously defined polynomials in Chapter 7.

- We can define a commutative ring $\mathbb{Z}'$ as follows:

  We define a binary operation $\widetilde{\times}$ on $\mathbb{Z}$ by

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

  Now, let $\mathbb{Z}'$ be the **set** $\mathbb{Z}$, endowed with the usual addition $+$ and the unusual multiplication $\widetilde{\times}$ and the elements $0_{\mathbb{Z}'} = 0$ and $1_{\mathbb{Z}'} = -1$.

  Is this $\mathbb{Z}'$ a commutative ring? Let us check the axioms:

  - The first four axioms involve only addition and 0 (but not multiplication and 1), and therefore still hold for $\mathbb{Z}'$ (because $\mathbb{Z}'$ has the same addition and 0 as $\mathbb{Z}$).
  - Associativity of multiplication in $\mathbb{Z}'$: We must check that

    $$a \widetilde{\times} \left(b \widetilde{\times} c\right) = \left(a \widetilde{\times} b\right) \widetilde{\times} c \qquad \text{for all } a, b, c \in \mathbb{Z}'.$$

    (Note that we cannot omit the "multiplication sign" $\widetilde{\times}$ here and simply write "bc" for "$b \widetilde{\times} c$", because "bc" already means something different.

Note also that "$a, b, c \in \mathbb{Z}'$" means the same as "$a, b, c \in \mathbb{Z}$", because $\mathbb{Z}' = \mathbb{Z}$ as sets.)

Checking this is straightforward: Let $a, b, c \in \mathbb{Z}'$. Then, comparing

$$a \mathbin{\widetilde{\times}} \underbrace{\left(b \mathbin{\widetilde{\times}} c\right)}_{=-bc} = a \mathbin{\widetilde{\times}} (-bc) = -a(-bc) = abc \qquad \text{with}$$
$$\underbrace{\left(a \mathbin{\widetilde{\times}} b\right)}_{=-ab} \mathbin{\widetilde{\times}} c = (-ab) \mathbin{\widetilde{\times}} c = -(-ab)\, c = abc,$$

we obtain $a \mathbin{\widetilde{\times}} \left(b \mathbin{\widetilde{\times}} c\right) = \left(a \mathbin{\widetilde{\times}} b\right) \mathbin{\widetilde{\times}} c$. Thus, associativity of multiplication holds for $\mathbb{Z}'$.

– Neutrality of one in $\mathbb{Z}'$: We must check that

$$a \mathbin{\widetilde{\times}} 1_{\mathbb{Z}'} = 1_{\mathbb{Z}'} \mathbin{\widetilde{\times}} a = a \qquad \text{for all } a \in \mathbb{Z}'.$$

This, too, is straightforward: If $a \in \mathbb{Z}'$, then $a \mathbin{\widetilde{\times}} \underbrace{1_{\mathbb{Z}'}}_{=-1} = a \mathbin{\widetilde{\times}} (-1) = -a(-1) = a$ and similarly $1_{\mathbb{Z}'} \mathbin{\widetilde{\times}} a = a$.

– Annihilation and commutativity of multiplication are just as easy to check.

– Distributivity for $\mathbb{Z}'$: We must check that

$$a \mathbin{\widetilde{\times}} (b + c) = a \mathbin{\widetilde{\times}} b + a \mathbin{\widetilde{\times}} c \qquad \text{and} \qquad (a + b) \mathbin{\widetilde{\times}} c = a \mathbin{\widetilde{\times}} c + b \mathbin{\widetilde{\times}} c$$

for all $a, b, c \in \mathbb{Z}'$.

So let $a, b, c \in \mathbb{Z}'$. In order to verify $a \mathbin{\widetilde{\times}} (b + c) = a \mathbin{\widetilde{\times}} b + a \mathbin{\widetilde{\times}} c$, we compare

$$a \mathbin{\widetilde{\times}} (b + c) = -a(b + c) = -ab - ac$$

with

$$a \mathbin{\widetilde{\times}} b + a \mathbin{\widetilde{\times}} c = (-ab) + (-ac) = -ab - ac.$$

Similarly we can check $(a + b) \mathbin{\widetilde{\times}} c = a \mathbin{\widetilde{\times}} c + b \mathbin{\widetilde{\times}} c$.

So $\mathbb{Z}'$ is a ring.

(Note that $\left(\mathbb{Z}, +, \widetilde{\times}, 0, 1\right)$ is not a ring.)

However, $\mathbb{Z}'$ is not a **new** ring. It is just $\mathbb{Z}$ with its elements renamed. Namely, if we rename each integer a as $-a$, then the operations of $+$ and $\cdot$ and the elements 0 and 1 of $\mathbb{Z}$ turn into the operations $+$ and $\widetilde{\times}$ and the elements 0 and $1_{\mathbb{Z}'}$ of $\mathbb{Z}'$. This is a confusing thing to say (please don't actually rename numbers as other numbers!); the rigorous (and hopefully not confusing) way to say this is as follows: The bijection

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

satisfies

$$\varphi(a+b) = \varphi(a) + \varphi(b) \qquad \text{for all } a,b \in \mathbb{Z}; \tag{46}$$

$$\varphi(ab) = \varphi(a) \mathbin{\widetilde{\times}} \varphi(b) \qquad \text{for all } a,b \in \mathbb{Z}; \tag{47}$$

$$\varphi(0) = 0 = 0_{\mathbb{Z}'}; \tag{48}$$

$$\varphi(1) = -1 = 1_{\mathbb{Z}'}. \tag{49}$$

Thus, we can view φ as a way of relabelling the integers so that the data $+, \cdot, 0, 1$ of the ring $\mathbb{Z}$ become the data $+, \widetilde{\times}, 0_{\mathbb{Z}'}, 1_{\mathbb{Z}'}$ of the ring $\mathbb{Z}'$. We will later call bijections like φ "ring isomorphisms". (See Definition 5.10.1 for the definition of a ring homomorphism.)

- Recall: If A and B are two sets, then

$$B^A := \{\text{maps } A \to B\}.$$

(This notation is not wantonly chosen to annoy you with its seeming backwardness; instead, it harkens back to the fact that $\left|B^A\right| = |B|^{|A|}$.)

The set $\mathbb{Q}^{\mathbb{Q}}$ of all the maps from $\mathbb{Q}$ to $\mathbb{Q}$ is a commutative ring, where

  - addition and multiplication are defined pointwise: i.e., if $f, g \in \mathbb{Q}^{\mathbb{Q}}$ are two maps, then the maps $f+g$ and $f \cdot g$ are defined by

$$(f+g)(x) = f(x) + g(x) \qquad \text{and}$$
$$(f \cdot g)(x) = f(x) \cdot g(x) \qquad \text{for all } x \in \mathbb{Q};$$

  - 0 means the "constant 0" function (i.e., the map $\mathbb{Q} \to \mathbb{Q},\ x \mapsto 0$);
  - 1 means the "constant 1" function (i.e., the map $\mathbb{Q} \to \mathbb{Q},\ x \mapsto 1$).

All the ring axioms are easy to check. For example, each $f \in \mathbb{Q}^{\mathbb{Q}}$ has an additive inverse (namely, the map $-f \in \mathbb{Q}^{\mathbb{Q}}$ that sends each $x \in \mathbb{Q}$ to $-f(x)$). Similarly, the sets $\mathbb{Q}^{\mathbb{C}}$ or $\mathbb{Q}^{\mathbb{N}}$ or $\mathbb{R}^{\mathbb{R}}$ (the set of "functions" you know from calculus) or $\mathbb{C}^{\mathbb{C}}$ (or, more generally, for $\mathbb{K}^S$, where $\mathbb{K}$ is any commutative ring and S is any set) can be made into commutative rings; but the set $\mathbb{N}^{\mathbb{Q}}$ cannot. The problem with $\mathbb{N}^{\mathbb{Q}}$ is that "existence of additive inverses" is not satisfied, since $-a \notin \mathbb{N}$ for positive $a \in \mathbb{N}$.

- Recall that

$$\mathbb{Z}\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a,b \in \mathbb{Z}\right\} \text{ is a ring.}$$

But the set $\left\{a + b\sqrt[3]{2} \mid a,b \in \mathbb{Z}\right\}$ (with the usual addition and multiplication) is **not** a ring. The reason is that multiplication is not a binary operation on this set, since it is possible that two numbers α and β lie in this set but their product $\alpha\beta$ does not. For example, $1 + \sqrt[3]{2}$ lies in this set, but

$$\left(1 + \sqrt[3]{2}\right)\left(1 + \sqrt[3]{2}\right) = 1 + 2\sqrt[3]{2} + \sqrt[3]{4}$$

does not. (That said, this set does satisfy all the eight ring axioms.)

- The set of 2×2-matrices with rational entries (endowed with matrix addition as $+$, matrix multiplication as $\cdot$, the zero matrix $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ as 0, and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ as 1) is a ring, but **not** a commutative ring. Indeed, the ring axioms are true (this is known from linear algebra), but commutativity of multiplication is not (the product AB of two 2×2-matrices A and B is not always equal to BA). The same applies to $n \times n$-matrices for arbitrary $n \in \mathbb{N}$. (We will see this in Corollary 5.8.11 below, in greater generality.)

- If you like the empty set, you will enjoy the *zero ring*. This is the one-element set $\{0\}$, endowed with the only possible addition (given by $0 + 0 = 0$), the only possible multiplication (given by $0 \cdot 0 = 0$), the only possible zero (namely, 0) and the only possible unity (also 0). This is a commutative ring, and is known as the *zero ring*. Resist the temptation of denoting its unity by 1, as this will quickly lead to painful confusion.

  (Some authors choose to forbid this ring, usually for no good reasons.)

- If n is an integer, then $\mathbb{Z}/n$ is a ring (with the operations $+$ and $\cdot$ that we defined, with the zero $[0]_n$ and the unity $[1]_n$). When the integer n is positive, this ring $\mathbb{Z}/n$ has n elements. (When n is prime, it can be shown that $\mathbb{Z}/n$ is the only ring with exactly n elements, up to relabeling its elements. In general, however, there can be several rings with n elements.)

- In set theory, the *symmetric difference* $A \triangle B$ of two sets A and B is defined to be the set

$$\begin{aligned}(A \cup B) \setminus (A \cap B) &= (A \setminus B) \cup (B \setminus A) \\ &= \{x \mid x \text{ belongs to } \textbf{exactly one} \text{ of } A \text{ and } B\}.\end{aligned}$$

  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). Then, it is easy to check that the following properties hold:

$$\begin{aligned}
A \triangle B &= B \triangle A && \text{for any sets } A \text{ and } B; \\
A \cap B &= B \cap A && \text{for any sets } A \text{ and } B; \\
(A \triangle B) \triangle C &= A \triangle (B \triangle C) && \text{for any sets } A, B, C; \\
(A \cap B) \cap C &= A \cap (B \cap C) && \text{for any sets } A, B, C; \\
A \triangle \varnothing &= \varnothing \triangle A = A && \text{for any set } A; \\
A \cap S &= S \cap A = A && \text{for any subset } A \text{ of } S; \\
A \triangle A &= \varnothing && \text{for any set } A; \\
\varnothing \cap A &= A \cap \varnothing = \varnothing && \text{for any set } A; \\
A \cap (B \triangle C) &= (A \cap B) \triangle (A \cap C) && \text{for any sets } A, B, C; \\
(A \triangle B) \cap C &= (A \cap C) \triangle (B \cap C) && \text{for any sets } A, B, C.
\end{aligned}$$

Therefore, the set $\mathcal{P}(S)$, endowed with the addition $\triangle$, the multiplication $\cap$, the zero $\varnothing$ and the unity S is a commutative ring. Furthermore, the additive inverse of any $A \in \mathcal{P}(S)$ is A itself (since $A \triangle A = \varnothing$). Moreover, each $A \in \mathcal{P}(S)$ satisfies $A \cap A = A$, which means (in the language of ring operations) that its square is itself. Thus, $\mathcal{P}(S)$ is what is called a *Boolean ring*. (See Exercise 2 on midterm #2 for the precise definition and a few properties of Boolean rings.)

Let us now see some non-examples – i.e., examples of things that are not rings:

- You probably remember the *cross product* from analytic geometry. In a nutshell: The set $\mathbb{R}^3$ of vectors in 3-dimensional space has a binary operation $\times$ defined on it, which is given by

$$(a_1, a_2, a_3) \times (b_1, b_2, b_3) = (a_2 b_3 - a_3 b_2, a_3 b_1 - a_1 b_3, a_1 b_2 - a_2 b_1).$$

  Is the set $\mathbb{R}^3$, equipped with the addition $+$ and the multiplication $\times$ (and some elements playing the roles of zero and unity) a ring?

  The answer is "no", no matter which elements you want to play the roles of zero and unity. Indeed, the "Associativity of multiplication" axiom does not hold, because three vectors $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{R}^3$ usually do **not** satisfy $\mathbf{a} \times (\mathbf{b} \times \mathbf{c}) = (\mathbf{a} \times \mathbf{b}) \times \mathbf{c}$.

  Nevertheless, not all is lost; for example, the "Distributivity" axiom holds. The structure formed by the set $\mathbb{R}^3$, its addition $+$ and its cross product $\times$ is an instance of a different concept – namely, of a Lie algebra.

- So the cross product does not work; what about the dot product? The dot product of two vectors (a_1, a_2, a_3) and (b_1, b_2, b_3) in $\mathbb{R}^3$ is a real number given by

$$(a_1, a_2, a_3) \cdot (b_1, b_2, b_3) = a_1 b_1 + a_2 b_2 + a_3 b_3.$$

  Can this be used to make $\mathbb{R}^3$ into a ring?

  No, because the dot product is not even a binary operation on $\mathbb{R}^3$. Indeed, our definition of a binary operation requires that its output belongs to the same domain as its two inputs; this is clearly not true of the dot product (since its output is a real number, while its two inputs are vectors).

- The set $\left\{ a + b\sqrt[3]{2} \mid a, b \in \mathbb{Z} \right\}$ is not a ring (despite the superficial similarity to $\left\{ a + b\sqrt{2} \mid a, b \in \mathbb{Z} \right\}$, which is a ring), at least not if we try to use the usual multiplication of real numbers as its multiplication. In fact, this multiplication is not a binary operation on this set, because the product of $\sqrt[3]{2}$ and $\sqrt[3]{2}$ is not an element of this set.

  However, the larger set $\left\{ a + b\sqrt[3]{2} + c\left(\sqrt[3]{2}\right)^2 \mid a, b \in \mathbb{Z} \right\}$ is a ring (endowed with the usual addition, the usual multiplication, the usual 0 and the usual 1). (Check this!)

- For each $a, b \in \mathbb{R}$, we let $A_{a,b}$ be the function

$$\mathbb{R} \to \mathbb{R}, \qquad x \mapsto ax + b.$$

This sort of function is called "linear function" in high school; research mathematicians prefer to call it "affine-linear function" instead (while reserving the word "linear" for a more restrictive class of functions). Let ALF be the set of these affine-linear functions $A_{a,b}$ for all $a, b \in \mathbb{R}$.

We can define a pointwise addition $+$ on ALF; that is, for any $f, g \in A_{a,b}$, we define a function $f + g \in A_{a,b}$ by

$$(f+g)(x) = f(x) + g(x) \qquad \text{for all } x \in \mathbb{R}.$$

We can also try to define a multiplication $\cdot$ on ALF. One obvious choice would be to define multiplication to be composition (that is, $f \cdot g = f \circ g$); another would be pointwise multiplication (that is, $(f \cdot g)(x) = f(x) \cdot g(x)$ for all $x \in \mathbb{R}$). Does any of these lead to a ring?

No. If we define multiplication to be composition, then the "Distributivity" axiom is violated, since affine-linear functions f, g, h do not always satisfy $f \circ (g + h) = f \circ g + f \circ h$. If we define multiplication to be pointwise multiplication, then it is not a binary operation on ALF, since the pointwise product of two affine-linear functions is not an affine-linear function in general.

- You know from high school that you cannot divide by 0. Why not?

Let us make the question precise. Of course, we cannot find an integer a that satisfies $0 \cdot a = 1$, or a real, or a complex number, etc. But could we perhaps find such a number a in some larger "number system"?

The answer, of course, depends on what "number system" means for you. If it means a ring, then we cannot find such an a in any ring.

Indeed, assume that we can. In other words, assume that there is a ring $\mathbb{K}$ that contains the usual set $\mathbb{Z}$ of integers as well as a new element ∞ such that $0 \cdot \infty = 1$. And assume (this is a very reasonable assumption) that the numbers 0 and 1 are indeed the zero and the unity of this ring. Then, the Annihilation axiom yields $0 \cdot \infty = 0$, so that $0 = 0 \cdot \infty = 1$, which is absurd. So such a ring $\mathbb{K}$ cannot exist. Thus, we cannot divide by 0, even if we extend our "number system".

- Here is an "almost-ring" beloved to combinatorialists: the *max-plus semiring* $\mathbb{T}$ (also known as the *tropical semiring*[64]).

We introduce a new symbol $-\infty$, and we set $\mathbb{T} = \mathbb{Z} \cup \{-\infty\}$ as sets. But we do **not** "inherit" the addition and multiplication from $\mathbb{Z}$. Instead, let us

[64] To be pedantic: The name "tropical semiring" refers to several different objects, of which $\mathbb{T}$ is but one.

define two new "addition" and "multiplication" operations $+_{\mathbb{T}}$ and $\cdot_{\mathbb{T}}$ (not to be mistaken for the original addition $+$ and multiplication $\cdot$ of integers) as follows:

$$\begin{aligned} a +_{\mathbb{T}} b &= \max\{a, b\}; \\ a \cdot_{\mathbb{T}} b &= a + b \qquad \text{(usual addition of integers)}, \end{aligned}$$

where we set

$$\begin{aligned} \max\{-\infty, n\} = \max\{n, -\infty\} &= n \qquad \text{and} \\ (-\infty) + n = n + (-\infty) &= -\infty \qquad \text{for any } n \in \mathbb{Z} \cup \{-\infty\}. \end{aligned}$$

This set $\mathbb{T}$ endowed with the "addition" $+_{\mathbb{T}}$, "multiplication" $\cdot_{\mathbb{T}}$, "zero" $-\infty$ and "unity" 0 satisfies all but one of the ring axioms.[65] The only one that it does not satisfy is the existence of additive inverses. Such a structure is called a *semiring*.

- Consider the set

$$2\mathbb{Z} := \{2a \mid a \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = \{\text{all even integers}\}.$$

Endowing this set with the usual addition and multiplication (and 0), we obtain a structure that is like a ring but has no unity. This is called a *nonunital ring*. There is no way to find a unity for it, because (for example) 2 is not a product of any two elements of $2\mathbb{Z}$.

5.3. Subrings

Looking back at the examples of rings listed above, you might notice that a lot of them are "nested" inside one another: For example, the rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ form a chain $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ in which each ring not only is a subset of the subsequent one[66], but also has "the same" addition, multiplication, zero and unity as the subsequent one. Of course, when we are saying "the same" here, we do

[65] For example, the distributivity axiom for $\mathbb{T}$ boils down to the two identities

$$\begin{aligned} a + \max\{b, c\} &= \max\{a + b, a + c\} \qquad \text{and} \\ \max\{a, b\} + c &= \max\{a + c, b + c\}. \end{aligned}$$

[66] To be fully honest, we are relying on Convention 4.1.7 in order to make $\mathbb{R}$ a subset of $\mathbb{C}$. And if you look closely at the definitions of $\mathbb{Q}$ and $\mathbb{R}$, the relations $\mathbb{Z} \subseteq \mathbb{Q}$ and $\mathbb{Q} \subseteq \mathbb{R}$ are also not immediately satisfied but rather rely on similar conventions. For example, rational numbers are defined as equivalence classes of pairs of integers; an integer is not an equivalence class of such pairs. Thus, we need a convention which identifies each integer z with an appropriate rational number in order to turn $\mathbb{Z}$ into a subset of $\mathbb{Q}$. Similarly for turning $\mathbb{Q}$ into a subset of $\mathbb{R}$. But let us not worry about this issue for now.

not literally mean "the same binary operation"[67]; we mean that, e.g., if we add two integers in $\mathbb{Z}$, we get the same result as if we add the same two integers as elements of $\mathbb{Q}$, or as elements of $\mathbb{R}$, or as elements of $\mathbb{C}$. In other words, the addition operation of the ring $\mathbb{Z}$ is a **restriction** of the addition operation of the ring $\mathbb{Q}$, which in turn is a restriction of the addition operation of the ring $\mathbb{R}$, etc.. The same holds for multiplication. The zeroes of the rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are literally identical, as are the unities of these rings.

It is worth introducing a name for this situation:

Definition 5.3.1. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. We say that $\mathbb{K}$ is a *subring* of $\mathbb{L}$ if and only if it satisfies the following five requirements:

- the set $\mathbb{K}$ is a subset of $\mathbb{L}$;
- the addition of $\mathbb{K}$ is a restriction of the addition of $\mathbb{L}$ (that is, we have $a_1 +_{\mathbb{K}} a_2 = a_1 +_{\mathbb{L}} a_2$ for all $a_1, a_2 \in \mathbb{K}$);
- the multiplication of $\mathbb{K}$ is a restriction of the multiplication of $\mathbb{L}$ (that is, we have $a_1 \cdot_{\mathbb{K}} a_2 = a_1 \cdot_{\mathbb{L}} a_2$ for all $a_1, a_2 \in \mathbb{K}$);
- the zero of $\mathbb{K}$ is the zero of $\mathbb{L}$ (that is, we have $0_{\mathbb{K}} = 0_{\mathbb{L}}$);
- the unity of $\mathbb{K}$ is the unity of $\mathbb{L}$ (that is, we have $1_{\mathbb{K}} = 1_{\mathbb{L}}$).

Thus, according to this definition:

- the ring $\mathbb{Z}$ is a subring of $\mathbb{Q}$;
- the ring $\mathbb{Q}$ is a subring of $\mathbb{R}$;
- the ring $\mathbb{R}$ is a subring of $\mathbb{C}$;
- the ring $\mathbb{Z}[i]$ (of Gaussian integers) is a subring of $\mathbb{C}$;
- every ring $\mathbb{K}$ is a subring of itself.

What is an example of two rings $\mathbb{K}$ and $\mathbb{L}$ for which the set $\mathbb{K}$ is a **subset** of $\mathbb{L}$ yet the ring $\mathbb{K}$ is **not a subring** of $\mathbb{L}$? Here is one example of an "almost-subring":

Example 5.3.2. One of our above examples of rings (in Section 5.2) is the power set of any set S. Namely, if S is any set, then we have observed that its power set $\mathcal{P}(S)$, endowed with the addition $\triangle$, the multiplication $\cap$, the zero $\varnothing$ and the unity S is a commutative ring. We shall refer to this ring by $\mathcal{P}(S)$ (omitting mention of its addition, multiplication, zero and unity).

[67] The addition of $\mathbb{R}$ is a map from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$, while the addition of $\mathbb{C}$ is a map from $\mathbb{C} \times \mathbb{C}$ to $\mathbb{C}$. Thus, of course, these two additions are not literally the same binary operation.

Now, let T be a subset of a set S. Is $\mathcal{P}(T)$ a subring of the ring $\mathcal{P}(S)$? The first four requirements of Definition 5.3.1 are satisfied: The set $\mathcal{P}(T)$ is a subset of $\mathcal{P}(S)$; its addition is a restriction of the addition of $\mathcal{P}(S)$ (indeed, both of these additions turn two sets A and B into $A \triangle B$); its multiplication is a restriction of the multiplication of $\mathcal{P}(S)$; its zero is the zero of $\mathcal{P}(S)$. But its unity is not the unity of $\mathcal{P}(S)$ (unless $T = S$); indeed, the former unity is T, while the latter unity is S. Thus, $\mathcal{P}(T)$ is not a subring of $\mathcal{P}(S)$ (unless $T = S$). It fails the fifth requirement of Definition 5.3.1.

(As we have remarked, some authors do not require rings to have a unity. Correspondingly, these authors do not pose the fifth requirement in Definition 5.3.1. Thus, for these authors, $\mathcal{P}(T)$ is a subring of $\mathcal{P}(S)$.)

For a less subtle example, recall the ring $\mathbb{Z}'$ constructed in Section 5.2. The sets $\mathbb{Z}'$ and $\mathbb{Z}$ are identical, but the rings $\mathbb{Z}'$ and $\mathbb{Z}$ are not, so the ring $\mathbb{Z}'$ is not a subring of $\mathbb{Z}$ despite being a subset of $\mathbb{Z}$.

When we have two rings $\mathbb{K}$ and $\mathbb{L}$ such that $\mathbb{K} \subseteq \mathbb{L}$ as sets (or, more generally, such that $\mathbb{K}$ and $\mathbb{L}$ have elements in common), we generally need to be careful using the symbol "$+$": This symbol may mean both the addition of $\mathbb{K}$ and the addition of $\mathbb{L}$, and these additions might not be the same. Thus it is prudent to disambiguate its meaning by attaching a subscript "$_{\mathbb{K}}$" or "$_{\mathbb{L}}$" to it. The same applies to the symbols "$\cdot$", "0" and "1" and expressions like "ab" (which have an implicit multiplication sign). However, when $\mathbb{K}$ is a subring of $\mathbb{L}$, we do not need to take this precaution; in this case, the meaning of expressions like "$a + b$" does not depend on whether you read "$+$" as the addition of $\mathbb{K}$ or as the addition of $\mathbb{L}$.

The following facts are essentially obvious:

Proposition 5.3.3. A subring of a commutative ring is always commutative.

Proposition 5.3.4. Let $\mathbb{L}$ be a ring. Let S be a subset of $\mathbb{L}$ that satisfies the following four conditions:[68]

- We have $0 \in S$ and $1 \in S$.
- The subset S is *closed under addition*. (This means that all $a, b \in S$ satisfy $a + b \in S$.)
- The subset S is *closed under additive inverses*. (This means that all $a \in S$ satisfy $-a \in S$.)
- The subset S is *closed under multiplication*. (This means that all $a, b \in S$ satisfy $ab \in S$.)

Then, the set S itself becomes a ring if we endow it with the following two operations:

- an addition operation $+$ which is defined as the restriction of the addition operation of the ring $\mathbb{L}$;
- a multiplication operation $\cdot$ which is defined as the restriction of the multiplication operation of the ring $\mathbb{L}$,

and the zero 0 and the unity 1. Furthermore, this ring S is a subring of $\mathbb{L}$.

Definition 5.3.5. Let $\mathbb{L}$ be a ring. Let S be a subset of $\mathbb{L}$ that satisfies the four conditions of Proposition 5.3.4. Then, we shall say that "S is a subring of $\mathbb{L}$". Technically speaking, this is premature, since S is so far just a subset of $\mathbb{L}$ without the structure of a ring; however, Proposition 5.3.4 shows that there is an obvious way of turning S into a ring (viz.: define two operations $+$ and $\cdot$ by restricting the corresponding operations of $\mathbb{L}$, and steal the zero and the unity from $\mathbb{L}$), and we shall automatically regard S as becoming a ring in this way (unless we say otherwise). We say that the operations $+$ and $\cdot$ on S (obtained by restricting the corresponding operations on $\mathbb{L}$) and the zero and the unity of S (which are exactly those of $\mathbb{L}$) are *inherited from* $\mathbb{L}$.

Thus, finding subrings of a ring $\mathbb{L}$ boils down to finding subsets that contain its 0 and 1 and are closed under addition, under additive inverses and under multiplication; the ring axioms don't need to be re-checked. This offers an easy way to discover subrings:

Example 5.3.6. Let us define a few subsets of the ring $\mathbb{Z}[i]$ and see whether they are subrings.

(a) Let

$$S_1 = \{a+bi \mid a,b \in \mathbb{Z}, \text{ and } b \text{ is even}\} = \{a+2ci \mid a,c \in \mathbb{Z}\}.$$

Is S_1 a subring of $\mathbb{Z}[i]$?

It is easy to check that $0 \in S_1$ and $1 \in S_1$. Let us now check that S_1 is closed under multiplication: Let $\alpha, \beta \in S_1$; we need to show that $\alpha\beta \in S_1$. We have $\alpha \in S_1 = \{a+2ci \mid a,c \in \mathbb{Z}\}$; in other words, we can write α in the form $\alpha = x+2yi$ for some $x,y \in \mathbb{Z}$. Similarly, we can write β in the form $\beta = z+2wi$ for some $z,w \in \mathbb{Z}$. Now, multiplying the two equalities $\alpha = x+2yi$ and $\beta = z+2wi$, we obtain

$$\begin{aligned}\alpha\beta &= (x+2yi)(z+2wi) = xz+2xwi+2yzi+4yw\underbrace{i^2}_{=-1} \\ &= (xz-4yw)+2(xw+yz)i.\end{aligned}$$

[68] In this proposition, the symbols "$+$", "$\cdot$", "0" and "1" mean the addition, the multiplication, the zero and the unity of $\mathbb{L}$.

Thus, $\alpha\beta$ can be written in the form $a+2ci$ for some $a, c \in \mathbb{Z}$ (namely, for $a = xz - 4yw$ and $c = xw + yz$). Thus, $\alpha\beta \in S_1$. Now, forget that we fixed α, β. We thus have shown that all $\alpha, \beta \in S_1$ satisfy $\alpha\beta \in S_1$. In other words, S_1 is closed under multiplication. Similar arguments show that S_1 is closed under addition and under additive inverses. Thus, S_1 is a subring of $\mathbb{Z}[i]$.

This subring S_1 is only "half as large" as $\mathbb{Z}[i]$ (in a vague sense that can be made precise), but it has rather different properties. For example, $\mathbb{Z}[i]$ has greatest common divisors and unique factorization into primes; the subring S_1 does not.

There is nothing special about the number 2; we could have just as easily shown that $\{a+kci \mid a, c \in \mathbb{Z}\}$ is a subring of $\mathbb{Z}[i]$ for each $k \in \mathbb{Z}$.

(b) Let

$$S_2 = \{a+bi \mid a, b \in \mathbb{Z}, \text{ and } a \text{ is even}\} = \{2c+bi \mid c, b \in \mathbb{Z}\}.$$

Is S_2 a subring of $\mathbb{Z}[i]$? No, since $1 \notin S_2$.

(c) Let

$$S_3 = \{a+bi \mid a, b \in \mathbb{Z}, \text{ and } b \text{ is a multiple of } a\} = \{a+aci \mid a, c \in \mathbb{Z}\}.$$

Is S_3 a subring of $\mathbb{Z}[i]$? The subset S_3 does contain both 0 and 1 and is closed under additive inverses; but S_3 is not closed under addition (nor under multiplication). Thus, S_3 is not a subring of $\mathbb{Z}[i]$. (For a concrete example: The numbers $1+2i$ and $1+3i$ both belong to S_3, but their sum $2+5i$ does not.)

(d) Let

$$S_4 = \{a+bi \mid a, b \in \mathbb{N}\}.$$

Is S_4 a subring of $\mathbb{Z}[i]$? No, because S_4 is not closed under additive inverses (although S_4 satisfies two of the other conditions of Proposition 5.3.4).

(e) A pattern emerges: It appears that the only subrings of $\mathbb{Z}[i]$ are the ones of the form $\{a+kci \mid a, c \in \mathbb{Z}\}$ for $k \in \mathbb{Z}$. This is indeed true. (It is not hard to prove, if you are so inclined! **Hint:** Let S be any subring of $\mathbb{Z}[i]$. Clearly, S contains 1 and therefore all the integer multiples of 1; in other words, $\mathbb{Z} \subseteq S$. Hence, if $S \subseteq \mathbb{Z}$, then clearly $S = \mathbb{Z}$, which means that $S = \{a+kci \mid a, c \in \mathbb{Z}\}$ for $k = 0$. Thus, we can WLOG assume that $S \not\subseteq \mathbb{Z}$. Hence, there exists at least one $a+bi \in S$ with $b \neq 0$. Thus, there exists at least one $a+bi \in S$ with $b > 0$ (indeed, if $b < 0$, then we replace this element by its additive inverse). Pick the one with the **smallest** b. Then, from $a+bi \in S$ and $a \in \mathbb{Z} \subseteq S$, we obtain $(a+bi) - a \in S$ (since S is a ring), which means that $bi \in S$. Next, argue that $S = \{a+kci \mid a, c \in \mathbb{Z}\}$ for $k = b$.)

5.4. Additive inverses, sums, powers and their properties

What can you do when you have a ring?

Convention 5.4.1. For the rest of this section, we fix a ring $\mathbb{K}$, and we denote its addition, multiplication, zero and unity by $+$, $\cdot$, 0 and 1.

One thing you can do is subtraction. This relies on the following fact:

Theorem 5.4.2. Let $a \in \mathbb{K}$. Then, a has exactly one additive inverse.

Before we prove this, let us recall how additive inverses are defined:

Definition 5.4.3. Let $a \in \mathbb{K}$. An *additive inverse* of a means an element a' of $\mathbb{K}$ such that $a + a' = a' + a = 0$.

Definition 5.4.4. **(a)** If $a \in \mathbb{K}$, then the additive inverse of a will be called $-a$. (This is well-defined, since Theorem 5.4.2 shows that this additive inverse is unique.)

(b) If $a \in \mathbb{K}$ and $b \in \mathbb{K}$, then we define the *difference* $a - b$ to be the element $a + (-b)$ of $\mathbb{K}$. This new binary operation $-$ on $\mathbb{K}$ is called "*subtraction*".

Additive inverses and subtraction satisfy certain rules that should not surprise you:

Proposition 5.4.5. Let $a, b, c \in \mathbb{K}$.

(a) We have $a - b = c$ if and only if $a = b + c$. (Roughly speaking, this means that subtraction undoes addition.)

(b) We have $-(a + b) = (-a) + (-b)$.

(c) We have $-0 = 0$.

(d) We have $0 - a = -a$.

(e) We have $-(-a) = a$.

(f) We have $-(ab) = (-a)\, b = a\,(-b)$.

(g) We have $a - b - c = a - (b + c)$. (Here and in the following, "$a - b - c$" should be read as "$(a - b) - c$".)

(h) We have $a\,(b - c) = ab - ac$ and $(a - b)\, c = ac - bc$.

(i) We have $-(a - b) = b - a$.

(j) We have $a - (-b) = a + b$.

(k) We have $(-1)\, a = -a$. (Here, the "1" on the left hand side means the unity of $\mathbb{K}$.)

(l) If $-a = -b$, then $a = b$.

If $a, b \in \mathbb{K}$, then the expression "$-ab$" can be considered ambiguous, since it can be read either as "$(-a)\, b$" or as "$-(ab)$". But Proposition 5.4.5 **(f)** shows that these two readings yield the same result; therefore, you need not fear this ambiguity.

Furthermore, we don't need to parenthesize expressions like $a + b + c$ or abc. Indeed:

Theorem 5.4.6. Finite sums of elements of $\mathbb{K}$ can be defined in the same way as finite sums of usual (i.e., real or rational) numbers (with the empty sum defined to be 0). That is, if S is a finite set, and if $a_s \in \mathbb{K}$ for each $s \in S$, then $\sum_{s \in S} a_s$ is well-defined and satisfies the usual rules, such as

$$\sum_{s \in S} (a_s + b_s) = \sum_{s \in S} a_s + \sum_{s \in S} b_s.$$

Thus, in particular, sums like $\sum_{i=p}^{q} a_i$ or $a_1 + a_2 + \cdots + a_k$ are well-defined. We don't need to put parentheses or specify the order of summation in order to make them non-ambiguous.

What about finite products? Is $\prod_{s \in S} a_s$ well-defined? Not always, but only for commutative rings. Indeed, a product like $\prod_{s \in S} a_s$ has no pre-defined order of multiplication (in general), so for it to be well-defined, it would have to be independent of the order; but this would require the commutativity of multiplication.

Theorem 5.4.7. (a) Finite products of elements of $\mathbb{K}$ can be defined in the same way as finite products of usual (i.e., real or rational) numbers (with the empty product defined to be 1) **as long as the ring $\mathbb{K}$ is commutative**.

(b) For general (not necessarily commutative) rings $\mathbb{K}$, we can still define products with a pre-determined order, such as $a_1 a_2 \cdots a_k$ (where $a_1, a_2, \ldots, a_k \in \mathbb{K}$). These products can be defined recursively as follows:

$$a_1 a_2 \cdots a_k = 1 \qquad \text{if } k = 0;$$

otherwise,

$$a_1 a_2 \cdots a_k = (a_1 a_2 \cdots a_{k-1})\, a_k.$$

These products still satisfy the rule

$$a_1 a_2 \cdots a_k = (a_1 a_2 \cdots a_i)\,(a_{i+1} a_{i+2} \cdots a_k) \qquad \text{for all } i \in \{0, 1, \ldots, k\}.$$

Theorem 5.4.7 **(b)** is called the *general associativity theorem for rings*. Note that Theorem 5.4.7 **(b)** entails that if we have k elements $a_1, a_2, \ldots, a_k$ of a ring $\mathbb{K}$, then any two ways of parenthesizing the product $a_1 a_2 \cdots a_k$ yield the same result. For example, for $k = 4$, we have

$$((a_1 a_2)\, a_3)\, a_4 = (a_1\,(a_2 a_3))\, a_4 = (a_1 a_2)\,(a_3 a_4) = a_1\,((a_2 a_3)\, a_4) = a_1\,(a_2\,(a_3 a_4)).$$

(It is not hard to prove this particular chain of identities by applying the associativity of multiplication in the appropriate places; but for higher values of k, such a manual approach becomes more and more cumbersome.)

What else can we do with our ring $\mathbb{K}$?

By definition, we know how to multiply two elements of $\mathbb{K}$. But there is also a natural way to multiply an element of $\mathbb{K}$ with an integer. This is defined as follows:

Definition 5.4.8. Let $a \in \mathbb{K}$ and $n \in \mathbb{Z}$. Then, we define an element na of $\mathbb{K}$ by

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

The "na" that we have just defined has nothing to do with the multiplication $\cdot$ of $\mathbb{K}$, since n is not (generally) an element of $\mathbb{K}$. However, when $\mathbb{K}$ is one of the usual rings of numbers (like $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$), then this kind of multiplication is a restriction of the multiplication $\cdot$ of $\mathbb{K}$ (that is, na means the same thing). Indeed, Definition 5.4.8 clearly generalizes the definition of na for rational numbers a. Furthermore, when $\mathbb{K} = \mathbb{Z}/n$ for some integer n, Definition 5.4.8 agrees with Definition 3.4.18 (in the sense that both definitions yield the same result for $r\alpha$ when $r \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}/n$). (This is easy to prove by induction.)

The "na" multiplication introduced in Definition 5.4.8 has several properties that you would expect such an operation to have:

Proposition 5.4.9. We have

$$(n+m)\,a = na + ma \qquad \text{for all } a \in \mathbb{K} \text{ and } n, m \in \mathbb{Z}; \tag{50}$$

$$n\,(a+b) = na + nb \qquad \text{for all } a, b \in \mathbb{K} \text{ and } n \in \mathbb{Z}; \tag{51}$$

$$-\,(na) = (-n)\,a = n\,(-a) \qquad \text{for all } a \in \mathbb{K} \text{ and } n \in \mathbb{Z}; \tag{52}$$

$$(nm)\,a = n\,(ma) \qquad \text{for all } a \in \mathbb{K} \text{ and } n, m \in \mathbb{Z}; \tag{53}$$

$$n\,(ab) = (na)\,b = a\,(nb) \qquad \text{for all } a, b \in \mathbb{K} \text{ and } n \in \mathbb{Z}; \tag{54}$$

$$n0_{\mathbb{K}} = 0_{\mathbb{K}} \qquad \text{for all } n \in \mathbb{Z}; \tag{55}$$

$$1a = a \qquad \text{for all } a \in \mathbb{K} \tag{56}$$

(here, the "1" means the integer 1) ;

$$0a = 0_{\mathbb{K}} \qquad \text{for all } a \in \mathbb{K} \tag{57}$$

(here, the "0" on the left hand side means the integer 0) ;

$$(-1)\,a = -a \qquad \text{for all } a \in \mathbb{K}; \tag{58}$$

(here, the "-1" means the integer -1) .

In particular:

- The equality (52) shows that the expression "$-na$" (with $a \in \mathbb{K}$ and $n \in \mathbb{Z}$) is unambiguous (since its two possible interpretations, namely $-\,(na)$ and $(-n)\,a$, yield equal results).

- The equality (53) shows that the expression "nma" (with $a \in \mathbb{K}$ and $n, m \in \mathbb{Z}$) is unambiguous.
- The equality (54) shows that the expression "nab" (with $a, b \in \mathbb{K}$ and $n \in \mathbb{Z}$) is unambiguous.

Exercise 5.4.1. Prove Proposition 5.4.9.

[**Hint:** The proofs of the rules in Proposition 5.4.9 are analogous to the proofs of the corresponding rules for rationals – at least if you know the right proofs of the latter. One way is to start by proving the equalities (57), (56) and (58), which follow almost immediately from Definition 5.4.8; then, prove (50) for $n, m \in \mathbb{N}$; then, prove (55) and (51) for $n \in \mathbb{N}$; then, prove (53) for $n, m \in \mathbb{N}$; then, prove (54) for $n \in \mathbb{N}$; then, show that $(-n)\, a = -(na)$ for all $a \in \mathbb{K}$ and $n \in \mathbb{Z}$ (by distinguishing between the cases $n > 0$, $n = 0$ and $n < 0$); and then extend the identities that have already been shown for elements of $\mathbb{N}$ to elements of $\mathbb{Z}$ (using Proposition 5.4.5). Note that this is rather similar to the process by which we proved Proposition 4.1.20 in the solution to Exercise 4.1.1, with the main difference being that we now are studying multiples instead of powers (and addition instead of multiplication). Our solution to Exercise 4.1.1 cannot be copied literally, however, because the way we defined na for negative n in Definition 5.4.8 is somewhat different from the way we defined α^n for negative n in Definition 4.1.19.]

We can also define powers of elements of a ring:

Definition 5.4.10. Let $a \in \mathbb{K}$ and $n \in \mathbb{N}$. Then, we define an element a^n of $\mathbb{K}$ by

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

This definition clearly generalizes the definition of a^n for rational numbers a. Furthermore, when $\mathbb{K} = \mathbb{Z}/n$ for some integer n, Definition 5.4.10 agrees with Definition 3.4.20 (in the sense that both definitions yield the same result for α^k when $\alpha \in \mathbb{Z}/n$ and $k \in \mathbb{N}$). (This follows from Theorem 3.4.26 **(c)**.) Furthermore, when $\mathbb{K} = \mathbb{C}$, Definition 5.4.10 agrees with Definition 4.1.18.

Powers of elements of a ring satisfy some properties you would expect but fail to satisfy some others:

Proposition 5.4.11. (a) We have

$$a^0 = 1 \qquad \text{for all } a \in \mathbb{K}; \tag{59}$$

$$1^n = 1 \qquad \text{for all } n \in \mathbb{N} \tag{60}$$

(here, the "1" means the unity of $\mathbb{K}$);

$$0^n = \begin{cases} 0, & \text{if } n > 0 \\ 1, & \text{if } n = 0 \end{cases} \qquad \text{for all } n \in \mathbb{N} \tag{61}$$

(here, the "0" in "0^n" means the zero of $\mathbb{K}$);

$$a^{n+m} = a^n a^m \qquad \text{for all } a \in \mathbb{K} \text{ and } n, m \in \mathbb{N}; \tag{62}$$

$$(a^n)^m = a^{nm} \qquad \text{for all } a \in \mathbb{K} \text{ and } n, m \in \mathbb{N}. \tag{63}$$

(b) For any $a, b \in \mathbb{K}$, we have

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) = a(a+b) + b(a+b) \\ &= aa + ab + ba + bb = a^2 + ab + ba + b^2.\end{aligned}$$

This further equals $a^2 + 2ab + b^2$ if $\mathbb{K}$ is commutative.

(c) Let $a, b \in \mathbb{K}$ satisfy $ab = ba$. (This holds automatically when $\mathbb{K}$ is commutative.) Then:

$$ab^n = b^n a \qquad \text{for all } n \in \mathbb{N}; \tag{64}$$

$$a^i b^j = b^j a^i \qquad \text{for all } i, j \in \mathbb{N}; \tag{65}$$

$$(ab)^n = a^n b^n \qquad \text{for all } n \in \mathbb{N}; \tag{66}$$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \qquad \text{for all } n \in \mathbb{N}. \tag{67}$$

(d) Let $a, b \in \mathbb{K}$ satisfy $ab = ba$. Then,

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}\right) \qquad \text{for all } n \in \mathbb{N}.$$

5.5. Multiplicative inverses and fields

Convention 5.5.1. For the rest of this section, we fix a ring $\mathbb{K}$, and we denote its addition, multiplication, zero and unity by $+$, $\cdot$, 0 and 1.

Each element a of the ring $\mathbb{K}$ has an additive inverse $-a$, which satisfies $(-a) + a = a + (-a) = 0$. What about a "multiplicative inverse"?

Definition 5.5.2. Let $a \in \mathbb{K}$. A *multiplicative inverse* of a means an element a' of $\mathbb{K}$ such that $aa' = a'a = 1$.

Multiplicative inverses don't always exist. In the ring $\mathbb{Q}$, the number 0 has none. In the ring $\mathbb{Z}$, the number 2 has none (since $\frac{1}{2} \notin \mathbb{Z}$). But when they do exist, they are unique:

Theorem 5.5.3. Let $a \in \mathbb{K}$. Then, a has **at most one** multiplicative inverse.

Warning: In Definition 5.4.3, we could have replaced "$a + a' = a' + a = 0$" by "$a + a' = 0$", since $a + a' = a' + a$ already follows from commutativity of addition. But in Definition 5.5.2, we cannot replace "$aa' = a'a = 1$" by "$aa' = 1$", since $\mathbb{K}$ need not be commutative. If we require $aa' = 1$ only, then a' is just a *right inverse* of a; such a right inverse is not necessarily unique.

The following definition generalizes Definition 3.5.6, Definition 4.1.13 and Definition 4.1.14:

Definition 5.5.4. (a) An element $a \in \mathbb{K}$ is said to be *invertible* if it has a multiplicative inverse. An invertible element is also called a *unit*.

(b) If $a \in \mathbb{K}$ is invertible, then the multiplicative inverse of a will be called a^{-1}. (This is well-defined, since Theorem 5.5.3 shows that this multiplicative inverse is unique.)

(c) Assume that $\mathbb{K}$ is commutative. If $a \in \mathbb{K}$ and $b \in \mathbb{K}$ are such that b is invertible, then we define the *quotient* a/b (also called $\frac{a}{b}$) to be the element ab^{-1} of $\mathbb{K}$. This new binary partial operation $/$ on $\mathbb{K}$ is called "*division*".

The word "partial" in "partial operation" means that it is not always defined. We already have seen this for rational numbers: We cannot divide by 0.

Again, we follow PEMDAS rules as far as division is concerned. Do not use the ambiguous expression "a/bc"; it can mean either $a/(bc)$ or $(a/b)\,c$, depending on whom you ask, and thus should always be parenthesized.

The notion of "unit" we have just defined generalizes the units of $\mathbb{Z}[i]$. Don't confuse "unit" (= invertible element) with "unity" (= $1_{\mathbb{K}}$). The unity is always a unit (by Exercise 5.5.1 **(a)** further below), but often not the only unit.

Definition 5.5.4 **(c)** generalizes the usual meaning of a/b in $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$.

Please do not use Definition 5.5.4 **(c)** when $\mathbb{K}$ is not commutative; that would cause confusion, since ab^{-1} and $b^{-1}a$ would have equal rights to the name "$\frac{a}{b}$".

If $\mathbb{K} = \mathbb{Z}/n$ for a positive integer n, and if $\alpha \in \mathbb{K}$, then the multiplicative inverse of α is the same as an inverse of α (as defined in Definition 3.5.2). Thus, multiplicative inverses in arbitrary rings generalize the concept of inverses in $\mathbb{Z}/n$. Likewise, they generalize inverses in $\mathbb{C}$; that is, an inverse of a complex number $\alpha \in \mathbb{C}$ (as defined in Definition 4.1.11) is the same as a multiplicative inverse of α.

Again, it is not hard to check that multiplicative inverses and division have the properties you would hope them to have:

Exercise 5.5.1. Prove the following:

(a) The element $1_{\mathbb{K}}$ of $\mathbb{K}$ is always invertible.

(b) The element $-1_{\mathbb{K}}$ of $\mathbb{K}$ is always invertible. (Note that $-1_{\mathbb{K}}$ is not always distinct from $1_{\mathbb{K}}$.)

(c) Let $a \in \mathbb{K}$ be invertible. Then, its inverse a^{-1} is invertible as well, and its inverse is $\left(a^{-1}\right)^{-1} = a$.

(d) Let $a, b \in \mathbb{K}$ be invertible. Then, their product ab is invertible as well, and its inverse is $(ab)^{-1} = b^{-1}a^{-1}$. (Mind the order of multiplication: it is $b^{-1}a^{-1}$, not $a^{-1}b^{-1}$.)

(e) Assume that $\mathbb{K}$ is commutative. Let $a, b, c, d \in \mathbb{K}$ be such that b and d are invertible. Then,

$$a/b + c/d = (ad + bc) / (bd) \qquad \text{and} \qquad (a/b)(c/d) = (ac) / (bd).$$

Some rings have many invertible elements (such as $\mathbb{Q}$, where each nonzero element is invertible), while others have few (such as $\mathbb{Z}$, whose only invertible elements are 1 and -1). The extreme case on the former end is called a *skew field* or a *field*, depending on its commutativity:

Definition 5.5.5. (a) An element $a \in \mathbb{K}$ is said to be *nonzero* if $a \neq 0$. (Here, of course, 0 means the zero of $\mathbb{K}$.)

(b) We say that $\mathbb{K}$ is a *skew field* if $0 \neq 1$ in $\mathbb{K}$ and if every nonzero $a \in \mathbb{K}$ is invertible. (Here, "$0 \neq 1$ in $\mathbb{K}$" means "$0_{\mathbb{K}} \neq 1_{\mathbb{K}}$"; we are clearly not requiring the **integers** 0 and 1 to be distinct.)

(c) We say that $\mathbb{K}$ is a *field* if $\mathbb{K}$ is a commutative skew field.

The condition "$0 \neq 1$ in $\mathbb{K}$" has been made to rule out an annoying exception. It is easy to see that if a ring $\mathbb{K}$ satisfies $0 = 1$ in $\mathbb{K}$, then it has only one element (to wit: any $a \in \mathbb{K}$ must satisfy $a = \underbrace{1}_{=0} \cdot a = 0 \cdot a = 0$), which entails that $\mathbb{K}$ is the zero ring (up to relabeling of its element 0). We do not want the zero ring to count as a skew field[69]; thus we require $0 \neq 1$ in $\mathbb{K}$ in Definition 5.5.5.

Some authors call skew fields *division rings*.

Remark 5.5.6. If you work in constructive logic, you will want to replace the condition

$$\text{"every nonzero } a \in \mathbb{K} \text{ is invertible"} \tag{68}$$

in Definition 5.5.5 **(b)** by the stronger condition

$$\text{"every } a \in \mathbb{K} \text{ equals } 0_{\mathbb{K}} \text{ or is invertible"}. \tag{69}$$

While the condition (69) is clearly equivalent to (68) in classical logic, it is stronger in constructive logic, because it can be applied to any $a \in \mathbb{K}$ that is not a-priori known to be either zero or nonzero (whereas (68) requires a to be known to be nonzero, which is too burdensome a requirement to make it useful in constructive logic).

[69] just as we don't want the number 1 to count as a prime

Example 5.5.7. **(a)** The rings $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.

If you work in constructive logic, then you cannot prove that $\mathbb{R}$ and $\mathbb{C}$ are fields, because constructively there is no way to tell whether a real number is 0 or not. This is not a big issue for us, since we never truly use $\mathbb{R}$ and $\mathbb{C}$ in these notes (and when we do, we can replace them by smaller subrings of $\mathbb{C}$ that can be shown to be fields constructively – such as the Gaussian rationals).

(b) The rings $\mathbb{Z}$, $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\sqrt{2}\right]$ are not fields (since, for example, 2 is not invertible in any of these rings). However, $\mathbb{Z}[i]$ and $\mathbb{Z}\left[\sqrt{2}\right]$ would become fields if we had used $\mathbb{Q}$ instead of $\mathbb{Z}$ in their definitions.

(c) The polynomial ring $\mathbb{Z}[x]$ (which we will formally define in Chapter 7) is not a field (since, for example, x is not invertible in it). There is a way to get a field out of it, similarly to how $\mathbb{Q}$ is obtained from $\mathbb{Z}$. (This leads to the so-called *rational functions*.)

(d) Recall the commutative ring $\mathbb{Q}^{\mathbb{Q}}$; the elements of this ring are functions from $\mathbb{Q}$ to $\mathbb{Q}$, and the operations $+$ and $\cdot$ are defined pointwise. Is this ring a field?

Let us see what the multiplicative inverse of a function $f \in \mathbb{Q}^{\mathbb{Q}}$ is. If $f, g \in \mathbb{Q}^{\mathbb{Q}}$ are two functions, then we have the following chain of equivalences:

$$\begin{aligned}
&(g \text{ is the multiplicative inverse of } f) \\
&\iff \left(fg = gf = 1_{\mathbb{Q}^{\mathbb{Q}}}\right) \\
&\iff \left((fg)(x) = (gf)(x) = 1_{\mathbb{Q}^{\mathbb{Q}}}(x) \text{ for all } x \in \mathbb{Q}\right) \\
&\iff (f(x) \cdot g(x) = g(x) \cdot f(x) = 1 \text{ for all } x \in \mathbb{Q}) \\
&\qquad \left(\begin{array}{c} \text{since each } x \in \mathbb{Q} \text{ satisfies } (fg)(x) = f(x) \cdot g(x) \\ \text{and } (gf)(x) = g(x) \cdot f(x) \text{ and } 1_{\mathbb{Q}^{\mathbb{Q}}}(x) = 1 \end{array} \right) \\
&\iff \left(g(x) = \frac{1}{f(x)} \text{ for all } x \in \mathbb{Q}\right).
\end{aligned}$$

(Note that this is **not** the same as saying that f and g are inverse maps! The multiplication of $\mathbb{Q}^{\mathbb{Q}}$ is not given by composition of maps.)

This shows that a function $f \in \mathbb{Q}^{\mathbb{Q}}$ is invertible in $\mathbb{Q}^{\mathbb{Q}}$ if and only if it never takes the value 0 (because its multiplicative inverse g would have to satisfy $g(x) = \dfrac{1}{f(x)}$ for all $x \in \mathbb{Q}$). But a function $f \in \mathbb{Q}^{\mathbb{Q}}$ can be 0 at some point and $\neq 0$ at another. Then, it is not invertible (since it is 0 at some point) yet nonzero (since it is $\neq 0$ at another). For example, the function $\mathrm{id} \in \mathbb{Q}^{\mathbb{Q}}$ is not invertible yet nonzero. Thus, $\mathbb{Q}^{\mathbb{Q}}$ is not a field.

(e) The ring $\mathbb{Q}^{2\times 2}$ of 2×2-matrices with rational entries is not a skew field. Indeed, the 2×2-matrix $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ is nonzero but not invertible. (More generally: For each $n \in \mathbb{N}$, the $n \times n$-matrices over $\mathbb{Q}$ form a ring, which we will study

later. Our notion of "invertible" for elements of this ring coincides with the usual notion of "invertible" for $n \times n$-matrices in linear algebra.)

What about $\mathbb{Z}/n$?

Theorem 5.5.8. Let n be a positive integer. The ring $\mathbb{Z}/n$ is a field if and only if n is prime.

It is tricky to find a skew field that is not a field. Here is the simplest example of such a skew field:

Example 5.5.9. Informally, we have obtained $\mathbb{C}$ from $\mathbb{R}$ by throwing in a new number i that satisfies $i^2 = -1$. In order for i not to feel alone, let us introduce yet another new "number" j such that $j^2 = -1$ and $ji = -ij$. Now we try to calculate with these i and j. Of course, i and j cannot belong to a commutative ring together, but let us assume that they (and the further numbers we obtain from them) at least satisfy the ring axioms.

We have

$$i \cdot ij = \underbrace{ii}_{=i^2=-1} j = (-1)\, j = -j \qquad \text{and}$$

$$j \cdot ij = \underbrace{ji}_{=-ij} j = -i \underbrace{jj}_{=j^2=-1} = -i\,(-1) = i \qquad \text{and}$$

$$ij \cdot ij = i \underbrace{ji}_{=-ij} j = - \underbrace{ii}_{=i^2=-1} \underbrace{jj}_{=j^2=-1} = -\,(-1)\,(-1) = -1$$

and (using the distributivity laws)

$$\begin{aligned}(1 + 2i + 3ij)\,(2 - 3j) &= 2 + 4i + 6ij - 3j - 6ij - 9i \underbrace{j^2}_{=-1} \\ &= 2 + 4i - 3j + 9i = 2 + 13i - 3j.\end{aligned}$$

Similarly, any of these new "numbers" can be written in the form $a + bi + cj + dij$ for reals a, b, c, d.

Blithely introducing new "numbers" like this can be risky. It could happen that (just as with defining ∞ to be $\dfrac{1}{0}$) our new numbers would lead to contradictions. For example, what if we have some expression that involves i and j and that can be simplified to 0 in one way and simplified to 1 in another; would that mean that $0 = 1$? No; it would simply mean that the new "numbers" we have introduced do not actually exist. (Or, speaking more abstractly: that the new numbers are just the zero ring in a complicated disguise.)

So it makes sense to look for a rigorous definition of our new numbers. There is a direct (though rather painful) way of doing this: We can rigorously define

our new numbers as 4-tuples (a,b,c,d) of real numbers, with addition and subtraction defined entrywise, and with multiplication given by

$$\begin{aligned}&(x_1,x_2,x_3,x_4)\cdot(y_1,y_2,y_3,y_4)\\&=(x_1y_1-x_2y_2-x_3y_3-x_4y_4, x_1y_2+x_2y_1+x_3y_4-x_4y_3,\\&\qquad x_1y_3-x_2y_4+x_3y_1+x_4y_2, x_1y_4+x_2y_3-x_3y_2+x_4y_1).\end{aligned}$$

(The 4-tuple (a,b,c,d) is a rigorous model for the "number" $a+bi+cj+dij$.)

These new numbers are known as the *quaternions*. It turns out that they form a skew field, albeit not a field (since commutativity is lacking). They have several properties that make them useful in physics and space geometry. For one, they encode both the dot product and the cross product of two vectors in $\mathbb{R}^3$: Namely, if $\mathbf{a}=\begin{pmatrix}a_1\\a_2\\a_3\end{pmatrix}\in\mathbb{R}^3$ and $\mathbf{b}=\begin{pmatrix}b_1\\b_2\\b_3\end{pmatrix}\in\mathbb{R}^3$ are two vectors, then the quaternion

$$\begin{aligned}&(0,a_1,a_2,a_3)\cdot(0,b_1,b_2,b_3)\\&=\left(\underbrace{-a_1b_1-a_2b_2-a_3b_3}_{\substack{=-\mathbf{a}\cdot\mathbf{b}\\(\text{where }\cdot\text{ stands for}\\\text{the dot product})}}, \underbrace{a_2b_3-a_3b_2, a_3b_1-a_1b_3, a_1b_2-a_2b_1}_{\substack{\text{the three coordinates}\\\text{of the cross product }\mathbf{a}\times\mathbf{b}}}\right).\end{aligned}$$

Also, the quaternions can be used to encode rotations in 3-dimensional space (see, e.g., [Jia13]).

Exercise 5.5.2. Let $\mathbb{K}$ be a skew field. Let $x,y\in\mathbb{K}$ satisfy $xy=0$. (Here, of course, "0" means the zero of $\mathbb{K}$.) Prove that $x=0$ or $y=0$.

Exercise 5.5.3. Let $\mathbb{K}$ be a ring. Let $a,b,c\in\mathbb{K}$ be such that $ab=1$ and $bc=1$. Prove that the element b is invertible and its multiplicative inverse satisfies $b^{-1}=a=c$.

5.6. Hunting for finite fields I

Definition 5.6.1. **(a)** The *ground set* of a ring $(\mathbb{K},+,\cdot,0,1)$ is defined to be the set $\mathbb{K}$.

(b) The *elements* of a ring are defined to be the elements of its ground set.

(c) The *size* (or *cardinality*) of a ring is defined to be the size of its ground set.

(d) A ring is said to be *finite* if its size is finite (i.e., if it has only finitely many elements).

(e) A ring is said to be *trivial* if its size is 1.

We have seen a bunch of finite rings. For example, if S is a finite set, then the commutative ring $(\mathcal{P}(S), \triangle, \cap, \varnothing, S)$ (which was constructed in one of the examples in Section 5.2) has size $|\mathcal{P}(S)| = 2^{|S|}$, and thus is finite.

We also have seen infinitely many finite fields:

$$\mathbb{Z}/2, \qquad \mathbb{Z}/3, \qquad \mathbb{Z}/5, \qquad \mathbb{Z}/7, \qquad \mathbb{Z}/11, \qquad \ldots$$

Indeed, Theorem 5.5.8 yields that $\mathbb{Z}/p$ is a finite field whenever p is a prime.

Question 5.6.2. Are there any further finite fields?

Remark 5.6.3. Why do we care?

Recall Shamir's Secret Sharing Scheme, which we introduced in Subsection 1.6.7. The way we defined the Scheme, it had a problem: It relied on a spurious notion of a "uniformly random rational number", which does not exist in nature. Now we can fix this problem: Replace rational numbers by elements of a finite field. More precisely, let N again be the length of the bitstring that we want to encrypt. Pick a prime p that satisfies both $p \geq 2^N$ and $p > n$; this exists due to Theorem 2.13.43. Now, use elements of the finite field $\mathbb{Z}/p$ instead of integers. (Thus, a bitstring $a_{N-1}a_{N-2}\cdots a_0$ will be encoded as the residue class $\left[a_{N-1}\cdot 2^{N-1} + a_{N-2}\cdot 2^{N-2} + \cdots + a_0 \cdot 2^0\right]_p \in \mathbb{Z}/p$ rather than as the number $a_{N-1}\cdot 2^{N-1} + a_{N-2}\cdot 2^{N-2} + \cdots + a_0 \cdot 2^0 \in \mathbb{Z}$. This encoding can be uniquely decoded, because $p \geq 2^N$.) Instead of picking two uniformly random bitstrings $\mathbf{c}$ and $\mathbf{b}$ and transforming them into numbers c and b, just pick two uniformly random residue classes $c, b \in \mathbb{Z}/p$. (This is possible, since $\mathbb{Z}/p$ is a finite set.)

This relies on having a well-behaved notion of polynomials over $\mathbb{Z}/p$, which should satisfy the obvious analogue of Proposition 1.6.6 (with "numbers" replaced by "elements of $\mathbb{Z}/p$"). We will give a rigorous definition of this notion in Chapter 7.

Finite fields have many uses – not just in making Shamir's Secret Sharing Scheme work. One great source of applications is *coding theory*, which we will briefly encounter in Subsection 7.7.5.

Let us take some first steps towards addressing Question 5.6.2. We have found a field of size p for each prime p. Are there fields of other finite sizes? Let us first focus on the probably simplest case beyond $\mathbb{Z}/p$: Given a prime p, can we construct a field of size p^2 ?

First idea: Let us try to get such a field by "duplicating" the known field $\mathbb{Z}/p$. Thus, we fix a prime p, and consider the Cartesian product $(\mathbb{Z}/p) \times (\mathbb{Z}/p)$. Define addition, subtraction and multiplication on this Cartesian product entrywise[70]. This will yield a commutative ring with zero $\left([0]_p, [0]_p\right)$ and unity $\left([1]_p, [1]_p\right)$.

[70] That is,

$$\begin{aligned}(a,b) + (c,d) &= (a+c, b+d);\\ (a,b) - (c,d) &= (a-c, b-d);\\ (a,b)\,(c,d) &= (ac, bd)\end{aligned}$$

However, the element $\left([0]_p , [1]_p \right)$ of this ring is nonzero (because it is not $\left([0]_p , [0]_p \right)$) but has no inverse (since multiplying it by anything will never make its first entry anything other than $[0]_p$). So this ring is not a field.

(This is not a useless construction – we will see it in greater generality in Section 5.7 below. But it does not help us find new fields.)

Second idea: We obtained $\mathbb{C}$ from $\mathbb{R}$ by "adjoining" a square root of -1. (In abstract algebra, the verb "adjoin" means "insert" or "add" – not in the sense of the addition operation $+$, but in the sense of throwing in something new into an existing collection.)

Let us try to do this with $\mathbb{Z}/p$ instead of $\mathbb{R}$.

More generally, let us start with an arbitrary commutative ring $\mathbb{K}$, and try to "adjoin" a square root of -1 to it. We are bold and don't care whether there might already be such a square root in $\mathbb{K}$; if there is, then we will get a second one!

Let 0 and 1 stand for the zero and the unity of $\mathbb{K}$. If $\mathbb{K} = \mathbb{Z}/n$ for some integer n, then these are the residue classes $[0]_n$ and $[1]_n$.

Now, we want to define a new commutative ring $\mathbb{K}'$ by "adjoining" a square root of -1 to $\mathbb{K}$. A way to make this rigorous is as follows (just as we defined $\mathbb{C}$ rigorously in Definition 4.1.1):

Definition 5.6.4. Let $\mathbb{K}$ be a commutative ring.

(a) Let $\mathbb{K}'$ be the set of all pairs $(a, b) \in \mathbb{K} \times \mathbb{K}$.

(b) For each $r \in \mathbb{K}$, we denote the pair $(r, 0) \in \mathbb{K}'$ by $r_{\mathbb{K}'}$. We identify $r \in \mathbb{K}$ with $r_{\mathbb{K}'} = (r, 0) \in \mathbb{K}'$, so that $\mathbb{K}$ becomes a subset of $\mathbb{K}'$.

(c) We let i be the pair $(0, 1) \in \mathbb{K}'$.

(d) We define three binary operations $+$, $-$ and $\cdot$ on $\mathbb{K}'$ by setting

$$\begin{aligned} (a, b) + (c, d) &= (a + c, b + d), \\ (a, b) - (c, d) &= (a - c, b - d), \qquad \text{and} \\ (a, b) \cdot (c, d) &= (ac - bd, ad + bc) \end{aligned}$$

for all $(a, b) \in \mathbb{K}'$ and $(c, d) \in \mathbb{K}'$.

(e) If $\alpha, \beta \in \mathbb{K}'$, then we write $\alpha\beta$ for $\alpha \cdot \beta$.

You will, of course, recognize this definition to be a calque of Definition 4.1.1 with $\mathbb{R}$ and $\mathbb{C}$ replaced by $\mathbb{K}$ and $\mathbb{K}'$. The elements of $\mathbb{K}'$ are like complex numbers, but built upon $\mathbb{K}$ instead of $\mathbb{R}$.

Proposition 5.6.5. (a) The set $\mathbb{K}'$ defined in Definition 5.6.4 (equipped with the operations $+$ and $\cdot$ and the elements $0_{\mathbb{K}'}$ and $1_{\mathbb{K}'}$) is a commutative ring. Its subtraction is the binary operation $-$ defined in Definition 5.6.4 **(d)**.

(b) Furthermore, the ring $\mathbb{K}$ is a subring of $\mathbb{K}'$ (where we regard $\mathbb{K}$ as a subset of $\mathbb{K}'$ as explained in Definition 5.6.4 **(b)**).

for all $(a, b), (c, d) \in (\mathbb{Z}/p) \times (\mathbb{Z}/p)$.

Convention 5.6.6. For the rest of this section, we let $\mathbb{K}'$ be the commutative ring constructed in Proposition 5.6.5 (i.e., the set $\mathbb{K}'$ equipped with the operations $+$ and $\cdot$ and the elements $0_{\mathbb{K}'}$ and $1_{\mathbb{K}'}$).

Thus, if $\mathbb{K} = \mathbb{Z}/p$, then $\mathbb{K}'$ is a commutative ring with p^2 elements.

Question 5.6.7. When is $\mathbb{K}'$ is a field?

Assume that $0 \neq 1$ in $\mathbb{K}$; thus, $0 \neq 1$ in $\mathbb{K}'$ as well (since $0_{\mathbb{K}'} = (0,0) \neq (1,0) = 1_{\mathbb{K}'}$). Hence, in order for $\mathbb{K}'$ to be a field, every nonzero $\xi \in \mathbb{K}'$ needs to have a multiplicative inverse. Thus, in particular, every nonzero element of $\mathbb{K}$ must have a multiplicative inverse in $\mathbb{K}'$. It is easy to see that such an inverse, if it exists, must belong to $\mathbb{K}$ as well (i.e., it must have the form $r_{\mathbb{K}'}$ for some $r \in \mathbb{K}$); thus, this means that every nonzero element of $\mathbb{K}$ must have a multiplicative inverse in $\mathbb{K}$. In other words, $\mathbb{K}$ itself must be a field.

Thus, we assume from now on that $\mathbb{K}$ is a field. But we are not done yet. It is definitely not always true that $\mathbb{K}'$ is a field. For example, if $\mathbb{K} = \mathbb{Z}/2$, then the element $(1,1)$ of $\mathbb{K}'$ has no inverse (check this!), and so $\mathbb{K}'$ is not a field in this case. What must $\mathbb{K}$ satisfy in order for $\mathbb{K}'$ to be a field?

We know what it must satisfy: The condition is that every nonzero $\xi \in \mathbb{K}'$ has a multiplicative inverse. We just need to see when this condition holds.

So let $\xi = (x,y) \in \mathbb{K}'$ (with $x, y \in \mathbb{K}$) be nonzero. Thus, $(x,y) \neq (0,0)$.

How to find ξ^{-1} ? Notice that $\xi = (x,y) = x + yi$ (this is proven just as for complex numbers). Thus, you can try to compute ξ^{-1} by rationalizing the denominator (just as we learned to divide complex numbers):

$$\frac{1}{\xi} = \frac{1}{x+yi} = \frac{x-yi}{(x+yi)(x-yi)} = \frac{x-yi}{x^2+y^2}$$

(since $(x+yi)(x-yi) = (x,y)(x,-y) = \left(x^2+y^2, 0\right)$, as you can easily see using the definition of $\cdot$ on $\mathbb{K}'$).

We need $x^2 + y^2 \neq 0$ in $\mathbb{K}$ for this to work. In other words, we need the following condition to hold:

> *Condition 1:* For every pair $(x,y) \in \mathbb{K} \times \mathbb{K}$ satisfying $(x,y) \neq (0,0)$, we have $x^2 + y^2 \neq 0$ in $\mathbb{K}$.

Thus, $\mathbb{K}'$ is a field if Condition 1 holds. Conversely, if $\mathbb{K}'$ is a field, then Condition 1 holds (because if $(x,y) \in \mathbb{K} \times \mathbb{K}$ satisfies $(x,y) \neq (0,0)$, then $(x,y)(x,-y) = \left(x^2+y^2, 0\right)$ would have to be $\neq (0,0)$ in order for $\mathbb{K}'$ to be a field[71]). So $\mathbb{K}'$ is a field if and only if Condition 1 holds.

If $\mathbb{K} = \mathbb{Z}/p$ for some prime p, then Condition 1 can be restated as follows:

> *Condition 1':* For every pair $(x,y) \in (\mathbb{Z}/p) \times (\mathbb{Z}/p)$ satisfying $(x,y) \neq (0,0)$, we have $x^2 + y^2 \neq 0$ in $\mathbb{Z}/p$.

[71] by Exercise 5.5.2

We can further restate Condition 1′ in terms of integers by replacing the residue classes x and y with their representatives a and b:

> *Condition 2:* For every pair $(a,b) \in \mathbb{Z} \times \mathbb{Z}$ such that **not both** a and b are divisible by p, the sum $a^2 + b^2$ is not divisible by p.

So the ring $\mathbb{K}'$ constructed from $\mathbb{K} = \mathbb{Z}/p$ is a field if and only if Condition 2 holds. When does Condition 2 hold?

Example 5.6.8. Let $\mathbb{K} = \mathbb{Z}/p$.
(a) If $p = 2$, then Condition 2 fails for $(a,b) = (1,1)$. So $\mathbb{K}'$ is not a field for $p = 2$.
(b) If $p = 3$, then Condition 2 holds. So $\mathbb{K}'$ is a field for $p = 3$. Thus we have found a field with $3^2 = 9$ elements.
(c) If $p = 5$, then Condition 2 fails for $(a,b) = (1,2)$. So $\mathbb{K}'$ is not a field for $p = 5$.

This suggests that the following:

Proposition 5.6.9. A prime p satisfies Condition 2 if and only if $p \equiv 3 \bmod 4$.

Thus, if we set $\mathbb{K} = \mathbb{Z}/p$ where p is a prime of Type 3, then $\mathbb{K}'$ will be a field. So we have found a field $\mathbb{K}'$ with p^2 elements for any prime p of Type 3. What about the other primes?

We can try to vary the construction above: Instead of adjoining a square root of -1, we adjoin a square root of some other element $\eta \in \mathbb{Z}/p$.

Definition 5.6.10. Let $\mathbb{K}$ be a ring. A *square* (in $\mathbb{K}$) means an element of the form a^2 for some $a \in \mathbb{K}$.

Now, we generalize Definition 5.6.4 as follows:

Definition 5.6.11. Let $\mathbb{K}$ be a commutative ring. Let $\eta \in \mathbb{K}$.
(a) Let $\mathbb{K}'_\eta$ be the set of all pairs $(a,b) \in \mathbb{K} \times \mathbb{K}$.
(b) For each $r \in \mathbb{K}$, we denote the pair $(r,0) \in \mathbb{K}'_\eta$ by $r_{\mathbb{K}'_\eta}$. We identify $r \in \mathbb{K}$ with $r_{\mathbb{K}'_\eta} = (r,0) \in \mathbb{K}'_\eta$, so that $\mathbb{K}$ becomes a subset of $\mathbb{K}'_\eta$.
(c) We let i_η be the pair $(0,1) \in \mathbb{K}'_\eta$.
(d) We define three binary operations $+$, $-$ and $\cdot$ on $\mathbb{K}'_\eta$ by setting

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d), \\ (a,b) - (c,d) &= (a-c, b-d), \qquad \text{and} \\ (a,b) \cdot (c,d) &= (ac + \eta bd, ad + bc) \end{aligned}$$

for all $(a,b) \in \mathbb{K}'_\eta$ and $(c,d) \in \mathbb{K}'_\eta$.
(e) If $\alpha, \beta \in \mathbb{K}'_\eta$, then we write $\alpha\beta$ for $\alpha \cdot \beta$.

Note that $\mathbb{K}'_\eta$ differs from $\mathbb{K}'$ only in how the multiplication is defined. Note also that $\mathbb{K}'_{-1} = \mathbb{K}'$.

Theorem 5.6.12. **(a)** The set $\mathbb{K}'_\eta$ defined in Definition 5.6.11 (equipped with the operations $+$ and $\cdot$ and the elements $0_{\mathbb{K}'_\eta}$ and $1_{\mathbb{K}'_\eta}$) is a commutative ring. Its subtraction is the operation $-$ defined in Definition 5.6.11 **(d)**.

(b) If $\mathbb{K}$ is a field and η is not a square in $\mathbb{K}$, then $\mathbb{K}'_\eta$ is a field.

(c) Let p be a prime. There always exists an element $\eta \in \mathbb{Z}/p$ that is not a square, **unless** $p = 2$.

Now, if p is a prime with $p > 2$, then Theorem 5.6.12 **(c)** yields that there exists an element $\eta \in \mathbb{Z}/p$ that is not a square; therefore, Theorem 5.6.12 **(b)** shows that $\mathbb{K}'_\eta$ is a field where $\mathbb{K} = \mathbb{Z}/p$. This is a field with p^2 elements.

Is there a field of size 4, too?

We cannot get such a field by adjoining a square root to $\mathbb{Z}/2$. So let us instead try to adjoin an element j such that $j^2 = j + 1$. Formally, we can do this as follows: We define $\mathbb{K}''$ as the set of all pairs $(a, b) \in (\mathbb{Z}/2) \times (\mathbb{Z}/2)$, and we define three operations $+$, $-$ and $\cdot$ on $\mathbb{K}''$ by

$$\begin{aligned} (a,b) + (c,d) &= (a+c, b+d), \\ (a,b) - (c,d) &= (a-c, b-d), \qquad \text{and} \\ (a,b) \cdot (c,d) &= (ac+bd, ad+bc+bd). \end{aligned}$$

You can check that this is a field with 4 elements.

Thus, for each prime p, we have found a field with p^2 elements.

For the sake of completeness, let me mention a **third idea** for constructing fields of size p^2: Recall that our field $\mathbb{Z}/p$ of size p consisted of residue classes of integers modulo p. What happens if we take the residue classes of Gaussian integers modulo a Gaussian prime π ?

I will not go into details, but here is a summary:

- The result is always a field of size $\mathrm{N}(\pi)$.
- If π is not unit-equivalent to an integer, then this is a field that we already know (namely, $\mathbb{Z}/p$ for $p = \mathrm{N}(\pi)$) with its elements relabelled.
- If π is unit-equivalent to an integer, then π is unit-equivalent to a prime p of Type 3, and the field of residue classes modulo π will be a field with p^2 elements. Namely, it will be the field $\mathbb{K}'$ we constructed above (for $\mathbb{K} = \mathbb{Z}/p$), with its elements relabelled.

So this approach only gets us fields of size p^2 when p is a prime of Type 3; it is thus inferior to the second idea above. Nevertheless, it illustrates a general idea: that residue classes make sense not only for integers.

Warning: When p is a prime, the ring $\mathbb{Z}/p^2$ is **not** a field; thus, the field with p^2 elements that we constructed is not $\mathbb{Z}/p^2$.

Now, what about finite fields of size $p^3, p^4, \ldots$? What about finite fields of size 6 ?

Spoiler: It turns out that the former exist, while the latter do not. We will hopefully prove this later. More generally, for an integer $n > 1$, there exists a field of size n if and only if n is a prime power (= a positive power of a prime). Even better, if n is a prime power, then a field of size n is unique up to relabeling. We hope to see a proof of this (at least of the existence part) further on in this class.

5.7. Cartesian products

Next comes a basic and unimaginative way of constructing new rings from old:

Definition 5.7.1. Let $\mathbb{K}_1, \mathbb{K}_2, \ldots, \mathbb{K}_n$ be n rings. Consider the set $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$, whose elements are n-tuples $(k_1, k_2, \ldots, k_n)$ with $k_i \in \mathbb{K}_i$.

We define operations $+$ and $\cdot$ on $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$ by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \qquad \text{and}$$
$$(a_1, a_2, \ldots, a_n) \cdot (b_1, b_2, \ldots, b_n) = (a_1 b_1, a_2 b_2, \ldots, a_n b_n) .$$

Proposition 5.7.2. Let $\mathbb{K}_1, \mathbb{K}_2, \ldots, \mathbb{K}_n$ be n rings.

(a) The set $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$, endowed with the operations $+$ and $\cdot$ we just defined and with the zero $(0, 0, \ldots, 0)$ and the unity $(1, 1, \ldots, 1)$, is a ring.

(b) If the rings $\mathbb{K}_1, \mathbb{K}_2, \ldots, \mathbb{K}_n$ are commutative, then so is the ring $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$.

Definition 5.7.3. The ring $\mathbb{K}_1 \times \mathbb{K}_2 \times \cdots \times \mathbb{K}_n$ constructed in Proposition 5.7.2 is called the *Cartesian product* (or *direct product*) of the rings $\mathbb{K}_1, \mathbb{K}_2, \ldots, \mathbb{K}_n$.

Example 5.7.4. We have already seen a Cartesian product. Indeed, recall the binary operations XOR defined back in Subsection 1.6.4.

(a) We first defined an operation XOR on bits (Definition 1.6.3), and then defined an operation XOR on bitstrings (Definition 1.6.4). It is easy to see that

$$(\{0, 1\}, \mathrm{XOR}, \cdot, 0, 1)$$

is a commutative ring. Let me call this ring $\mathbb{X}$ for now. Note that this ring $\mathbb{X}$ can be seen as $\mathbb{Z}/2$ with its elements relabeled (more precisely, the elements $[0]_2$ and $[1]_2$ of $\mathbb{Z}/2$ need to be relabelled as 0 and 1 in order to get $\mathbb{X}$); for example, the correspondence between the XOR operation on $\mathbb{X}$ and the addition on $\mathbb{Z}/2$ can be seen by comparing their results face to face:

$$\begin{aligned}
0 \,\mathrm{XOR}\, 0 = 0 \qquad &\text{and} \qquad [0]_2 + [0]_2 = [0]_2 , \\
0 \,\mathrm{XOR}\, 1 = 1 \qquad &\text{and} \qquad [0]_2 + [1]_2 = [1]_2 , \\
1 \,\mathrm{XOR}\, 0 = 1 \qquad &\text{and} \qquad [1]_2 + [0]_2 = [1]_2 , \\
1 \,\mathrm{XOR}\, 1 = 0 \qquad &\text{and} \qquad [1]_2 + [1]_2 = [0]_2 .
\end{aligned}$$

(b) Let $m \in \mathbb{N}$. In Definition 1.6.4, we defined a binary operation XOR on $\{0,1\}^m$, i.e., on length-m bitstrings. This gives a ring

$$\left(\{0,1\}^m, \text{XOR}, \text{entrywise multiplication}, 00\cdots0, 11\cdots1\right)$$

of bitstrings. This ring is precisely the Cartesian product

$$\underbrace{\mathbb{X} \times \mathbb{X} \times \cdots \times \mathbb{X}}_{m \text{ times}}.$$

5.8. Matrices and matrix rings

Convention 5.8.1. In this section, we fix a ring $\mathbb{K}$.

We take the familiar concept of matrices, and generalize it in a straightforward way, allowing matrices with entries in $\mathbb{K}$:

Definition 5.8.2. Given $n, m \in \mathbb{N}$, we define an *$n \times m$-matrix over $\mathbb{K}$* to be a rectangular table with n rows and m columns whose entries are elements of $\mathbb{K}$. When $\mathbb{K}$ is clear from the context (or irrelevant), we just say "$n \times m$-matrix" instead of "$n \times m$-matrix over $\mathbb{K}$".

For example, if $\mathbb{K} = \mathbb{Q}$, then

$$\begin{pmatrix} 0 & 1/3 & -6 \\ -1 & -2/5 & 1 \end{pmatrix}$$

is a 2×3-matrix over $\mathbb{K}$.

(Formally, an $n \times m$-matrix is defined as a map from $\{1,2,\ldots,n\} \times \{1,2,\ldots,m\}$ to $\mathbb{K}$. Its entry in row i and column j is then defined to be the image of the pair (i,j) under this map.)

Note that the "$\times$" symbol in the notion of an "$n \times m$-matrix" is just a symbol, not an invitation to actually multiply the numbers n and m together! For example, $2 \cdot 3 = 3 \cdot 2$, yet a 2×3-matrix is not the same as a 3×2-matrix.

Let us define two pieces of notation:

Definition 5.8.3. Let A be an $n \times m$-matrix over $\mathbb{K}$. Let $i \in \{1,2,\ldots,n\}$ and $j \in \{1,2,\ldots,m\}$. The *(i,j)-th entry of A* is defined to be the entry of A in row i and column j.

Definition 5.8.4. Let $n, m \in \mathbb{N}$. Assume that we are given some element $a_{i,j} \in \mathbb{K}$ for every $(i,j) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,m\}$. Then, we shall use the notation

$$\left(a_{i,j}\right)_{1 \le i \le n,\ 1 \le j \le m} \tag{70}$$

for the $n \times m$-matrix

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{pmatrix}$$

(this is the $n \times m$-matrix whose (i,j)-th entry is $a_{i,j}$ for all i and j).

For example,

$$(i+j)_{1 \leq i \leq 3,\ 1 \leq j \leq 4} = \begin{pmatrix} 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 7 \end{pmatrix} \qquad \text{and}$$

$$(i-j)_{1 \leq i \leq 3,\ 1 \leq j \leq 4} = \begin{pmatrix} 0 & -1 & -2 & -3 \\ 1 & 0 & -1 & -2 \\ 2 & 1 & 0 & -1 \end{pmatrix}.$$

The letters i and j in the notation (70) are not set in stone; we can use any other letters instead. For example,

$$(i-j)_{1 \leq i \leq 3,\ 1 \leq j \leq 4} = (x-y)_{1 \leq x \leq 3,\ 1 \leq y \leq 4} = (j-i)_{1 \leq j \leq 3,\ 1 \leq i \leq 4}.$$

Definition 5.8.5. Let $n, m \in \mathbb{N}$. Then, $\mathbb{K}^{n \times m}$ will denote the set of all $n \times m$-matrices. (Some call it $\mathrm{M}_{n,m}(\mathbb{K})$ instead.)

Again, the "$\times$" symbol in this notation is just a symbol; it does not stand for a product of numbers.

Definition 5.8.6. **(a)** A *matrix* means an $n \times m$-matrix for some $n, m \in \mathbb{N}$.
(b) A *square matrix* means an $n \times n$-matrix for some $n \in \mathbb{N}$.

For example, $\begin{pmatrix} 1 & 2 & 6 \\ 3 & 4 & 5 \end{pmatrix}$ is a matrix, and $\begin{pmatrix} 2 & 6 \\ 4 & 5 \end{pmatrix}$ is a square matrix.
We now define various operations with matrices:

Definition 5.8.7. Fix $n, m \in \mathbb{N}$.
(a) The *sum* $A + B$ of two $n \times m$-matrices A and B is defined entrywise: i.e., if $A = \left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$ and $B = \left(b_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$, then

$$A + B = \left(a_{i,j} + b_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}.$$

(b) The *difference* $A - B$ of two $n \times m$-matrices A and B is defined entrywise: i.e., if $A = \left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$ and $B = \left(b_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$, then

$$A - B = \left(a_{i,j} - b_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}.$$

(c) We define *scaling* of $n \times m$-matrices as follows: If $\lambda \in \mathbb{K}$ and $A \in \mathbb{K}^{n \times m}$, then the matrix $\lambda A \in \mathbb{K}^{n \times m}$ is defined by multiplying each entry of A by λ. Formally speaking: if $A = \left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$, then

$$\lambda A = \left(\lambda a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}.$$

To be more honest, the operation we defined in Definition 5.8.7 **(c)** should have been called "left scaling" rather than "scaling". And we should have defined an analogous operation called "right scaling", which takes an element $\lambda \in \mathbb{K}$ and a matrix $A = \left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m} \in \mathbb{K}^{n \times m}$, and returns a new matrix

$$A\lambda = \left(a_{i,j}\lambda\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}.$$

But we will mostly be dealing with the case when the ring $\mathbb{K}$ is commutative; and in this case, we always have $A\lambda = \lambda A$ (meaning that "right scaling" and "left scaling" are the same operation). Thus, we take the liberty to neglect the "right scaling" operation. (Its properties are analogous to the corresponding properties of "left scaling" anyway.)

Let us now define an operation on matrices that is **not** computed entrywise: their product.

Definition 5.8.8. Let $n, m, p \in \mathbb{N}$. Let $A = \left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$ be an $n \times m$-matrix. Let $B = \left(b_{i,j}\right)_{1 \leq i \leq m,\ 1 \leq j \leq p}$ be an $m \times p$-matrix. Then, we define the *product* AB of the two matrices A and B by

$$AB = \left(\sum_{k=1}^{m} a_{i,k} b_{k,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq p}.$$

This is an $n \times p$-matrix.

So you can add together two $n \times m$-matrices, but only multiply an $n \times m$-matrix with an $m \times p$-matrix. (You cannot multiply two $n \times m$-matrices, unless $n = m$.)

Next, we define two special families of matrices:

Definition 5.8.9. (a) If $n, m \in \mathbb{N}$, then the $n \times m$ *zero matrix* is defined to be the $n \times m$-matrix

$$(0)_{1 \leq i \leq n,\ 1 \leq j \leq m} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

It is called $0_{n \times m}$.

(b) If $n \in \mathbb{N}$, then the $n \times n$ *identity matrix* is defined to be the $n \times n$-matrix

$$\left(\delta_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq n} = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix},$$

where

$$\delta_{i,j} = \begin{cases} 1, & \text{if } i = j; \\ 0, & \text{if } i \neq j \end{cases}.$$

(Note that using the Iverson bracket notation we introduced in Exercise 2.17.2, we have $\delta_{i,j} = [i = j] \cdot 1_{\mathbb{K}}$.)

The $n \times n$ identity matrix is called I_n.

Note that the 0 and the 1 here are the zero and the unity of $\mathbb{K}$.

Thus, a zero matrix can be of any size, but an identity matrix has to be a square matrix.

If $n, m \in \mathbb{N}$ and $A \in \mathbb{K}^{n \times m}$, then $-A$ shall denote the matrix $0_{n \times m} - A \in \mathbb{K}^{n \times m}$.

The following rules hold for addition, subtraction, multiplication and scaling of matrices:

Theorem 5.8.10. Let $n, m, p, q \in \mathbb{N}$.

(a) We have $A + B = B + A$ for any $A, B \in \mathbb{K}^{n \times m}$.

(b) We have $A + (B + C) = (A + B) + C$ for any $A, B, C \in \mathbb{K}^{n \times m}$.

(c) We have $A + 0_{n \times m} = 0_{n \times m} + A = A$ for any $A \in \mathbb{K}^{n \times m}$.

(d) We have $A \cdot I_m = I_n \cdot A = A$ for any $A \in \mathbb{K}^{n \times m}$.

(e) In general, we **do not** have $AB = BA$. In fact, it can happen that one of AB and BA is defined and the other is not; but even if both are defined, they can be distinct (even if $\mathbb{K}$ is commutative).

(f) We have $A(BC) = (AB)C$ for any $A \in \mathbb{K}^{n \times m}$, $B \in \mathbb{K}^{m \times p}$ and $C \in \mathbb{K}^{p \times q}$.

(g) We have $A(B + C) = AB + AC$ for any $A \in \mathbb{K}^{n \times m}$ and $B, C \in \mathbb{K}^{m \times p}$.

We have $(A + B)C = AC + BC$ for any $A, B \in \mathbb{K}^{n \times m}$ and $C \in \mathbb{K}^{m \times p}$.

(h) We have $A \cdot 0_{m \times p} = 0_{n \times p}$ and $0_{p \times n} \cdot A = 0_{p \times m}$ for any $A \in \mathbb{K}^{n \times m}$.

(i) If $A, B, C \in \mathbb{K}^{n \times m}$, then we have the equivalence $(A - B = C) \iff (A = B + C)$.

(j) We have $r(A + B) = rA + rB$ for any $r \in \mathbb{K}$ and $A, B \in \mathbb{K}^{n \times m}$.

(k) We have $(r + s)A = rA + sA$ for any $r, s \in \mathbb{K}$ and $A \in \mathbb{K}^{n \times m}$.

(l) We have $r(sA) = (rs)A$ for any $r, s \in \mathbb{K}$ and $A \in \mathbb{K}^{n \times m}$.

(m) We have $r(AB) = (rA)B = A(rB)$ for any $r \in \mathbb{K}$ and $A \in \mathbb{K}^{n \times m}$ and $B \in \mathbb{K}^{m \times p}$ if $\mathbb{K}$ is commutative. The first equality also holds in general.

(n) We have $-(rA) = (-r)A = r(-A)$ for any $r \in \mathbb{K}$ and $A \in \mathbb{K}^{n \times m}$.

(o) We have $1A = A$ for any $A \in \mathbb{K}^{n \times m}$.

(p) We have $(-1)A = -A$ for any $A \in \mathbb{K}^{n \times m}$.

(q) We have $-(A+B) = (-A) + (-B)$ for any $A, B \in \mathbb{K}^{n\times m}$.
(r) We have $-0_{n\times m} = 0_{n\times m}$.
(s) We have $-(-A) = A$ for any $A \in \mathbb{K}^{n\times m}$.
(t) We have $-(AB) = (-A)\,B = A\,(-B)$ for any $A \in \mathbb{K}^{n\times m}$ and $B \in \mathbb{K}^{m\times p}$.
(u) We have $A - B - C = A - (B + C)$ for any $A, B, C \in \mathbb{K}^{n\times m}$. (Here and in the following, "$A - B - C$" should be read as "$(A - B) - C$".)

Corollary 5.8.11. Let $n \in \mathbb{N}$. The set $\mathbb{K}^{n\times n}$ of all $n \times n$-matrices (endowed with addition $+$, multiplication $\cdot$, zero $0_{n\times n}$ and unity I_n) is a ring.

Definition 5.8.12. Let $n \in \mathbb{N}$. The ring $\mathbb{K}^{n\times n}$ defined in Corollary 5.8.11 is called the *n-th matrix ring* over $\mathbb{K}$.

So we know that $\mathbb{K}^{n\times n}$ is a ring whenever $n \in \mathbb{N}$. Hence, Proposition 5.4.6 shows that we can define finite sums and finite products in $\mathbb{K}^{n\times n}$ (but finite products need to have the order of their factors specified: i.e., we can make sense of "$A_1 A_2 \cdots A_k$" but not of "$\prod_{s\in S} A_s$"). These also make sense for non-square matrices whenever "their sizes match": e.g., you can define a sum of finitely many $n \times m$-matrices, and a product $A_1 A_2 \cdots A_k$ where each A_i is an $n_i \times n_{i+1}$-matrix (for any $n_1, n_2, \ldots, n_{k+1} \in \mathbb{N}$). Standard rules for sums and products hold, at least to the extent they don't rely on commutativity of multiplication.

But $\mathbb{K}^{n\times n}$ is not the only ring we can make out of matrices. In fact, $\mathbb{K}^{n\times n}$ is full of interesting subrings, which are obtained by restricting ourselves to special kinds of matrices. Here are some of these:

Definition 5.8.13. Let $n \in \mathbb{N}$. Let $A = \left(a_{i,j}\right)_{1\le i\le n,\ 1\le j\le n}$ be an $n \times n$-matrix.
(a) We say that A is *lower-triangular* if and only if

$$a_{i,j} = 0 \qquad \text{whenever } i < j.$$

(b) We say that A is *upper-triangular* if and only if

$$a_{i,j} = 0 \qquad \text{whenever } i > j.$$

(c) We say that A is *diagonal* if and only if

$$a_{i,j} = 0 \qquad \text{whenever } i \neq j.$$

For example, the 2×2-matrix $\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ is upper-triangular (but not lower-triangular), while the 2×2-matrix $\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}$ is lower-triangular (but not upper-triangular).

Proposition 5.8.14. Let $n \in \mathbb{N}$.
(a) The set of all lower-triangular $n \times n$-matrices is a subring of $\mathbb{K}^{n \times n}$.
(b) The set of all upper-triangular $n \times n$-matrices is a subring of $\mathbb{K}^{n \times n}$.
(c) The set of all diagonal $n \times n$-matrices is a subring of $\mathbb{K}^{n \times n}$.

Example 5.8.15. For $n = 2$, the multiplication of lower-triangular $n \times n$-matrices looks as follows:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix},$$

and the multiplication of diagonal $n \times n$-matrices looks as follows:

$$\begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & 0 \\ 0 & cz \end{pmatrix}.$$

Note that diagonal $n \times n$-matrices are "essentially" the same as n-tuples of elements of $\mathbb{K}$; the ring they form is $\underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ times}}$ in disguise. We will make this precise in Example 5.10.3 (using the notion of a ring isomorphism).

One of the most important operations on matrices is taking the transpose:

Definition 5.8.16. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $A = \left(a_{i,j}\right)_{1 \leq i \leq n,\ 1 \leq j \leq m}$ be an $n \times m$-matrix. Then, we define an $m \times n$-matrix A^T by

$$A^T = \left(a_{j,i}\right)_{1 \leq i \leq m,\ 1 \leq j \leq n}.$$

Thus, for each $i \in \{1, 2, \ldots, m\}$ and $j \in \{1, 2, \ldots, n\}$, the (i, j)-th entry of A^T is the (j, i)-th entry of A. This matrix A^T is called the *transpose* of A.

For example,

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}^T = \begin{pmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}^T = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix}.$$

Let us use this occasion to define column vectors and row vectors:

Definition 5.8.17. Let $n \in \mathbb{N}$.
(a) A *column vector of size n* will mean an $n \times 1$-matrix.
(b) A *row vector of size n* will mean a $1 \times n$-matrix.

For example, $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ is a column vector of size 2, while $\begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ is a row vector of size 3. We will often identify a row vector $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix} \in \mathbb{K}^{1 \times n}$ with the corresponding n-tuple $(a_1, a_2, \ldots, a_n)$.

If v is a column vector of size n, then v^T is a row vector of size n.

5.9. Ring homomorphisms

Definition 5.9.1. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. A *ring homomorphism* from $\mathbb{K}$ to $\mathbb{L}$ means a map $f : \mathbb{K} \to \mathbb{L}$ that satisfies the following four axioms:

- **(a)** We have $f(a+b) = f(a) + f(b)$ for all $a, b \in \mathbb{K}$. (This is called "f respects addition" or "f preserves addition".)
- **(b)** We have $f(0) = 0$. (This, of course, means $f(0_{\mathbb{K}}) = 0_{\mathbb{L}}$.)
- **(c)** We have $f(ab) = f(a) f(b)$ for all $a, b \in \mathbb{K}$. (This is called "f respects multiplication" or "f preserves multiplication".)
- **(d)** We have $f(1) = 1$. (This, of course, means $f(1_{\mathbb{K}}) = 1_{\mathbb{L}}$.)

Remark 5.9.2. The statement "$f(a+b) = f(a) + f(b)$" in Definition 5.9.1 should, of course, be understood as "$f(a +_{\mathbb{K}} b) = f(a) +_{\mathbb{L}} f(b)$". Likewise, the statement "$f(ab) = f(a) f(b)$" should be understood as "$f(a \cdot_{\mathbb{K}} b) = f(a) \cdot_{\mathbb{L}} f(b)$". In Definition 5.9.1, we could afford omitting the "$_{\mathbb{K}}$" and "$_{\mathbb{L}}$" subscripts under the "$+$" and "$\cdot$" signs because it is always clear whether the things being added (or multiplied) are in $\mathbb{K}$ or in $\mathbb{L}$; but in many practical situations we do not have such luxury (for example, because $\mathbb{K}$ and $\mathbb{L}$ have elements in common) and thus need to include these subscripts. (See Example 5.10.6 for an example of such a situation.)

Remark 5.9.3. The axiom **(b)** in Definition 5.9.1 is redundant – it follows from axiom **(a)**.

If the axiom **(b)** in Definition 5.9.1 is redundant, then why did we require it? One reason to do so is purely aesthetic: It ensures that each of the two "multiplicative" axioms (viz., axioms **(c)** and **(d)**) is matched by a corresponding "additive" axiom (viz., axioms **(a)** and **(b)**). We cannot omit axiom **(d)**[72]; thus, to avoid breaking the symmetry, I prefer not to omit axiom **(b)** either. But there is also another reason to keep axiom **(b)**. Indeed, if we want to define *semiring homomorphisms* (i.e., the analogue of ring homomorphisms in which rings are replaced by semirings), then axiom **(b)** is no longer redundant (since we cannot subtract elements in a semiring); thus, if we omitted axiom **(b)**, our definition of ring homomorphisms would become less robust with respect to replacing "ring" by "semiring".

Example 5.9.4. Let $\mathbb{K}$ be any ring. The map $\mathrm{id} : \mathbb{K} \to \mathbb{K}$ is a ring homomorphism.

We can slightly generalize Example 5.9.4 as follows:

[72] More precisely: if we did, then we would obtain a weaker, less useful notion of ring homomorphism.

Example 5.9.5. Let $\mathbb{K}$ be a subring of a ring $\mathbb{L}$. Let $\iota : \mathbb{K} \to \mathbb{L}$ be the map that sends each $a \in \mathbb{K}$ to a itself. (This map is called the *inclusion map* from $\mathbb{K}$ to $\mathbb{L}$.) Then, ι is a ring homomorphism.

Example 5.9.6. Let $\mathbb{K}$ be any ring, and let $\mathbb{M}$ be the zero ring $\{0\}$. Then, the map

$$\mathbb{K} \to \mathbb{M}, \qquad a \mapsto 0$$

is a ring homomorphism.

Example 5.9.7. Let n be an integer. Consider the projection

$$\begin{aligned} \pi_{\underset{n}{\equiv}} : \mathbb{Z} &\to \mathbb{Z}/n, \\ s &\mapsto [s]_n . \end{aligned}$$

This is a ring homomorphism.

Example 5.9.8. Let n be a positive integer. Consider the map

$$\begin{aligned} R_n : \mathbb{Z}/n &\to \mathbb{Z}, \\ [s]_n &\mapsto s\%n. \end{aligned}$$

(This is the map sending $[0]_n, [1]_n, \ldots, [n-1]_n$ to the numbers $0, 1, \ldots, n-1$.) This map R_n is **not** a ring homomorphism.

Warning: The same people who don't require rings to have a unity, of course, do not require ring homomorphisms to satisfy axiom **(d)**. So for them, R_n would be a ring homomorphism for $n = 1$.

Example 5.9.9. Let n and d be integers such that $d \mid n$. Then, the map

$$\begin{aligned} \pi_{n,d} : \mathbb{Z}/n &\to \mathbb{Z}/d, \\ [s]_n &\mapsto [s]_d \end{aligned}$$

is a ring homomorphism.

Remark 5.9.10. Let n and d be integers. Then:
(a) If $d \mid n$, then the only ring homomorphism from $\mathbb{Z}/n$ to $\mathbb{Z}/d$ is $\pi_{n,d}$.
(b) If $d \nmid n$, then there is no ring homomorphism from $\mathbb{Z}/n$ to $\mathbb{Z}/d$.

Remark 5.9.10 is not hard to prove, but we won't do this here.

Example 5.9.11. Consider the map $\mu : \mathbb{C} \to \mathbb{R}^{2\times 2}$ defined in Proposition 4.1.31. This map μ is a ring homomorphism.

Example 5.9.12. Let $\iota_{\mathbb{C}}$ be the map

$$\begin{aligned} &\mathbb{R} \to \mathbb{C}, \\ &r \mapsto r_{\mathbb{C}} = (r, 0). \end{aligned}$$

This is a ring homomorphism.

Example 5.9.13. Let $\mathbb{K}$ be a commutative ring.

Let $\mathbb{K}^{2\leq 2}$ be the ring of upper-triangular 2×2-matrices. (This is a ring, by Proposition 5.8.14.)

Let $\mathbb{K}^{2\geq 2}$ be the ring of lower-triangular 2×2-matrices. (This is a ring, by Proposition 5.8.14.)

(a) Consider the map

$$\begin{aligned} &\mathbb{K}^{2\leq 2} \to \mathbb{K}^{2\geq 2}, \\ &\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ b & c \end{pmatrix}. \end{aligned}$$

In other words, this is the map sending each A to A^T (the transpose of A). Is this a ring homomorphism? No, because $(AB)^T$ is $B^T A^T$, not $A^T B^T$ (in general). This is called a *ring antihomomorphism*. Note that if $\mathbb{K}$ was an arbitrary (not commutative) ring, then $(AB)^T$ would (in general!) equal neither $B^T A^T$ nor $A^T B^T$.

(b) Consider the map

$$\begin{aligned} &\mathbb{K}^{2\leq 2} \to \mathbb{K}^{2\geq 2}, \\ &\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mapsto \begin{pmatrix} c & 0 \\ b & a \end{pmatrix}. \end{aligned}$$

In other words, this is the map that reverses the order of the rows and reverses the order of the columns. You can check that this is a ring homomorphism. This holds even if $\mathbb{K}$ is an arbitrary (not commutative) ring.

Proposition 5.9.14. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism.

(a) We have $f(-a) = -f(a)$ for all $a \in \mathbb{K}$. (In other words, f "preserves additive inverses".)

(b) If $a \in \mathbb{K}$ is invertible, then $f(a) \in \mathbb{L}$ is also invertible, and we have $f\left(a^{-1}\right) = (f(a))^{-1}$. (In other words, f "preserves multiplicative inverses".)

(c) We have $f(a - b) = f(a) - f(b)$ for all $a, b \in \mathbb{K}$.

(d) If the rings $\mathbb{K}$ and $\mathbb{L}$ are commutative, then we have $f\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)}$ for all $a, b \in \mathbb{K}$ for which b is invertible.

(e) We have $f\left(\sum_{s\in S} a_s\right) = \sum_{s\in S} f(a_s)$ whenever S is a finite set and $a_s \in \mathbb{K}$ for all $s \in S$.

(f) We have $f(a_1 a_2 \cdots a_k) = f(a_1) f(a_2) \cdots f(a_k)$ whenever $a_1, a_2, \ldots, a_k \in \mathbb{K}$.

(g) If the rings $\mathbb{K}$ and $\mathbb{L}$ are commutative, then $f\left(\prod_{s\in S} a_s\right) = \prod_{s\in S} f(a_s)$ whenever S is a finite set and $a_s \in \mathbb{K}$ for all $s \in S$.

(h) We have $f(a^n) = (f(a))^n$ for each $a \in \mathbb{K}$ and each $n \in \mathbb{N}$.

(i) We have $f(na) = nf(a)$ for each $a \in \mathbb{K}$ and each $n \in \mathbb{Z}$.

The composition of two ring homomorphisms is again a ring homomorphism, as the following proposition shows:

Proposition 5.9.15. Let $\mathbb{K}$, $\mathbb{L}$ and $\mathbb{M}$ be three rings. Let $f : \mathbb{K} \to \mathbb{L}$ and $g : \mathbb{L} \to \mathbb{M}$ be two ring homomorphisms. Then, the composition $g \circ f : \mathbb{K} \to \mathbb{M}$ is also a ring homomorphism.

5.10. Ring isomorphisms

Definition 5.10.1. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a map. Then, f is called a *ring isomorphism* if and only if f is invertible (i.e., bijective) and both f and f^{-1} are ring homomorphisms.

Example 5.10.2. Let $\mathbb{K}$ be a ring. The identity map $\mathrm{id} : \mathbb{K} \to \mathbb{K}$ is a ring isomorphism.

Example 5.10.3. Let $\mathbb{K}$ be a ring. Let $n \in \mathbb{N}$. Consider the map

$$\mathbf{d}_n : \underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ times}} \to \{\text{diagonal } n \times n\text{-matrices over } \mathbb{K}\},$$

$$(d_1, d_2, \ldots, d_n) \mapsto \begin{pmatrix} d_1 & 0 & 0 & \cdots & 0 \\ 0 & d_2 & 0 & \cdots & 0 \\ 0 & 0 & d_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & d_n \end{pmatrix}.$$

Note that both $\underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ times}}$ and $\{\text{diagonal } n \times n\text{-matrices over } \mathbb{K}\}$ are rings (the former by Definition 5.7.3; the latter by Proposition 5.8.14 **(c)**).

The map $\mathbf{d}_n$ is invertible. I claim that furthermore, $\mathbf{d}_n$ is a ring isomorphism. This is easiest to check using Proposition 5.10.5 further below. Note that this claim is a rigorous version of our earlier informal statement that the ring formed by the diagonal $n \times n$-matrices is just $\underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ times}}$ in disguise. The isomorphism $\mathbf{d}_n$ is responsible for the disguise!

Example 5.10.4. The map from $\mathbb{K}^{2\leq 2}$ to $\mathbb{K}^{2\geq 2}$ introduced in Example 5.9.13 **(b)** is a ring isomorphism. Its inverse is the map

$$\begin{aligned}\mathbb{K}^{2\geq 2} &\to \mathbb{K}^{2\leq 2},\\ \begin{pmatrix} c & 0 \\ b & a \end{pmatrix} &\mapsto \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}.\end{aligned}$$

Proposition 5.10.5. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be an invertible ring homomorphism. Then, f is a ring isomorphism.

Example 5.10.6. Recall the ring $\mathbb{Z}'$ introduced in Section 5.2. It is the **set** $\mathbb{Z}$, endowed with the usual addition $+$ and the unusual multiplication $\widetilde{\times}$ and the elements $0_{\mathbb{Z}'} = 0$ and $1_{\mathbb{Z}'} = -1$.

As we have suggested back in that section, this ring $\mathbb{Z}'$ is simply a relabelled version of $\mathbb{Z}$. We now have the proper language for this: The map

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

is a ring isomorphism. This can easily be checked using Proposition 5.10.5, since this map φ is invertible (actually, $\varphi \circ \varphi = \mathrm{id}$), and since φ is a ring homomorphism (because of (46), (47), (48) and (49)).

Example 5.10.7. Let m and n be two coprime positive integers. Then, $(\mathbb{Z}/m) \times (\mathbb{Z}/n)$ is a ring (according to Definition 5.7.3). Theorem 3.6.2 says that the map

$$\begin{aligned}S_{m,n} : \mathbb{Z}/(mn) &\to (\mathbb{Z}/m) \times (\mathbb{Z}/n),\\ \alpha &\mapsto (\pi_{mn,m}(\alpha), \pi_{mn,n}(\alpha))\end{aligned}$$

is well-defined and is a bijection. This map $S_{m,n}$ is furthermore a ring isomorphism.

Note one more simple general fact:

Proposition 5.10.8. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring isomorphism. Then, $f^{-1} : \mathbb{L} \to \mathbb{K}$ is also a ring isomorphism.

Let me attempt to discuss the use of ring isomorphisms; unfortunately, I will have to be vague at this point. Ring homomorphisms allow us to transfer some things from one ring into another. For example, if $f : \mathbb{K} \to \mathbb{L}$ is a ring homomorphism from a ring $\mathbb{K}$ to a ring $\mathbb{L}$, then f sends any invertible element of $\mathbb{K}$ to an invertible element of $\mathbb{L}$ (by Proposition 5.9.14 **(b)**). However, they are generally only "one-way roads". For instance, if $f : \mathbb{K} \to \mathbb{L}$ is a ring homomorphism from a ring $\mathbb{K}$ to a ring $\mathbb{L}$, and if $a \in \mathbb{K}$ is such that $f(a) \in \mathbb{L}$ is invertible, then a may and

may not be invertible. A ring homomorphism from a ring $\mathbb{K}$ to a ring $\mathbb{L}$ does not determine either ring in terms of the other. You can have homomorphisms between completely different rings, such as from $\mathbb{Z}$ to the zero ring, or from $\mathbb{Z}$ to $\mathbb{C}$.

On the other hand, ring isomorphisms let us go "back and forth" between the rings they connect; if we have a ring isomorphism $f : \mathbb{K} \to \mathbb{L}$, we can regard $\mathbb{L}$ as being "the same ring as $\mathbb{K}$, with its elements renamed". (The isomorphism f does the renaming: you should think of each $a \in \mathbb{K}$ being renamed as $f(a)$.)

Thus, when you have a ring isomorphism $f : \mathbb{K} \to \mathbb{L}$, you can take any "intrinsic" property[73] of $\mathbb{K}$ and obtain the corresponding property of $\mathbb{L}$, and vice versa. Here is an example:

Proposition 5.10.9. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring isomorphism.

(a) If $\mathbb{K}$ is commutative, then $\mathbb{L}$ is commutative.

(b) If $0 \neq 1$ in $\mathbb{K}$, then $0 \neq 1$ in $\mathbb{L}$.

(c) If $\mathbb{K}$ is a skew field, then $\mathbb{L}$ is a skew field.

(d) If $\mathbb{K}$ is a field, then $\mathbb{L}$ is a field.

The idea of the above proof (and of many similar proofs, which we will omit) is that if you have a ring isomorphism $f : \mathbb{K} \to \mathbb{L}$, you can transport any equality or element from $\mathbb{K}$ to $\mathbb{L}$ (via f) or vice versa (via f^{-1}); and each time, the ring operations ($+$, $-$, $\cdot$, $\sum$, 0, 1) do not get damaged on the way (since f and f^{-1} are ring homomorphisms).

Here is another example of this sort of reasoning:

Proposition 5.10.10. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring isomorphism. Then:

(a) We have

$$|\{\text{invertible elements of } \mathbb{K}\}| = |\{\text{invertible elements of } \mathbb{L}\}|.$$

(b) We have

$$|\{\text{idempotent elements of } \mathbb{K}\}| = |\{\text{idempotent elements of } \mathbb{L}\}|.$$

Here, an element a of a ring $\mathbb{K}$ is said to be *idempotent* if $a^2 = a$.

Now let us see some applications of ring isomorphisms.

[73] What do we mean by "intrinsic"? Roughly speaking, an *intrinsic* property of a ring is a property that can be stated entirely in terms of its structure (i.e., its ground set and its operations $+$ and $\cdot$ and its elements 0 and 1), without referring to outside objects. For instance, "every element a of the ring satisfies $a^3 = a^2$" is an intrinsic property (since $a^3 = aaa$ and $a^2 = aa$ are defined purely in terms of the operation $\cdot$), and "the ring has two nonzero elements a and b such that $ab = 0$" is an intrinsic property as well (provided that "nonzero" and "0" refer to the zero of the ring, rather than the number 0), but "the ring contains the number $\sqrt[3]{2}$" is not an intrinsic property (since it refers to an outside object – namely, the number $\sqrt[3]{2}$).

Recall that we proved Theorem 2.14.4 using the Chinese Remainder Theorem in Section 3.6. Let us redo this proof in a shorter way:

The next exercise offers another example of the same strategy:

Exercise 5.10.1. Let p and q be two distinct primes. How many idempotent elements does the ring $\mathbb{Z}/(pq)$ have?

Example 5.10.11. Let A be the 2×2-matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \in \mathbb{Z}^{2\times 2}$.

On midterm #2 exercise 5, you have encountered the ring

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

This is a subring of the matrix ring $\mathbb{Z}^{2\times 2}$.

On homework set #5 exercise 5, you have encountered the ring

$$\mathbb{Z}[\phi] = \{a + b\phi \mid a, b \in \mathbb{Z}\},$$

where $\phi = \dfrac{1+\sqrt{5}}{2} = 1.618\ldots$ is the golden ratio. This is a subring of $\mathbb{R}$.

I claim that there is an isomorphism from $\mathbb{Z}[\phi]$ to $\mathcal{F}$. Namely, the map

$$\begin{aligned} f : \mathbb{Z}[\phi] &\to \mathcal{F}, \\ a + b\phi &\mapsto bA + aI_2 = \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \end{aligned}$$

is a ring isomorphism (but not the only one!).

(Check this by hand.)

Definition 5.10.12. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. We say that the rings $\mathbb{K}$ and $\mathbb{L}$ are *isomorphic* if there exists a ring isomorphism $f : \mathbb{K} \to \mathbb{L}$.

We write "$\mathbb{K} \cong \mathbb{L}$ (as rings)" to say that the rings $\mathbb{K}$ and $\mathbb{L}$ are isomorphic.

Example 5.10.13. Let $\mathbb{K}$ be any ring, and let $\mathbb{M}$ be the zero ring $\{0\}$. In Example 5.9.6, we saw that the map

$$\mathbb{K} \to \mathbb{M}, \qquad a \mapsto 0$$

is a ring homomorphism. This homomorphism is a ring isomorphism if and only if the ring $\mathbb{K}$ is trivial (i.e., has only one element). Thus, each trivial ring is isomorphic to the zero ring.

5.11. Freshman's Dream

Let us now prove a property of p-th powers in rings. At this point, this property appears to be a mere curiosity, but it will come useful later (in proving Theorem 2.17.20).

Theorem 5.11.1. Let p be a prime. Let $\mathbb{K}$ be a ring such that $p \cdot 1_{\mathbb{K}} = 0$. Let $a, b \in \mathbb{K}$ be such that $ab = ba$. Then,

$$(a+b)^p = a^p + b^p.$$

Theorem 5.11.1 is often called "Freshman's Dream" (in writing) or "Idiot's Binomial Formula" (colloquially).

Example 5.11.2. Let p be a prime.

(a) The simplest example of a ring $\mathbb{K}$ in which $p \cdot 1_{\mathbb{K}} = 0$ (apart from the zero ring) is the ring $\mathbb{Z}/p$. Unfortunately, this is too simple to make a good example for Theorem 5.11.1. Indeed, if $\mathbb{K} = \mathbb{Z}/p$, then any $\alpha \in \mathbb{K}$ satisfies $\alpha^p = \alpha$ (because we can write α as $[a]_p$ for some $a \in \mathbb{Z}$, and then apply Theorem 2.15.1 **(b)** to this a). Thus, as long as we are staying in $\mathbb{K} = \mathbb{Z}/p$, the equality $(a+b)^p = a^p + b^p$ claimed by Theorem 5.11.1 boils down to $a + b = a + b$ (since $(a+b)^p = a + b$ and $a^p = a$ and $b^p = b$).

(b) In Section 5.6, we have taken a prime $p > 2$, and constructed a finite field $\mathbb{K}'_\eta$ of size p^2 (by picking a non-square $\eta \in \mathbb{Z}/p$ and performing the construction in Definition 5.6.11). This field satisfies $p \cdot 1_{\mathbb{K}'_\eta} = 0$, so we can apply Theorem 5.11.1 to it as well. This time, $\alpha^p = \alpha$ will no longer hold for all α in the field, so the result we get will not be obvious.

(c) Here is another example. Let $n \in \mathbb{N}$, and let $\mathbb{K}$ be the matrix ring $(\mathbb{Z}/p)^{n \times n}$. This matrix ring $\mathbb{K}$ satisfies $p \cdot 1_{\mathbb{K}} = 0$ (since scaling is defined entrywise on matrices). Thus, Theorem 5.11.1 yields that any $a, b \in \mathbb{K}$ satisfying $ab = ba$ must satisfy $(a+b)^p = a^p + b^p$. Of course, not every two matrices $a, b \in \mathbb{K}$ satisfy $ab = ba$, but there are many matrices that do.

A particularly striking situation is the following: Assume that $n \leq p$, and let $N \in \mathbb{K}$ be a strictly lower-triangular $n \times n$-matrix. For example, if $n = 3$, then N has the form $\begin{pmatrix} 0 & 0 & 0 \\ u & 0 & 0 \\ v & w & 0 \end{pmatrix}$. Then, I claim that

$$(I_n + N)^p = I_n. \tag{71}$$

To prove this, we observe that $I_n \cdot N = N = N \cdot I_n$. Hence, Theorem 5.11.1 can be applied to $a = I_n$ and $b = N$. As a result, we obtain $(I_n + N)^p = I_n^p + N^p$. But N is a strictly lower-triangular $n \times n$-matrix, and therefore satisfies $N^n = 0_{n \times n}$

(by [Grinbe18, Corollary 3.78]), and therefore

$$N^p = \underbrace{N^n}_{=0_{n\times n}} N^{p-n} \qquad (\text{since } n \leq p)$$
$$= 0_{n\times n} N^{p-n} = 0_{n\times n}.$$

Furthermore, $I_n^p = I_n$ (since I_n is the unity of the ring $\mathbb{K}$). Hence, $(I_n + N)^p = \underbrace{I_n^p}_{=I_n} + \underbrace{N^p}_{=0_{n\times n}} = I_n + 0_{n\times n} = I_n$. This proves (71).

We note that Theorem 5.11.1 would be false if p wasn't assumed to be prime. For example, it would be false for $p = 4$ (a simple counterexample being $\mathbb{K} = \mathbb{Z}/4$, $a = 1$ and $b = 1$).

As a consequence of Theorem 5.11.1, we obtain some unexpected ring homomorphisms:

Corollary 5.11.3. Let p be a prime. Let $\mathbb{K}$ be a commutative ring such that $p \cdot 1_{\mathbb{K}} = 0$. Let F be the map

$$\mathbb{K} \to \mathbb{K}, \qquad a \mapsto a^p.$$

Then, F is a ring homomorphism.

The ring homomorphism F in Corollary 5.11.3 is called the *Frobenius endomorphism*[74] of $\mathbb{K}$.

6. Linear algebra over commutative rings

We shall now continue studying rings, but slowly shift our focus: So far, we have been studying rings themselves, but now we are going to move towards structures "over" rings, such as matrices and $\mathbb{K}$-modules (a generalization of vector spaces). The rings will no longer be the place where everything happens, but rather they will "act" on our structures in the way scalars act on vectors in linear algebra.

6.1. An overview of matrix algebra over fields

Next I shall give a quick review of matrix algebra adapted to the situation in which the entries of the vectors belong to an arbitrary field. This review will be quick and terse, but can be skipped, since the rest of this course will not depend on it. It does, however, provide context and examples for several constructions we will do further on.

[74] The word "endomorphism" means "homomorphism of some object (here, a ring) to itself", i.e., "homomorphism whose domain and codomain are the same".

I assume you have seen some basic matrix algebra: Gaussian elimination, ranks of matrices, inverses of matrices, determinants, etc. (If not, see [Heffer17].)

Usually, these things are done for matrices over $\mathbb{R}$ or $\mathbb{C}$. But we can try doing the same with matrices over an arbitrary commutative ring $\mathbb{K}$.

6.1.1. Matrices over fields

Let us first study the situation when $\mathbb{K}$ is a field.

Example: Let $\mathbb{K} = \mathbb{Z}/3$, and let $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in \mathbb{K}^{3\times 3}$. (Here, of course, "0" and "1" mean $[0]_3$ and $[1]_3$.) Let $b = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in \mathbb{K}^{3\times 1}$. We want to find a column vector $x \in \mathbb{K}^{3\times 1}$ such that $Ax = b$. This means, explicitly, to find $x_1, x_2, x_3 \in \mathbb{K}$ such that

$$\begin{cases} 0x_1 + 1x_2 + 1x_3 = 1; \\ 1x_1 + 0x_2 + 1x_3 = 1; \\ 1x_1 + 1x_2 + 0x_3 = 1. \end{cases}$$

Can we do this? Well, we can try: Augment the matrix A with the column b, obtaining the augmented matrix

$$(A \mid b) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Now, we shall transform this matrix into reduced row echelon form (see [Strick13, §5] or [Heffer17, Chapter One, §III][75]) by a series of row operations (this is called *Gauss–Jordan reduction* in [Heffer17, Chapter One, §III], and also appears as Method

[75]The reduced row echelon form is called "reduced echelon form" in [Heffer17].

6.3 in [Strick13]):

$$(A \mid b) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \overset{\text{swap row 2 with row 1}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

$$\overset{\text{subtract row 1 from row 3}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 2 & 0 \end{pmatrix} \qquad (\text{since } -1 = 2 \text{ in } \mathbb{Z}/3)$$

$$\overset{\text{subtract row 2 from row 3}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

(this is a row echelon form, but not a reduced one)

$$\overset{\text{subtract row 3 from row 1}}{\mapsto} \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix}$$

$$\overset{\text{subtract row 3 from row 2}}{\mapsto} \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

So for any vector $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{K}^{3\times 1}$, we have the following chain of equivalences:

$$\begin{aligned}
&(Ax = b) \\
&\iff (Ax - b = 0_{3\times 1}) \\
&\iff \left((A \mid b) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ -1 \end{pmatrix} = 0_{3\times 1} \right) \qquad \left(\text{since } Ax - b = (A \mid b) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ -1 \end{pmatrix} \right) \\
&\iff \left(\begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ -1 \end{pmatrix} = 0_{3\times 1} \right) \\
&\qquad \left(\text{since } (A \mid b) \mapsto \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 2 \end{pmatrix} \text{ by a sequence of row operations} \right) \\
&\iff \left(\begin{pmatrix} x_1 - 2 \\ x_2 - 2 \\ x_3 - 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right) \iff \left(\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix} \right).
\end{aligned}$$

So our linear system has the unique solution

$$x = \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix}.$$

Next, let us try doing the same for $\mathbb{K} = \mathbb{Z}/2$, with the "same" matrix. (It will not be literally the same matrix, of course, since 0 and 1 will now mean $[0]_2$ and $[1]_2$.)

Thus, let $\mathbb{K} = \mathbb{Z}/2$, and let $A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \in \mathbb{K}^{3\times 3}$. (Here, of course, "0" and "1" mean $[0]_2$ and $[1]_2$.) Let $b = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in \mathbb{K}^{3\times 1}$. We want to find a column vector $x \in \mathbb{K}^{3\times 1}$ such that $Ax = b$. This means, explicitly, to find $x_1, x_2, x_3 \in \mathbb{K}$ such that

$$\begin{cases} 0x_1 + 1x_2 + 1x_3 = 1; \\ 1x_1 + 0x_2 + 1x_3 = 1; \\ 1x_1 + 1x_2 + 0x_3 = 1. \end{cases}$$

Can we do this? We can try as before: Augment the matrix A with the column b, obtaining

$$(A \mid b) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}.$$

Now, we shall transform this matrix into reduced row echelon form by a series of row operations:

$$(A \mid b) = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix} \overset{\text{swap row 2 with row 1}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{pmatrix}$$

$$\overset{\text{subtract row 1 from row 3}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad (\text{since } -1 = 1 \text{ in } \mathbb{Z}/2)$$

$$\overset{\text{subtract row 2 from row 3}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\overset{\text{subtract row 3 from row 1}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\overset{\text{subtract row 3 from row 2}}{\mapsto} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

So for any vector $x = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \in \mathbb{K}^{3\times 1}$, we have the following chain of equivalences:

$$\begin{aligned}
&(Ax = b) \\
\iff &(Ax - b = 0_{3\times 1}) \\
\iff &\left((A \mid b) \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ -1 \end{pmatrix} = 0_{3\times 1} \right) \\
\iff &\left(\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ -1 \end{pmatrix} = 0_{3\times 1} \right) \\
\iff &\left(\begin{pmatrix} x_1 + x_3 \\ x_2 + x_3 \\ -1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \right) \iff (\text{false})
\end{aligned}$$

(since $-1 \neq 0$ in $\mathbb{K}$). So our linear system has no solution.

By the way, you could have easily seen this from the system itself:

$$\begin{cases} 0x_1 + 1x_2 + 1x_3 = 1; \\ 1x_1 + 0x_2 + 1x_3 = 1; \\ 1x_1 + 1x_2 + 0x_3 = 1. \end{cases}$$

Adding together the three equations, we get $0 = 1$ (since $1+1 = 0$ and $1+1+1 = 1$ in $\mathbb{Z}/2$), which is absurd. So the system has no solution.

Upshot: We can do linear algebra over any field more or less in the same as we did over real/complex numbers. But the result may depend on the field.

Let me recall a couple theorems from linear algebra that hold (with the same proofs) over any field:

Theorem 6.1.1. Let $\mathbb{K}$ be a field.

(a) Any matrix over $\mathbb{K}$ has a unique reduced row echelon form (abbreviated RREF).

(b) If $A \in \mathbb{K}^{n\times m}$ is any matrix and R is its RREF, then the row space, kernel (= nullspace) and rank of A are equal to those of R. (Here, the *row space*, *kernel* and *rank* of a matrix are defined in the same way as for real/complex matrices.)

(c) If $A \in \mathbb{K}^{n\times m}$ is any matrix, and if $b \in \mathbb{K}^{n\times 1}$ is any column vector, then the equation $Ax = b$ (for an unknown column vector $x \in \mathbb{K}^{m\times 1}$) can be solved using the Gaussian elimination algorithm (e.g., by forming the augmented matrix $(A \mid b)$, then transforming it into RREF, and reading off the solutions from this RREF by the same method as you learned in Linear Algebra).

(d) If $A \in \mathbb{K}^{n \times m}$ is a matrix with $n < m$, then there exists a nonzero $x \in \mathbb{K}^{m \times 1}$ such that $Ax = 0_{n \times 1}$. ("Nonzero" means "distinct from $0_{m \times 1}$"; a nonzero vector can have some zero entries.)

(e) Let $A \in \mathbb{K}^{n \times n}$. Then, the following are equivalent:

- The matrix A is invertible.
- The matrix A is row-equivalent to I_n. (Two matrices are said to be *row-equivalent* if one can be transformed into the other via row operations: swapping rows, scaling rows and adding a multiple of one row to another.)
- The matrix A is column-equivalent to I_n. (The definition of "*column-equivalent*" is the same as of "row-equivalent", but with columns being used instead of rows.)
- The RREF of A is I_n.
- The RREF of A has n pivots.
- The rank of A is n.
- The equation $Ax = 0_{n \times 1}$ (for an unknown $x \in \mathbb{K}^{n \times 1}$) has only the trivial solution (that is, $x = 0_{n \times 1}$).
- For each vector $b \in \mathbb{K}^{n \times 1}$, the equation $Ax = b$ has a solution.
- For each vector $b \in \mathbb{K}^{n \times 1}$, the equation $Ax = b$ has a unique solution.
- The columns of A are linearly independent.
- The rows of A are linearly independent.
- There is a matrix $B \in \mathbb{K}^{n \times n}$ such that $AB = I_n$.
- There is a matrix $B \in \mathbb{K}^{n \times n}$ such that $BA = I_n$.
- We have $\det A \neq 0$. (We will later define determinants.)

(Matrices satisfying these equivalent conditions are called *nonsingular*.)

6.1.2. What if $\mathbb{K}$ is not a field?

Things get weird when $\mathbb{K}$ is not a field. For an example, set $\mathbb{K} = \mathbb{Z}/26$. This is not a field, since 26 is not prime (after all, $26 = 2 \cdot 13$). The ring $\mathbb{Z}/26$ has been used in classical cryptography, since its elements are in bijection with the letters of the (modern) Roman alphabet:

$$0 \mapsto A, \qquad 1 \mapsto B, \qquad 2 \mapsto C, \qquad \ldots.$$

For example, the *Hill cipher* lets you encrypt a word using a 3×3-matrix over $\mathbb{Z}/26$ as a key. The idea is simple: You split the word into 3-letter chunks; you turn each chunk into a column vector in $(\mathbb{Z}/26)^{3\times 1}$; and you multiply each of these columns vectors by your key matrix. To decrypt, you would have to invert the key matrix.

So we want to know how to invert a matrix over $\mathbb{Z}/26$.

If $\mathbb{Z}/26$ was a field, you would know how to do this via Gaussian elimination.

Most of Theorem 6.1.1 collapses when $\mathbb{K}$ is not a field. For example, let $\mathbb{K} = \mathbb{Z}/26$ and

$$A = \begin{pmatrix} 2 & 13 \\ 13 & 20 \end{pmatrix} \in \mathbb{K}^{2\times 2}.$$

(We are abusing notation here: In truth, the entries of A are not the integers $2, 13, 13, 20$ but rather their residue classes $[2]_{26}, [13]_{26}, [13]_{26}, [20]_{26}$. But we shall simply write the integers instead and hope that the reader knows what we mean.)

Is this matrix A invertible?

Let us first try to find the RREF of A. If we would blindly follow the Gaussian elimination algorithm, we would fail very quickly: None of the 4 entries of A has a multiplicative inverse; thus we could not transform any entry of A into 1 by scaling a row of A. But we can try to loosen Gaussian elimination by allowing more strategic row operations: Instead of trying to get a 1 in a pivot position immediately by scaling a row, we can attempt to obtain a 1 by row addition operations. For example, we can transform our matrix A above as follows:

$$\begin{pmatrix} 2 & 13 \\ 13 & 20 \end{pmatrix}$$
$$\overset{\text{subtract 6 times row 1 from row 2}}{\mapsto} \begin{pmatrix} 2 & 13 \\ 1 & 20 \end{pmatrix}$$
$$\overset{\text{swap row 1 with row 2}}{\mapsto} \begin{pmatrix} 1 & 20 \\ 2 & 13 \end{pmatrix}$$
$$\overset{\text{subtract 2 times row 1 from row 2}}{\mapsto} \begin{pmatrix} 1 & 20 \\ 0 & 25 \end{pmatrix}$$
$$\overset{\text{scale row 2 by } -1}{\mapsto} \begin{pmatrix} 1 & 20 \\ 0 & 1 \end{pmatrix}$$
$$\overset{\text{subtract 20 times row 2 from row 1}}{\mapsto} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

So our matrix A does have a RREF (namely, I_2), and even is invertible! (We can find an inverse of A by computing an RREF of the block matrix $(A \mid I_2)$; see, e.g., [Strick13, Method 11.11] for this procedure.)

What exactly was the method behind our above row-reduction procedure? Let

us see how the first column has been transformed:

$$\begin{pmatrix} 2 \\ 13 \end{pmatrix} \overset{\text{subtract 6 times row 1 from row 2}}{\mapsto} \begin{pmatrix} 2 \\ 1 \end{pmatrix} \overset{\text{swap row 1 with row 2}}{\mapsto} \begin{pmatrix} 1 \\ 2 \end{pmatrix}$$
$$\overset{\text{subtract 2 times row 1 from row 2}}{\mapsto} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

So what we did was progressively making the entries of the first column smaller by subtracting a multiple of the first entry from the second entry (and swapping the two entries, in order to move the smaller entry into the first position). This is exactly the Euclidean algorithm! (Or, rather, it would be the Euclidean algorithm if we had used honest integers instead of residue classes in $\mathbb{Z}/26$.)

What happens in general? In general, when $\mathbb{K} = \mathbb{Z}/n$, the Gaussian elimination algorithm as defined in linear algebra does not always work. Nevertheless, a variant of it works, in which you do not directly scale rows to turn entries into 1, but instead "minimize" the whole column using the Euclidean algorithm as we did with our matrix A above. You will not always be able to get 1's in pivot positions, because the gcd (which the Euclidean algorithm computes) may not be 1; thus, the result will not always be an RREF in the classical sense, but rather something loosely resembling it.

For details, look up the *Smith normal form* (e.g., in [Elman18, §113]). Note that for $n = 0$, we have $\mathbb{Z}/n \cong \mathbb{Z}$ (as rings), so this applies to matrices with integer entries.

6.1.3. Review of basic notions from linear algebra

Convention 6.1.2. For the rest of this section, we fix a field $\mathbb{K}$. The elements of $\mathbb{K}$ will be referred to as *scalars*.

In the linear algebra you have seen before, the scalars are usually real numbers (i.e., we have $\mathbb{K} = \mathbb{R}$), but much of the theory works in the same way for every field.

Definition 6.1.3. Let $n \in \mathbb{N}$. Recall that $\mathbb{K}^{1\times n}$ is the set of all row vectors of size n.

A *subspace* of $\mathbb{K}^{1\times n}$ means a subset $S \subseteq \mathbb{K}^{1\times n}$ satisfying the following axioms:

- **(a)** We have $0_{1\times n} \in S$.
- **(b)** If $a, b \in S$, then $a + b \in S$.
- **(c)** If $a \in S$ and $\lambda \in \mathbb{K}$, then $\lambda a \in S$.

In other words, a subspace of $\mathbb{K}^{1\times n}$ is a subset of $\mathbb{K}^{1\times n}$ that contains the zero vector and is closed under addition and scaling.

Subspaces are often called *vector subspaces*.

A similar definition defines subspaces of $\mathbb{K}^{n\times 1}$ (column vectors).

There is a more general version of this definition, which extends it to subspaces of arbitrary vector spaces (see Definition 6.7.3).

Definition 6.1.4. Let $n \in \mathbb{N}$. Let $v_1, v_2, \ldots, v_k$ be some row vectors in $\mathbb{K}^{1\times n}$.

(a) A *linear combination* of $v_1, v_2, \ldots, v_k$ means a row vector of the form

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k, \qquad \text{with } \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}.$$

(b) The *span* of $v_1, v_2, \ldots, v_k$ is defined to be the subset

$$\begin{aligned}&\{\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k \mid \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}\} \\ &= \{\text{linear combinations of } v_1, v_2, \ldots, v_k\}\end{aligned}$$

of $\mathbb{K}^{1\times n}$. This span is a subspace of $\mathbb{K}^{1\times n}$. (This is easy to check.)

(c) The vectors $v_1, v_2, \ldots, v_k$ are said to be *linearly independent* if the only k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k = 0_{1\times n}$ is $\left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$.

(d) Let U be a subspace of $\mathbb{K}^{1\times n}$. We say that $v_1, v_2, \ldots, v_k$ form a *basis* of U (or, more formally, $(v_1, v_2, \ldots, v_k)$ is a basis of U) if and only if the vectors $v_1, v_2, \ldots, v_k$ are linearly independent and their span is U.

(e) Let U be a subspace of $\mathbb{K}^{1\times n}$. We say that the list $(v_1, v_2, \ldots, v_k)$ *spans* U if and only if the span of $v_1, v_2, \ldots, v_k$ is U. (More informally, instead of saying "the list $(v_1, v_2, \ldots, v_k)$ *spans* U", we can say "the vectors $v_1, v_2, \ldots, v_k$ *span* U"; of course, this is not the same as saying that each of these k vectors on its own spans U.)

All the terminology we have just introduced depends on $\mathbb{K}$. Whenever the field $\mathbb{K}$ is not clear from the context, you can insert it into this terminology to make it unambiguous: e.g., say "$\mathbb{K}$-linear combination" instead of "linear combination", and "$\mathbb{K}$-span" instead of "span".

Theorem 6.1.5. Let $n \in \mathbb{N}$. Let U be a subspace of $\mathbb{K}^{1\times n}$.

(a) There exists at least one basis of U.

(b) Any two bases of U have the same size (= number of vectors).

(c) Given k linearly independent vectors in U, and given ℓ vectors that span U, we always have $k \leq \ell$.

(d) Any list of k linearly independent vectors in U can be extended to a basis of U.

(e) Any list of ℓ vectors that span U can be shrunk to a basis of U (i.e., we can remove some vectors from this list to get a basis of U).

Again, the same holds for column vectors.

Definition 6.1.6. Let $n \in \mathbb{N}$. Let U be a subspace of $\mathbb{K}^{1\times n}$.

The *dimension* of U is defined to be the size of a basis of U. (Parts **(a)** and **(b)** of Theorem 6.1.5 show that this is indeed well-defined.) The dimension of U is denoted by $\dim U$.

Proposition 6.1.7. Let $n \in \mathbb{N}$. Let U and V be two subspaces of $\mathbb{K}^{1\times n}$ such that $U \subseteq V$.

(a) We have $\dim U \leq \dim V$.

(b) If $\dim U = \dim V$, then $U = V$.

Now, let us connect this with matrices:

Definition 6.1.8. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n\times m}$ be a matrix.

(a) The *row space* of A is defined to be the span of the rows of A. This is a subspace of $\mathbb{K}^{1\times m}$, and is called $\operatorname{Row} A$.

(b) The *column space* of A is defined to be the span of the columns of A. This is a subspace of $\mathbb{K}^{n\times 1}$, and is called $\operatorname{Col} A$.

Theorem 6.1.9. Let $A \in \mathbb{K}^{n\times m}$ be a matrix. Then, $\dim \operatorname{Row} A = \dim \operatorname{Col} A$.

Definition 6.1.10. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n\times m}$ be a matrix. Theorem 6.1.9 shows that $\dim \operatorname{Row} A = \dim \operatorname{Col} A$. This number $\dim \operatorname{Row} A = \dim \operatorname{Col} A$ is called the *rank* of A and is denoted by $\operatorname{rank} A$.

The following is easy to see:

Proposition 6.1.11. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n\times m}$ be a matrix. Then, $\operatorname{rank} A$ is an integer between 0 and $\min\{n, m\}$.

So we have seen that a matrix gives rise to two subspaces: its row space and its column space. But there is more:

Definition 6.1.12. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n\times m}$ be a matrix.

(a) The *kernel* (or *nullspace*) of A is defined to be the set of all column vectors $v \in \mathbb{K}^{m\times 1}$ such that $Av = 0_{n\times 1}$. This is a subspace of $\mathbb{K}^{m\times 1}$, and is called $\operatorname{Ker} A$.

(b) The *left kernel* (or *left nullspace*) of A is defined to be the set of all row vectors $w \in \mathbb{K}^{1\times n}$ such that $wA = 0_{1\times m}$. This is a subspace of $\mathbb{K}^{1\times n}$.

Altogether, we have thus found four subspaces coming out of a matrix A. These are the famous "four fundamental subspaces" (in Gilbert Strang's terminology). One result that connects two of them is the following fact, known as the *rank-nullity theorem*:

Theorem 6.1.13. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be a matrix. Then,

$$\operatorname{rank} A + \dim \operatorname{Ker} A = m.$$

Note that the number $\dim \operatorname{Ker} A$ is known as the *nullity* of a matrix A.

6.1.4. Linear algebra over $\mathbb{Z}/2$: "button madness" / "lights out"

We now discuss an old puzzle, which is known as "button madness" or "lights out" (more precisely, these are two slightly different variants of the same puzzle). You can try it out on

`https://bz.var.ru/comp/web/js/floor.html`

(see also `https://www.win.tue.nl/~aeb/ca/madness/madrect.html` for a list of mathematical sources on this puzzle).

One version of this puzzle gives you 16 lamps arranged into a 4×4-grid. Each lamp comes with a lightswitch; but flipping this lightswitch toggles not just this lamp, but also its four adjacent lamps (or three or two adjacent lamps, if the switch you have flipped is at the border of the grid). For example, if your grid looks like this:

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

(where an entry 1 means a lamp turned on, and an entry 0 means a lamp turned off), and you flip the lightswitch in cell $(2,3)$ (that is, the third cell from the left in the second row from the top), then you obtain the grid

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

.

(A total of 5 lamps have changed their state: three have been turned off, and two have been turned on.) If you then flip the lightswitch in cell $(1,3)$ of this new grid, then you obtain the grid

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

.

At the beginning, all lamps are turned off. Your goal is to achieve the opposite state (i.e., all lamps being on at the same time) by flipping a sequence of lightswitches. Is this possible, and how? (In some versions of this puzzle – such as the "lights out" version – it's exactly the other way round: The lights are all on initially, and you must turn them all off. Of course, this makes no difference to the solution.)

In some versions of this puzzle, the grid is "toroidal", in the sense that it is understood to wrap around – for example, the cells $(1,4)$ and $(1,1)$ are considered to be adjacent, and so are the cells $(4,1)$ and $(1,1)$. We shall not consider this case here, but it can be solved by the same method.

Of course, you can play the same game on larger grids, triangular grids, etc.. But in order to get a grip on how to solve such a puzzle, we shall first analyze a much simpler version: the "1-dimensional version" of the puzzle.

Here is this "1-dimensional version": We have 4 lamps in a row (numbered $1,2,3,4$), each equipped with a lightswitch. The lightswitch at lamp i toggles lamp i, lamp $i-1$ (if it exists) and lamp $i+1$ (if it exists). Initially, all 4 lamps are off. Can we turn them all on by flipping a sequence of lightswitches?

Yes, of course: we just have to flip the lightswitches at lamps 1 and 4. But let us pretend that we aren't that smart, and instead try to solve the puzzle systematically.

We model the states of our lamps by a row vector in $(\mathbb{Z}/2)^{1\times 4}$. We write a row vector $\begin{pmatrix} a_1 & a_2 & \cdots & a_n \end{pmatrix}$ as $(a_1, a_2, \ldots, a_n)$.

More precisely, we model each state by the row vector $(a_1, a_2, a_3, a_4) \in (\mathbb{Z}/2)^{1\times 4}$, where

$$a_i = \begin{cases} [0]_2, & \text{if lamp } i \text{ is off;} \\ [1]_2, & \text{if lamp } i \text{ is on} \end{cases} = \underbrace{\left[\underbrace{[\text{lamp } i \text{ is on}]}_{\text{Iverson bracket}} \right]_2}_{\text{residue class}}.$$

We shall write 0 and 1 for $[0]_2$ and $[1]_2$ throughout this subsection (except in Proposition 6.1.14), so we can rewrite this as

$$a_i = \begin{cases} 0, & \text{if lamp } i \text{ is off;} \\ 1, & \text{if lamp } i \text{ is on} \end{cases} = \underbrace{[\text{lamp } i \text{ is on}]}_{\text{Iverson bracket}},$$

but keep in mind that these values are understood to be in $\mathbb{Z}/2$.

The initial state is $(0,0,0,0)$. The final state that we want to achieve is $(1,1,1,1)$. Flipping a lightswitch corresponds to adding a certain row vector to our state. Namely:

- Flipping lightswitch 1 means adding $(1,1,0,0)$.
- Flipping lightswitch 2 means adding $(1,1,1,0)$.
- Flipping lightswitch 3 means adding $(0,1,1,1)$.

- Flipping lightswitch 4 means adding $(0,0,1,1)$.

Thus, flipping a lightswitch means adding the corresponding row of the matrix

$$A := \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \in (\mathbb{Z}/2)^{4\times 4}$$

to our state. The reachable states are thus exactly the elements of Row A, the row space of A.

Hence, our goal is to show that $(1,1,1,1) \in \operatorname{Row} A$.

This is quite easy for the concrete matrix A above (just notice that $(1,1,1,1)$ is the sum of the 1-st and 4-th rows of A); but let us try a theoretical argument. It will rely on the following general fact:

Proposition 6.1.14. Let $n, m \in \mathbb{N}$. Let $\mathbb{K}$ be any field. Let $A \in \mathbb{K}^{n\times m}$ and $b \in \mathbb{K}^{1\times m}$. Assume the following:

> *Assumption 1:* If $c \in \mathbb{K}^{m\times 1}$ satisfies $Ac = 0$, then $bc = 0$. (Here, of course, the "0" in "$Ac = 0$" means $0_{n\times 1}$.)

Then, $b \in \operatorname{Row} A$.

Over the field $\mathbb{Z}/2$, this fact has the following consequence:

Corollary 6.1.15. Let $n \in \mathbb{N}$. Let $A \in (\mathbb{Z}/2)^{n\times n}$ be a symmetric matrix. ("*Symmetric*" means that the (i,j)-th entry of A equals the (j,i)-th entry of A for all i and j. In other words, it means that $A^T = A$.)

Let d be the diagonal of A, written as a row vector. (In other words, let $d = (a_{1,1}, a_{2,2}, \ldots, a_{n,n})$, where $a_{i,j}$ is the (i,j)-th entry of A.)

Then, $d \in \operatorname{Row} A$.

Note that Corollary 6.1.15 brutally fails over fields different from $\mathbb{Z}/2$. For example, if we allow A to be a matrix in $\mathbb{Z}^{n\times n}$ instead, then $A = \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$ is symmetric but its diagonal $d = (1,1)$ does not belong to Row A.

Now, why can the "lights out" puzzle be solved?

We want to prove that $(1,1,1,1) \in \operatorname{Row} A$ for our matrix $A \in (\mathbb{Z}/2)^{4\times 4}$.

This follows from Corollary 6.1.15, since the matrix A is symmetric, and since its diagonal is $(1,1,1,1)$.

The same argument works for the "proper" (2-dimensional) "lights out" puzzle; we just have to use row vectors of size 16 (not 4) and 16×16-matrices (not 4×4-matrices). More generally, the same argument works for any such puzzle on any "grid" as long as:

- each lamp i has a lightswitch which toggles at least lamp i;
- if the lightswitch at lamp i toggles lamp j, then the lightswitch at lamp j toggles lamp i.

These conditions guarantee that the corresponding matrix A will be symmetric and its diagonal will be $(1,1,\ldots,1)$ (and thus we can apply Corollary 6.1.15).

How to find the exact sequence of flips that results in all lights being on? This is tantamount to finding the coefficients of a linear combination of the rows of A that equals $(1,1,\ldots,1)$. This boils down to solving a system of linear equations over $\mathbb{Z}/2$, which can be achieved using Gaussian elimination.

What other states can be achieved by flipping lightswitches? Again, for each specific grid and each specific state, this can be solved by Gaussian elimination; but characterizing the reachable states more explicitly is a hard problem with no unified answer. (See the link above.)

6.1.5. A warning about orthogonality and positivity

I have said above that "more or less" all linear algebra over $\mathbb{R}$ works identically over any field $\mathbb{K}$. There is an exception: Anything that uses positivity will break down over some fields $\mathbb{K}$. Let me briefly telegraph what can go wrong. (Don't worry if the things I am mentioning are not familiar to you.)

One thing that uses positivity is QR-decomposition. And indeed, not every matrix over an arbitrary field has a QR-decomposition.

You can still define dot products and orthogonal complements of subspaces. But it is no longer true that $\mathbb{K}^{n\times 1} = U \oplus U^{\perp}$ for any subspace U of $\mathbb{K}^{n\times 1}$. It can happen that $U \cap U^{\perp} \neq \{0\}$. For example, there are column vectors $v \neq 0_{n\times 1}$ that are orthogonal to themselves with respect to the dot product (that is, $v^T v = 0$).

Example: In $\mathbb{Z}/3$, we have

$$\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}^T \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = (1,1,1) \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = 1\cdot 1 + 1\cdot 1 + 1\cdot 1 = 3 = 0.$$

So the vector $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in (\mathbb{Z}/3)^{3\times 1}$ is orthogonal to itself.

6.2. Matrix algebra vs. coordinate-free linear algebra

There are two common approaches to linear algebra: The first is the study of matrices and column vectors (or row vectors); this is down-to-earth but often clumsy and unenlightening. The second is the study of vector spaces and linear transformations; this is more abstract but more general and often better for conceptual

understanding. The first approach is known as *matrix algebra*; the second is called *coordinate-free linear algebra*.

These two approaches are closely connected: The first can be viewed as a particular case of the second (as the column vectors of a given size n form a vector space, and any matrix defines a linear map between two such vector spaces); the second appears more general but in reality can often be reduced to the first (viz., theorems about vector spaces can often be proven by "picking bases" and representing linear maps by matrices with respect to these bases). Thus, a sufficiently deep course on linear algebra will necessarily survey both of these approaches, and practitioners of the subject will often apply whichever approach fits a problem better.

In the previous section, we have seen how the first approach can be generalized from real or complex matrices to matrices over any field (and, as far as the basics are concerned, over any commutative ring). We shall now try this with the second approach. Over a field, the second approach turns out to work out in pretty much the same way as over the real or complex numbers; however, over a commutative ring, things become a lot more interesting.

6.3. $\mathbb{K}$-modules: the definition

Let us begin by defining the analogue of a vector space: a *module*. Roughly speaking, a module is the same as a vector space, except that it is over a commutative ring instead of a field:

Definition 6.3.1. Let $\mathbb{K}$ be a commutative ring.

A $\mathbb{K}$-*module* means a set M equipped with

- a binary operation $+$ on M (called "*addition*", and not to be confused with the addition $+_{\mathbb{K}}$ of $\mathbb{K}$),
- a map $\cdot : \mathbb{K} \times M \to M$ (called "*scaling*", and not to be confused with the multiplication $\cdot_{\mathbb{K}}$ of $\mathbb{K}$), and
- an element $0_M \in M$ (called "*zero vector*" or "*zero*", and not to be confused with the zero of $\mathbb{K}$)

satisfying the following axioms:

- **(a)** We have $a + b = b + a$ for all $a, b \in M$.
- **(b)** We have $a + (b + c) = (a + b) + c$ for all $a, b, c \in M$.
- **(c)** We have $a + 0_M = 0_M + a = a$ for all $a \in M$.
- **(d)** Each $a \in M$ has an additive inverse (i.e., there is an $a' \in M$ such that $a + a' = a' + a = 0_M$).

- **(e)** We have $\lambda(a+b) = \lambda a + \lambda b$ for all $\lambda \in \mathbb{K}$ and $a, b \in M$. Here and in the following, we use the notation "λc" (or, equivalently, "$\lambda \cdot c$") for the image of a pair $(\lambda, c) \in \mathbb{K} \times M$ under the "scaling" map $\cdot$ (similarly to how we write ab for the image of a pair $(a, b) \in \mathbb{K} \times \mathbb{K}$ under the "multiplication" map $\cdot$).
- **(f)** We have $(\lambda + \mu) a = \lambda a + \mu a$ for all $\lambda, \mu \in \mathbb{K}$ and $a \in M$.
- **(g)** We have $0a = 0_M$ for all $a \in M$. (Here, the "0" on the left hand side means the zero of $\mathbb{K}$.)
- **(h)** We have $(\lambda\mu) a = \lambda(\mu a)$ for all $\lambda, \mu \in \mathbb{K}$ and $a \in M$.
- **(i)** We have $1a = a$ for all $a \in M$.
- **(j)** We have $\lambda \cdot 0_M = 0_M$ for all $\lambda \in \mathbb{K}$.

These ten axioms are called the *module axioms*.

A $\mathbb{K}$-module is often called a "module over $\mathbb{K}$".

The axioms "$\lambda(a+b) = \lambda a + \lambda b$" and "$(\lambda+\mu) a = \lambda a + \mu a$" are known as the *distributivity laws for modules*. The axiom "$(\lambda\mu) a = \lambda(\mu a)$" is known as the *associativity law for modules*.

Definition 6.3.2. If $\mathbb{K}$ is a commutative ring and M is a $\mathbb{K}$-module, then the elements of M are called *vectors*, while the elements of $\mathbb{K}$ are called *scalars*. If $\lambda \in \mathbb{K}$ and $a \in M$, then λa (that is, the image of (λ, a) under the scaling map $\cdot : \mathbb{K} \times M \to M$) will be called the result of *scaling* the vector a by the scalar λ.

Definition 6.3.3. If $\mathbb{K}$ is a field, then $\mathbb{K}$-modules are called $\mathbb{K}$-*vector spaces*. (When $\mathbb{K} = \mathbb{R}$, these are the usual real vector spaces known from undergraduate linear algebra classes.)

6.4. Examples of $\mathbb{K}$-modules

Thus, any vector space you have seen in linear algebra is an example of a module. Let us see some other examples:

Example 6.4.1. Let $\mathbb{K}$ be a commutative ring. Then, $\mathbb{K}$ itself is a $\mathbb{K}$-module (with the addition given by the addition $+_{\mathbb{K}}$ of $\mathbb{K}$, and with the scaling given by the multiplication $\cdot_{\mathbb{K}}$ of $\mathbb{K}$, and with the zero vector given by the zero $0_{\mathbb{K}}$ of $\mathbb{K}$).

Example 6.4.2. Let $\mathbb{K}$ be a commutative ring. Let $n \in \mathbb{N}$. Equip the set $\mathbb{K}^n$ (that is, the set of all n-tuples of elements of $\mathbb{K}$) with entrywise addition (that is, a binary operation $+$ on $\mathbb{K}^n$ defined by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

for all $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in \mathbb{K}^n$) and entrywise scaling (that is, a map $\cdot : \mathbb{K} \times \mathbb{K}^n \to \mathbb{K}^n$ defined by

$$\lambda (a_1, a_2, \ldots, a_n) = (\lambda a_1, \lambda a_2, \ldots, \lambda a_n)$$

for all $\lambda \in \mathbb{K}$ and $(a_1, a_2, \ldots, a_n) \in \mathbb{K}^n$) and the zero vector $(0, 0, \ldots, 0) \in \mathbb{K}^n$. Then, $\mathbb{K}^n$ becomes a $\mathbb{K}$-module.

Example 6.4.3. Let $\mathbb{K}$ be a commutative ring. Let $n, m \in \mathbb{N}$. Equip the set $\mathbb{K}^{n \times m}$ (that is, the set of all $n \times m$-matrices over $\mathbb{K}$) with the addition defined in Definition 5.8.7 **(a)** and the scaling defined in Definition 5.8.7 **(c)** and the zero vector $0_{n \times m}$. Then, $\mathbb{K}^{n \times m}$ becomes a $\mathbb{K}$-module.

Example 6.4.4. Let $\mathbb{K}$ be a commutative ring. The one-element set $\{0\}$ is a $\mathbb{K}$-module (with $+$ and $\cdot$ and zero vector defined in the only possible way). This is called the *zero module*. It is often called 0.

Example 6.4.5. Let n be an integer. Then:

(a) The set $\mathbb{Z}/n$ is a $\mathbb{Z}$-module, if you equip it with the addition and the scaling that we defined above (in Definition 3.4.12 and Definition 3.4.18) and with the zero vector $[0]_n$.

(b) The set $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\} = \{\text{all multiples of } n\}$ is a $\mathbb{Z}$-module (again equipped with the usual addition as addition, and the usual multiplication as scaling, and the integer 0 as zero vector).

Example 6.4.6. (a) The set $\mathbb{Q}$ (equipped with the usual addition, and with a scaling defined by the usual multiplication, and the zero vector 0) is a $\mathbb{Z}$-module.

(b) For every $q \in \mathbb{Q}$, the subset $q\mathbb{Z} := \{qz \mid z \in \mathbb{Z}\}$ of $\mathbb{Q}$ (again equipped with the usual $+$ and $\cdot$ and 0) is a $\mathbb{Z}$-module. For example, $\frac{1}{2}\mathbb{Z} = \{\ldots, -2, -1.5, -1, -0.5, 0, 0.5, 1, 1.5, 2, \ldots\}$ is a $\mathbb{Z}$-module. Note that $\frac{1}{2}\mathbb{Z}$ is **not** a ring (at least not with the usual $\cdot$ as multiplication), since $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \notin \frac{1}{2}\mathbb{Z}$.

(c) What other $\mathbb{Z}$-modules can we find inside $\mathbb{Q}$? Quite a few, it turns out. Here is a more exotic one: Let us call an integer n *squarefree* if it is not divisible by any perfect square other than 1. It is easy to see that an integer n is squarefree if and only if n is a product of **distinct** primes (or, equivalently, $v_p(n) \leq 1$ for each prime p). Thus, the squarefree integers are $1, 2, 3, 5, 6, 7, 10, 11, 13, \ldots$ and their negatives. Now, let $\mathbb{Q}_{\text{sqf}}$ be the subset

$$\left\{ \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ with } b \text{ squarefree} \right\}$$

of $\mathbb{Q}$. Then, $\mathbb{Q}_{\text{sqf}}$ (equipped with the usual addition as addition, the usual multiplication as scaling, and the usual 0 as zero vector) is a $\mathbb{Z}$-module. (Check this!)

6.5. Cartesian products of $\mathbb{K}$-modules

Instead of giving further examples, let us show a way of constructing new $\mathbb{K}$-modules from old (analogous to Definition 5.7.3):

Definition 6.5.1. Let $\mathbb{K}$ be a commutative ring. Let $M_1, M_2, \ldots, M_n$ be n many $\mathbb{K}$-modules. Consider the set $M_1 \times M_2 \times \cdots \times M_n$, whose elements are n-tuples $(m_1, m_2, \ldots, m_n)$ with $m_i \in M_i$.

We define a binary operation $+$ on $M_1 \times M_2 \times \cdots \times M_n$ by

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n),$$

and we define a "scaling" map $\cdot : \mathbb{K} \times (M_1 \times M_2 \times \cdots \times M_n) \to M_1 \times M_2 \times \cdots \times M_n$ by

$$\lambda \cdot (a_1, a_2, \ldots, a_n) = (\lambda a_1, \lambda a_2, \ldots, \lambda a_n).$$

Proposition 6.5.2. Let $\mathbb{K}$ be a commutative ring. Let $M_1, M_2, \ldots, M_n$ be n many $\mathbb{K}$-modules. The set $M_1 \times M_2 \times \cdots \times M_n$, endowed with the operation $+$ and the map $\cdot$ we just defined and with the zero vector $(0, 0, \ldots, 0)$, is a $\mathbb{K}$-module.

Definition 6.5.3. The $\mathbb{K}$-module $M_1 \times M_2 \times \cdots \times M_n$ constructed in Proposition 6.5.2 is called the *Cartesian product* (or *direct product*) of the $\mathbb{K}$-modules $M_1, M_2, \ldots, M_n$.

The $\mathbb{K}$-module $\mathbb{K}^n$ introduced in Example 6.4.2 is actually a particular case of Definition 6.5.3; in fact, it is precisely the Cartesian product $\underbrace{\mathbb{K} \times \mathbb{K} \times \cdots \times \mathbb{K}}_{n \text{ times}}$ of the $\mathbb{K}$-modules $\mathbb{K}, \mathbb{K}, \ldots, \mathbb{K}$ (that is, n copies of the $\mathbb{K}$-module $\mathbb{K}$ defined in Example 6.4.1).

6.6. Features and rules

Again, we shall follow the PEMDAS convention for addition and scaling. For example, the expression "$a + \lambda b$" shall mean $a + (\lambda b)$.

Proposition 6.6.1. Axioms **(g)** and **(j)** in Definition 6.3.1 follow from the others.

Proposition 6.6.2. Axiom **(d)** in Definition 6.3.1 follows from the others.

Note that Proposition 6.6.1 and Proposition 6.6.2 cannot be merged: If we omit all three axioms **(d)**, **(g)** and **(j)**, then we cannot recover these axioms any more. (Indeed, our proof of axiom **(d)** relied on axiom **(g)** and vice versa.)

What can you do when you have a $\mathbb{K}$-module?

Convention 6.6.3. For the rest of this section, we fix a **commutative** ring $\mathbb{K}$, and we fix a $\mathbb{K}$-module M. We shall denote the zero vector 0_M of M by 0. (More generally, it is common to denote the zero vector of any $\mathbb{K}$-module by 0 as long as you are not afraid of confusion.)

Just as in a ring, elements of a module have unique additive inverses:

Theorem 6.6.4. Let $a \in M$. Then:
(a) The element a has exactly one additive inverse.
(b) This additive inverse is $(-1)\, a$.

We can now make the following definition, which copies Definition 5.4.4 almost verbatim:

Definition 6.6.5. (a) If $a \in M$, then the additive inverse of a will be called $-a$. (This is well-defined, since Theorem 6.6.4 **(a)** shows that this additive inverse is unique.)
(b) If $a \in M$ and $b \in M$, then we define the *difference* $a - b$ to be the element $a + (-b)$ of M. This new binary operation $-$ on M is called "*subtraction*".

Remark 6.6.6. The subtraction we just defined (in Definition 6.6.5 **(b)**) for an arbitrary $\mathbb{K}$-module generalizes both

- the subtraction of matrices (when the $\mathbb{K}$-module is $\mathbb{K}^{n\times m}$), and
- the subtraction in $\mathbb{Z}/n$ (when $\mathbb{K} = \mathbb{Z}$ and the $\mathbb{K}$-module is $\mathbb{Z}/n$).

Remark 6.6.6 is easy to prove, but we delay the proof until later, since it will become even easier after Proposition 6.6.7 has been proven.

Using Definition 6.6.5 **(a)**, we can rewrite Theorem 6.6.4 **(b)** as follows:

$$-a = (-1)\, a \qquad \text{for each } a \in M. \tag{72}$$

Additive inverses and subtraction satisfy certain rules that should not surprise you:

Proposition 6.6.7. Let $a, b, c \in M$.
(a) We have $a - b = c$ if and only if $a = b + c$. (Roughly speaking, this means that subtraction undoes addition.)
(b) We have $-(a + b) = (-a) + (-b)$.
(c) We have $-0 = 0$.
(d) We have $0 - a = -a$.
(e) We have $-(-a) = a$.
(f) We have $-(\lambda a) = (-\lambda)\, a = \lambda\, (-a)$ for all $\lambda \in \mathbb{K}$.

(g) We have $a - b - c = a - (b + c)$. (Here and in the following, "$a - b - c$" should be read as "$(a - b) - c$".)

(h) We have $\lambda (b - c) = \lambda b - \lambda c$ and $(\lambda - \mu) a = \lambda a - \mu a$ for all $\lambda, \mu \in \mathbb{K}$.

(i) We have $-(a - b) = b - a$.

(j) We have $a - (-b) = a + b$.

(k) We have $(-1) a = -a$. (Here, the "1" on the left hand side means the unity of $\mathbb{K}$.)

(l) If $-a = -b$, then $a = b$.

Again, Proposition 6.6.7 shows that certain expressions (such as "$-\lambda a$" for $\lambda \in \mathbb{K}$ and $a \in M$) are unambiguous.

Theorem 5.4.6 holds for the $\mathbb{K}$-module M just as it holds for the ring $\mathbb{K}$. Thus, we have a notion of finite sums of elements of M; it behaves exactly like finite sums of elements of $\mathbb{K}$ do. But Theorem 5.4.7 has no analogue for $\mathbb{K}$-modules. (However, you can get something similar to Theorem 5.4.7 **(b)** by defining finite products of the form $\lambda_1 \lambda_2 \cdots \lambda_k a$ with $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}$ and $a \in M$.)

Definition 5.4.8 can be extended to modules by simply replacing $\mathbb{K}$ with M:

Definition 6.6.8. Let $a \in M$ and $n \in \mathbb{Z}$. Then, we define an element na of M by

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

We cannot define a^n for $a \in M$ and $n \in \mathbb{N}$.

Proposition 5.4.9 has an analogue for a $\mathbb{K}$-module; namely, we have the following:

Proposition 6.6.9. We have

$$(n + m) a = na + ma \quad \text{for all } a \in M \text{ and } n, m \in \mathbb{Z}; \tag{73}$$

$$n (a + b) = na + nb \quad \text{for all } a, b \in M \text{ and } n \in \mathbb{Z}; \tag{74}$$

$$-(na) = (-n) a = n (-a) \quad \text{for all } a \in M \text{ and } n \in \mathbb{Z}; \tag{75}$$

$$(nm) a = n (ma) \quad \text{for all } a \in M \text{ and } n, m \in \mathbb{Z}; \tag{76}$$

$$n (\lambda a) = (n\lambda) a = \lambda (na) \quad \text{for all } a \in M \text{ and } \lambda \in \mathbb{K} \text{ and } n \in \mathbb{Z}; \tag{77}$$

$$n 0_M = 0_M \quad \text{for all } n \in \mathbb{Z}; \tag{78}$$

$$1a = a \quad \text{for all } a \in M; \tag{79}$$

$$0a = 0_M \quad \text{for all } a \in M; \tag{80}$$

$$(-1) a = -a \quad \text{for all } a \in M. \tag{81}$$

(Here, "1" stands for the integer $1 \in \mathbb{Z}$, not for the scalar $1 \in \mathbb{K}$. Likewise, the "0" in "$0a$", and the "-1" in "$(-1) a$" stand for integers.) In particular, these

equalities show that certain expressions (like "nma" and "$n\lambda a$") are unambiguous.

Upshot: All the rules relating to addition that we know from rings are still true for $\mathbb{K}$-modules. Some basic rules relating to multiplication can be salvaged (i.e., made to work for $\mathbb{K}$-modules) by replacing multiplication by scaling.

6.7. Submodules

Convention 6.7.1. For the rest of Chapter 6, we fix a **commutative** ring $\mathbb{K}$, and we denote its addition, multiplication, zero and unity by $+$, $\cdot$, 0 and 1.

In Section 5.3, we have defined the notion of a subring of a ring. Similarly, we shall now define a submodule of a $\mathbb{K}$-module. For example, the $\mathbb{Z}$-modules $q\mathbb{Z}$ and $\mathbb{Q}_{\text{sqf}}$ from Example 6.4.6 will fall under this concept. The idea is the same as for subrings: A submodule of a $\mathbb{K}$-module N is a $\mathbb{K}$-module M that is a subset of N and has "the same" addition, scaling and zero vector. Here is the formal definition (analogous to Definition 5.3.1):

Definition 6.7.2. Let M and N be two $\mathbb{K}$-modules. We say that M is a $\mathbb{K}$-*submodule* (or, for short, *submodule*) of N if and only if it satisfies the following four requirements:

- the set M is a subset of N;
- the addition of M is a restriction of the addition of N (that is, we have $a_1 +_M a_2 = a_1 +_N a_2$ for all $a_1, a_2 \in M$);
- the scaling of M is a restriction of the scaling of N (that is, we have $\lambda \cdot_M a = \lambda \cdot_N a$ for all $\lambda \in \mathbb{K}$ and $a \in M$);
- the zero vector of M is the zero vector of N (that is, we have $0_M = 0_N$).

Thus, according to this definition:

- the $\mathbb{Z}$-modules $n\mathbb{Z}$ from Example 6.4.5 **(b)** are $\mathbb{Z}$-submodules of $\mathbb{Z}$;
- the $\mathbb{Z}$-modules $q\mathbb{Z}$ and $\mathbb{Q}_{\text{sqf}}$ from Example 6.4.6 are $\mathbb{Z}$-submodules of $\mathbb{Q}$;
- every $\mathbb{K}$-module M is a $\mathbb{K}$-submodule of itself.

Again, you can find examples of two $\mathbb{K}$-modules M and N for which the set M is a **subset** of N yet the $\mathbb{K}$-module M is **not a $\mathbb{K}$-submodule** of N. For example, $\mathbb{C}$ becomes a $\mathbb{C}$-module in the usual way (with addition playing the role of addition,

and multiplication playing the role of scaling); but you can also define a second "scaling" operation $\bar{\cdot} : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ by setting

$$\alpha \mathbin{\bar{\cdot}} \beta = \overline{\alpha}\beta \qquad \text{for all } \alpha, \beta \in \mathbb{C}.$$

Then, we can turn the set $\mathbb{C}$ into a $\mathbb{C}$-module by endowing it with the usual addition, the unusual scaling operation $\bar{\cdot}$ and the zero vector 0. This new $\mathbb{C}$-module may be called $\overline{\mathbb{C}}$, and is useful in studying Hermitian forms. The $\mathbb{C}$-modules $\mathbb{C}$ and $\overline{\mathbb{C}}$ are equal as sets, but neither is a $\mathbb{C}$-submodule of the other.

Definition 6.7.3. If $\mathbb{K}$ is a field, then $\mathbb{K}$-submodules are also known as $\mathbb{K}$-*vector subspaces* (or, short, $\mathbb{K}$-*subspaces*).

When we have two $\mathbb{K}$-modules M and N such that $M \subseteq N$ as sets (or, more generally, such that M and N have elements in common), we generally need to be careful using the symbol "$+$": This symbol may mean both the addition of M and the addition of N, and these additions might not be the same. Thus it is prudent to disambiguate its meaning by attaching a subscript "$_M$" or "$_N$" to it. The same applies to the symbols "$\cdot$" and "0" and expressions like "λa" (which have an implicit scaling sign). However, when M is a $\mathbb{K}$-submodule of N, we do not need to take this precaution; in this case, the meaning of expressions like "$a + b$" does not depend on whether you read "$+$" as the addition of M or as the addition of N.

The following is analogous to Proposition 5.3.4:

Proposition 6.7.4. Let N be a $\mathbb{K}$-module. Let S be a subset of N that satisfies the following three conditions:[76]

- We have $0 \in S$.
- The subset S is *closed under addition*. (This means that all $a, b \in S$ satisfy $a + b \in S$.)
- The subset S is *closed under scaling*. (This means that all $\lambda \in \mathbb{K}$ and $a \in S$ satisfy $\lambda a \in S$.)

Then, the set S itself becomes a $\mathbb{K}$-module if we endow it with:

- an addition operation $+$ which is defined as the restriction of the addition operation of the $\mathbb{K}$-module N;
- a scaling map $\cdot : \mathbb{K} \times S \to S$ which is defined as the restriction of the scaling map of the $\mathbb{K}$-module N,

and the zero vector 0. Furthermore, this $\mathbb{K}$-module S is a $\mathbb{K}$-submodule of N.

[76] In this proposition, the symbols "$+$", "$\cdot$" and "0" mean the addition, the scaling and the zero vector of N.

Definition 6.7.5. Let N be a $\mathbb{K}$-module. Let S be a subset of N that satisfies the three conditions of Proposition 6.7.4. Then, we shall say that "S is a $\mathbb{K}$-submodule of N". Technically speaking, this is premature, since S is so far just a subset of N without the structure of a $\mathbb{K}$-module; however, Proposition 6.7.4 shows that there is an obvious way of turning S into a $\mathbb{K}$-module (viz.: define an operation $+$ by restricting the corresponding operation of N, define a map $\cdot$ similarly, and steal the zero vector from N), and we shall automatically regard S as becoming a $\mathbb{K}$-module in this way (unless we say otherwise). We say that the addition operation $+$ on S (obtained by restricting the corresponding operation on N) and the scaling map $\cdot$ of S and the zero vector of S are *inherited from* N.

Thus, finding $\mathbb{K}$-submodules of a $\mathbb{K}$-module N boils down to finding subsets that contain its 0 and are closed under addition and under scaling; the module axioms don't need to be re-checked.

Thus, in particular, when $\mathbb{K}$ is a field, the vector subspaces of $\mathbb{K}^{n\times 1}$ (as in Definition 6.1.3) are precisely the $\mathbb{K}$-submodules of $\mathbb{K}^{n\times 1}$. Many examples of $\mathbb{K}$-submodules can thus be found in textbooks on linear algebra. If M is any $\mathbb{K}$-module, then both M and the one-element subset $\{0_M\}$ are $\mathbb{K}$-submodules of M (this is easily checked); the more interesting submodules are the ones that lie in between these two extremes.

6.8. Linear maps, aka module homomorphisms

Recall Definition 5.9.1. In a similar way, we define $\mathbb{K}$-*module homomorphisms*, also known as $\mathbb{K}$-*linear maps*:

Definition 6.8.1. Let M and N be two $\mathbb{K}$-modules. A $\mathbb{K}$-*module homomorphism* from M to N means a map $f : M \to N$ that satisfies the following three axioms:

- **(a)** We have $f(a+b) = f(a) + f(b)$ for all $a, b \in M$. (This is called "f respects addition" or "f preserves addition".)
- **(b)** We have $f(0) = 0$. (This, of course, means $f(0_M) = 0_N$.)
- **(c)** We have $f(\lambda a) = \lambda f(a)$ for all $\lambda \in \mathbb{K}$ and $a \in M$. (This is called "f respects scaling" or "f preserves scaling".)

Instead of "$\mathbb{K}$-module homomorphism", we can also say "$\mathbb{K}$-*linear map*" or just "*linear map*" (when $\mathbb{K}$ is clear).

Remark 6.8.2. The axiom **(b)** in Definition 6.8.1 is redundant – it follows from axiom **(a)**.

Some authors (for example, Hefferon in [Heffer17, Chapter Three, Definition II.1.1], and the authors of [LaNaSc16, Definition 6.1.1]) omit the axiom **(b)** when

they define $\mathbb{K}$-linear maps. This does not change the concept, as Remark 6.8.2 shows.

What are some examples of module homomorphisms?

Example 6.8.3. Let M be a $\mathbb{K}$-module.

(a) The identity map $\mathrm{id} : M \to M$ is $\mathbb{K}$-linear.

(b) For any $\lambda \in \mathbb{K}$, the map $L_\lambda : M \to M,\ a \mapsto \lambda a$ is $\mathbb{K}$-linear.

(c) If $M = \mathbb{K}$ (specifically, the $\mathbb{K}$-module $\mathbb{K}$ defined in Example 6.4.1), then the maps L_λ (for $\lambda \in \mathbb{K}$) that we just defined are the only $\mathbb{K}$-linear maps from M to M.

Next comes a less basic example:

Theorem 6.8.4. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n\times m}$ be an $n \times m$-matrix. Define a map

$$\begin{aligned} L_A : \mathbb{K}^{m\times 1} &\to \mathbb{K}^{n\times 1}, \\ v &\mapsto Av. \end{aligned}$$

This map L_A is a $\mathbb{K}$-module homomorphism from $\mathbb{K}^{m\times 1}$ to $\mathbb{K}^{n\times 1}$.

Proposition 6.8.5. Let $n, m \in \mathbb{N}$. Each $\mathbb{K}$-module homomorphism from $\mathbb{K}^{m\times 1}$ to $\mathbb{K}^{n\times 1}$ has the form L_A for a unique $A \in \mathbb{K}^{n\times m}$ (where L_A is defined as in Theorem 6.8.4).

We shall delay the proof of this proposition until we have shown some auxiliary results. First, we define a specific kind of column vectors:

Definition 6.8.6. Let $m \in \mathbb{N}$. For each $j \in \{1, 2, \ldots, m\}$, we let $e_j \in \mathbb{K}^{m\times 1}$ be the column vector

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} = (0, 0, \ldots, 0, 1, 0, 0, \ldots, 0)^T$$

where the 1 is at the j-th position. (Strictly speaking, we should denote it by $e_{j,m}$ rather than e_j, since it depends on m and not just on j; but the m will always be clear from the context.)

These column vectors $e_1, e_2, \ldots, e_m$ are called the *standard basis vectors* of $\mathbb{K}^{m\times 1}$.

For example, if $m = 3$, then $e_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ and $e_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$ and $e_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$.

Lemma 6.8.7. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be an $n \times m$-matrix.
(a) We have $Ae_j = (\text{the } j\text{-th column of } A)$ for all $j \in \{1, 2, \ldots, m\}$.
(b) Consider the map L_A defined in Theorem 6.8.4. Then,

$$L_A\left(e_j\right) = (\text{the } j\text{-th column of } A) \qquad \text{for all } j \in \{1, 2, \ldots, m\}.$$

Proposition 6.8.8. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a $\mathbb{K}$-linear map.
(a) We have $f(\lambda a + \mu b) = \lambda f(a) + \mu f(b)$ for all $\lambda, \mu \in \mathbb{K}$ and $a, b \in M$.
(b) Let $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}$ and $a_1, a_2, \ldots, a_k \in M$. Then,

$$f\left(\sum_{i=1}^{k} \lambda_i a_i\right) = \sum_{i=1}^{k} \lambda_i f(a_i).$$

(In words: f "preserves linear combinations".)

Proposition 6.8.8 **(a)** has a converse:

Proposition 6.8.9. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a map. Assume that

$$f(\lambda a + \mu b) = \lambda f(a) + \mu f(b) \qquad \text{for all } \lambda, \mu \in \mathbb{K} \text{ and } a, b \in M. \tag{82}$$

Then, f is $\mathbb{K}$-linear.

Some authors use the axiom (82) as their definition of what it means for a map $f : M \to N$ between two $\mathbb{K}$-modules M and N to be $\mathbb{K}$-linear. This definition is equivalent to ours (due to Proposition 6.8.9 and Proposition 6.8.8 **(a)**).

Lemma 6.8.10. Let $m \in \mathbb{N}$, and let N be a $\mathbb{K}$-module. For each $j \in \{1, 2, \ldots, m\}$, we let define a column vector $e_j \in \mathbb{K}^{m \times 1}$ as in Definition 6.8.6.

Let $f, g : \mathbb{K}^{m \times 1} \to N$ be two $\mathbb{K}$-linear maps. Assume that $f\left(e_j\right) = g\left(e_j\right)$ for all $j \in \{1, 2, \ldots, m\}$. Then, $f = g$.

We are now ready to prove Proposition 6.8.5:

Definition 6.8.11. Let M and N be two $\mathbb{K}$-modules.
(a) Let $\operatorname{Hom}(M, N)$ be the set of all $\mathbb{K}$-module homomorphisms (= linear maps) from M to N. We shall now turn this set into a $\mathbb{K}$-module.
(b) We define an addition $+$ on $\operatorname{Hom}(M, N)$ as follows: If $f, g \in \operatorname{Hom}(M, N)$, then $f + g \in \operatorname{Hom}(M, N)$ is defined by

$$(f + g)(v) = f(v) + g(v) \qquad \text{for all } v \in M.$$

(That is, the addition is pointwise. This is well-defined by Proposition 6.8.12 **(a)** below.)

(c) We define a scaling $\cdot$ on $\operatorname{Hom}(M,N)$ as follows: If $\lambda \in \mathbb{K}$ and $f \in \operatorname{Hom}(M,N)$, then $\lambda f \in \operatorname{Hom}(M,N)$ is defined by

$$(\lambda f)(v) = \lambda \cdot f(v) \qquad \text{for all } v \in M.$$

(That is, the scaling is pointwise. This is well-defined by Proposition 6.8.12 **(b)** below.)

(d) We define a map $0_{M\to N} : M \to N$ by setting

$$0_{M\to N}(v) = 0 \qquad \text{for all } v \in M.$$

(e) We equip $\operatorname{Hom}(M,N)$ with the addition $+$, the scaling $\cdot$ and the zero vector $0_{M\to N}$ we have just defined. This yields a $\mathbb{K}$-module (by Proposition 6.8.12 **(d)** below).

Proposition 6.8.12. **(a)** The addition $+$ defined in Definition 6.8.11 **(b)** is well-defined (i.e., we have $f+g \in \operatorname{Hom}(M,N)$ for all $f,g \in \operatorname{Hom}(M,N)$).

(b) The scaling $\cdot$ defined in Definition 6.8.11 **(c)** is well-defined (i.e., we have $\lambda f \in \operatorname{Hom}(M,N)$ for all $\lambda \in \mathbb{K}$ and $f \in \operatorname{Hom}(M,N)$).

(c) The map $0_{M\to N}$ defined in Definition 6.8.11 **(d)** belongs to $\operatorname{Hom}(M,N)$.

(d) The set $\operatorname{Hom}(M,N)$, equipped with the addition $+$, the scaling $\cdot$ and the zero vector $0_{M\to N}$, is a $\mathbb{K}$-module.

Proposition 6.8.13. Let M, N and P be three $\mathbb{K}$-modules. Let $f : M \to N$ and $g : N \to P$ be two $\mathbb{K}$-module homomorphisms. Then, the composition $g \circ f : M \to P$ is also a $\mathbb{K}$-module homomorphism.

Note the analogy between Proposition 6.8.13 and Proposition 5.9.15.

We shall follow PEMDAS-style conventions when writing expressions involving addition and composition of $\mathbb{K}$-linear maps (where we treat composition as a multiplication-like operation). For example, the expression "$f \circ h + g \circ h$" (where f, g, h are three $\mathbb{K}$-linear maps) is to be understood as $(f \circ h) + (g \circ h)$.

The following rules hold for addition, multiplication and scaling of module homomorphisms (similarly to Theorem 5.8.10):

Theorem 6.8.14. Let N, M, P, Q be $\mathbb{K}$-modules.

(a) We have $f + g = g + f$ for any $f, g \in \operatorname{Hom}(M,N)$.

(b) We have $f + (g + h) = (f + g) + h$ for any $f, g, h \in \operatorname{Hom}(M,N)$.

(c) We have $f + 0_{M\to N} = 0_{M\to N} + f = f$ for any $f \in \operatorname{Hom}(M,N)$.

(d) We have $f \circ \mathrm{id}_M = \mathrm{id}_N \circ f = f$ for any $f \in \operatorname{Hom}(M,N)$.

(e) In general, we **do not** have $f \circ g = g \circ f$. In fact, it can happen that one of $f \circ g$ and $g \circ f$ is defined and the other is not; but even if both are defined, they can be distinct.

(f) We have $f \circ (g \circ h) = (f \circ g) \circ h$ for any $f \in \operatorname{Hom}(P, Q)$, $g \in \operatorname{Hom}(N, P)$ and $h \in \operatorname{Hom}(M, N)$.

(g) We have $f \circ (g + h) = f \circ g + f \circ h$ for any $f \in \operatorname{Hom}(N, P)$ and $g, h \in \operatorname{Hom}(M, N)$.

We have $(f + g) \circ h = f \circ h + g \circ h$ for any $f, g \in \operatorname{Hom}(N, P)$ and $h \in \operatorname{Hom}(M, N)$.

(h) We have $f \circ 0_{P \to M} = 0_{P \to N}$ and $0_{N \to P} \circ f = 0_{M \to P}$ for any $f \in \operatorname{Hom}(M, N)$.

(j) We have $r(f + g) = rf + rg$ for any $r \in \mathbb{K}$ and $f, g \in \operatorname{Hom}(M, N)$.

(k) We have $(r + s) f = rf + sf$ for any $r, s \in \mathbb{K}$ and $f \in \operatorname{Hom}(M, N)$.

(l) We have $r(sf) = (rs) f$ for any $r, s \in \mathbb{K}$ and $f \in \operatorname{Hom}(M, N)$.

(m) We have $r(f \circ g) = (rf) \circ g = f \circ (rg)$ for any $r \in \mathbb{K}$ and $f \in \operatorname{Hom}(N, P)$ and $g \in \operatorname{Hom}(M, N)$.

(o) We have $1f = f$ for any $f \in \operatorname{Hom}(M, N)$.

(The above list is skipping a few letters since we have not defined subtraction yet; nevertheless, subtraction exists and satisfies the appropriate rules. See below for the details.)

So far, we have not defined a subtraction operation $-$ on $\operatorname{Hom}(M, N)$ (where M and N are two $\mathbb{K}$-modules). But this does not mean that such an operation does not exist; we simply don't want to waste our time defining it "manually" when we can trivially obtain it from general principles. Namely: We know that $\operatorname{Hom}(M, N)$ is a $\mathbb{K}$-module, but Definition 6.6.5 shows that every $\mathbb{K}$-module automatically has a subtraction operation. Thus, we get a subtraction operation on $\operatorname{Hom}(M, N)$ for free. This subtraction is precisely the pointwise subtraction: i.e., it is given by

$$(f - g)(v) = f(v) - g(v) \qquad \text{for all } f, g \in \operatorname{Hom}(M, N) \text{ and } v \in M \tag{83}$$

[77].

Proposition 6.6.7 shows that the subtraction operation on $\operatorname{Hom}(M, N)$ (for arbitrary $\mathbb{K}$-modules M and N) has almost all the properties that one would expect. The only rule that we do not automatically obtain from these general principles is

$$-(f \circ g) = (-f) \circ g = f \circ (-g) \qquad \text{for all } f \in \operatorname{Hom}(N, P) \text{ and } g \in \operatorname{Hom}(M, N)$$

(where M, N and P are three $\mathbb{K}$-modules). But this rule is easily verified by direct comparison (using (83)).

[77] *Proof of (83):* Let $f, g \in \operatorname{Hom}(M, N)$ and $v \in M$. Then, $f - g$ has the property that $f = (f - g) + g$ (by Proposition 6.6.7 **(a)**). Applying both sides of this equality to v, we obtain

$$f(v) = ((f - g) + g)(v) = (f - g)(v) + g(v) \qquad \text{(by the definition of } (f - g) + g\text{)};$$

but this yields $(f - g)(v) = f(v) - g(v)$. This proves (83).

Corollary 6.8.15. Let M be a $\mathbb{K}$-module. The set $\operatorname{Hom}(M, M)$ of all $\mathbb{K}$-linear maps from M to M (endowed with the addition $+$, the multiplication $\circ$, the zero $0_{M \to M}$ and the unity id_M) is a ring. This ring is called the *endomorphism ring* of M, and is denoted by $\operatorname{End} M$; its elements (i.e., the $\mathbb{K}$-linear maps $M \to M$) are called the *endomorphisms* of M.

So the multiplication of the ring $\operatorname{End} M$ is composition of maps. This ring $\operatorname{End} M$ is, in general, not commutative.

Note that $\operatorname{End} M = \operatorname{Hom}(M, M)$ as sets, and the additions of $\operatorname{End} M$ and of $\operatorname{Hom}(M, M)$ are the same. But $\operatorname{End} M$ is a ring (thus has no scaling), whereas $\operatorname{Hom}(M, M)$ is a $\mathbb{K}$-module (thus has no multiplication).

6.9. $\mathbb{K}$-algebras

There is a notion which combines both the structure of a ring and the structure of a $\mathbb{K}$-module (so it has both multiplication and scaling); this is the notion of a $\mathbb{K}$-*algebra*. It is defined as follows:

Definition 6.9.1. A $\mathbb{K}$-*algebra* is a set M endowed with two binary operations $+$ and $\cdot$ (called "*addition*" and "*multiplication*") as well as a scaling map $\cdot : \mathbb{K} \times M \to M$ (not to be confused with the multiplication map, which is also denoted by $\cdot$) and two elements $0, 1 \in M$ that satisfy all the ring axioms (with $\mathbb{K}$ replaced by M) as well as all the module axioms (where the zero vector 0_M is taken to be the element $0 \in M$) and also the following axiom:

- **Scale-invariance of multiplication:** We have $\lambda (ab) = (\lambda a) \cdot b = a \cdot (\lambda b)$ for all $\lambda \in \mathbb{K}$ and $a, b \in M$. Here, as usual, we omit the "$\cdot$" sign both for the multiplication operation $\cdot$ (that is, we write "uv" for "$u \cdot v$" when $u, v \in M$) and for the scaling map $\cdot$ (that is, we write "λu" for "$\lambda \cdot u$" when $\lambda \in \mathbb{K}$ and $u \in M$).

It seems somewhat confusing that both the multiplication map $M \times M \to M$ and the scaling map $\mathbb{K} \times M \to M$ are denoted by the same symbol $\cdot$; but in practice, this does not cause any trouble, since it is (almost) always clear from the context which one is being applied (just check if the first argument belongs to M or to $\mathbb{K}$).

So, roughly speaking, a $\mathbb{K}$-*algebra* is a $\mathbb{K}$-module that is also a ring, with the same addition and the same zero, and satisfying the "Scale-invariance of multiplication" axiom. In other words, you get the definition of a $\mathbb{K}$-algebra by throwing the definitions of a ring and of a $\mathbb{K}$-module together, requiring the two additions $+$ to be the same map, requiring the zero of the ring to coincide with the zero vector of the $\mathbb{K}$-module, and requiring the multiplication to be "nice to the scaling" (in the sense that the "Scale-invariance of multiplication" axiom holds).

Examples of $\mathbb{K}$-algebras include the following:

- The commutative ring $\mathbb{K}$ itself is a $\mathbb{K}$-algebra (with both multiplication and scaling being the usual multiplication $\cdot$ of $\mathbb{K}$).
- If M is any $\mathbb{K}$-module, then the endomorphism ring $\operatorname{End} M$ becomes a $\mathbb{K}$-algebra. (Its multiplication is composition of maps, whereas its scaling is the scaling on $\operatorname{Hom}(M, M)$.)
- The matrix ring $\mathbb{K}^{n\times n}$ is a $\mathbb{K}$-algebra for any $n \in \mathbb{N}$.
- The ring $\mathbb{C}$ is an $\mathbb{R}$-algebra.
- The ring $\mathbb{R}$ is a $\mathbb{Q}$-algebra.
- More generally: If a commutative ring $\mathbb{K}$ is a subring of a commutative ring $\mathbb{L}$, then $\mathbb{L}$ becomes a $\mathbb{K}$-algebra in a natural way[78].
- The polynomial ring $\mathbb{K}[x]$ (introduced in Definition 7.4.10) is a $\mathbb{K}$-algebra.

Particularly common are the $\mathbb{Z}$-algebras: In fact, every ring $\mathbb{K}$ is a $\mathbb{Z}$-algebra in a natural way! To see this, we just need to equip every ring $\mathbb{K}$ with a scaling map $\cdot : \mathbb{Z} \times \mathbb{K} \to \mathbb{K}$ that satisfies the module axioms and the "Scale-invariance of multiplication" axiom. This is done as follows:

Example 6.9.2. Let $\mathbb{K}$ be any ring. Consider the map $\cdot : \mathbb{Z} \times \mathbb{K} \to \mathbb{K}$ sending each pair $(n, a) \in \mathbb{Z} \times \mathbb{K}$ to the element $na \in \mathbb{K}$ defined in Definition 5.4.8. (This map $\cdot$ is not the multiplication operation of $\mathbb{K}$ (unless $\mathbb{K} = \mathbb{Z}$), but we still use the same notation for it, since both of these maps are "multiplications" in a wide sense.) Then, the set $\mathbb{K}$, equipped with the binary operations $+$ and $\cdot$ (the multiplication operation of $\mathbb{K}$), the scaling map $\cdot$ we just defined, and the elements $0_{\mathbb{K}}$ and $1_{\mathbb{K}}$ is a $\mathbb{Z}$-algebra.

Convention 6.9.3. If M is a $\mathbb{K}$-algebra, then M automatically becomes a ring (by forgetting the scaling map) and a $\mathbb{K}$-module (by forgetting the multiplication operation and the unity, and declaring the element 0 to be the zero vector). We shall automatically treat any $\mathbb{K}$-algebra both as a ring and as a $\mathbb{K}$-module when needed: For example, if M and N are two $\mathbb{K}$-algebras, and we speak of a "ring homomorphism from M to N", then we mean a ring homomorphism from the ring M to the ring N, where M and N become rings in the way we just explained.

[78] Namely:

- We define the scaling of the $\mathbb{K}$-module $\mathbb{L}$ to be the restriction of the multiplication of the ring $\mathbb{L}$ to $\mathbb{K} \times \mathbb{L}$. (Thus, $\lambda \cdot a = \lambda \cdot a$ for all $\lambda \in \mathbb{K}$ and $a \in \mathbb{L}$, where the "$\cdot$" sign on the left hand side stands for scaling and where the "$\cdot$" sign on the right hand side stands for multiplication.)
- We define the zero vector of $\mathbb{L}$ to be the zero of the ring $\mathbb{L}$.

There is also a notion of a $\mathbb{K}$-*subalgebra* of a $\mathbb{K}$-algebra, which can be easily defined as follows:

Definition 6.9.4. Let A and B be two $\mathbb{K}$-algebras. We say that A is a $\mathbb{K}$-*subalgebra* (or, for short, *subalgebra*) of B if and only if it satisfies the following six requirements:

- the set A is a subset of B;
- the addition of A is a restriction of the addition of B (that is, we have $a_1 +_A a_2 = a_1 +_B a_2$ for all $a_1, a_2 \in A$);
- the multiplication of A is a restriction of the multiplication of B (that is, we have $a_1 \cdot_A a_2 = a_1 \cdot_B a_2$ for all $a_1, a_2 \in A$);
- the zero of A is the zero of B (that is, we have $0_A = 0_B$);
- the unity of A is the unity of B (that is, we have $1_A = 1_B$);
- the scaling of A is a restriction of the scaling of B (that is, we have $\lambda \cdot_A a = \lambda \cdot_B a$ for all $\lambda \in \mathbb{K}$ and $a \in A$).

Equivalently, A is a $\mathbb{K}$-subalgebra of B if and only if A is simultaneously a subring of B and a $\mathbb{K}$-submodule of B. (Here, we are treating $\mathbb{K}$-algebras as rings and as $\mathbb{K}$-modules, as explained in Convention 6.9.3.)

Similarly, there is a notion of a $\mathbb{K}$-algebra homomorphism:

Definition 6.9.5. Let A and B be two $\mathbb{K}$-algebras. A $\mathbb{K}$-*algebra homomorphism* from A to B means a map $f : A \to B$ that is simultaneously a ring homomorphism from A to B and a $\mathbb{K}$-module homomorphism from A to B. (That is, it means a map $f : A \to B$ that respects addition, respects multiplication, respects scaling, sends 0_A to 0_B, and sends 1_A to 1_B.)

Definition 6.9.6. We say that a $\mathbb{K}$-algebra is *commutative* if the underlying ring is commutative (i.e., if we have $ab = ba$ for each two elements a and b of this $\mathbb{K}$-algebra).

The following property of $\mathbb{K}$-algebras is easy to check but quite useful:

Proposition 6.9.7. Let A be a $\mathbb{K}$-algebra. Let $k \in \mathbb{N}$.

(a) Any $\lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}$ and $a_1, a_2, \ldots, a_k \in A$ satisfy

$$(\lambda_1 a_1)(\lambda_2 a_2) \cdots (\lambda_k a_k) = (\lambda_1 \lambda_2 \cdots \lambda_k)(a_1 a_2 \cdots a_k).$$

(b) Any $\lambda \in \mathbb{K}$ and $a \in A$ satisfy $(\lambda a)^k = \lambda^k a^k$.

6.10. Module isomorphisms

In analogy to Definition 5.10.1, we define:

Definition 6.10.1. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a map. Then, f is called a $\mathbb{K}$-*module isomorphism* if and only if f is invertible (i.e., bijective) and both f and f^{-1} are $\mathbb{K}$-module homomorphisms.

Example 6.10.2. Let M be a $\mathbb{K}$-module. The identity map $\mathrm{id} : M \to M$ is a $\mathbb{K}$-module isomorphism.

More generally:

Example 6.10.3. Let M be a $\mathbb{K}$-submodule of a $\mathbb{K}$-module N. Let $\iota : M \to N$ be the map that sends each $a \in M$ to a itself. (This map is called the *inclusion map* from M to N.)

(a) Then, the map ι is a $\mathbb{K}$-module homomorphism.

(b) It is an isomorphism if and only if $M = N$.

Proposition 5.10.5 has an analogue for $\mathbb{K}$-module isomorphisms:

Proposition 6.10.4. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be an invertible $\mathbb{K}$-module homomorphism. Then, f is a $\mathbb{K}$-module isomorphism.

The Chinese Remainder Theorem already brought us an example of a ring isomorphism (Example 5.10.7); we can also turn it into an example of a module isomorphism:

Example 6.10.5. Let m and n be two coprime positive integers. Then, $(\mathbb{Z}/m) \times (\mathbb{Z}/n)$ is a $\mathbb{Z}$-module (according to Definition 6.5.3). Theorem 3.6.2 says that the map

$$\begin{aligned} S_{m,n} : \mathbb{Z}/(mn) &\to (\mathbb{Z}/m) \times (\mathbb{Z}/n), \\ \alpha &\mapsto (\pi_{mn,m}(\alpha), \pi_{mn,n}(\alpha)) \end{aligned}$$

is well-defined and is a bijection. This map $S_{m,n}$ is furthermore a $\mathbb{Z}$-module isomorphism.

Definition 6.10.6. Let M and N be two $\mathbb{K}$-modules. We say that the $\mathbb{K}$-modules M and N are *isomorphic* if there exists a $\mathbb{K}$-module isomorphism $f : M \to N$.

We write "$M \cong N$ ($\mathbb{K}$-modules)" to say that the $\mathbb{K}$-modules M and N are isomorphic.

Keep in mind that one and the same symbol can stand both for a ring and for a $\mathbb{K}$-module. Thus, when saying something like "$M \cong N$", you should clarify whether you mean "$M \cong N$ (as rings)" or "$M \cong N$ ($\mathbb{K}$-modules)". For example,

$\mathbb{C}$ and $\mathbb{R} \times \mathbb{R}$ are both rings and $\mathbb{R}$-modules[79]. We do have $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$ as $\mathbb{R}$-modules, but we don't have $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$ as rings (since $\mathbb{C}$ is a field, but $\mathbb{R} \times \mathbb{R}$ is not a field). So an unqualified statement like "$\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$" would be dangerous.

Example 6.10.7. Let $n, m \in \mathbb{N}$. Then, the map

$$\begin{aligned} \mathbb{K}^{n \times m} &\to \mathbb{K}^{m \times n}, \\ A &\mapsto A^T \end{aligned}$$

is a $\mathbb{K}$-module isomorphism.

Example 6.10.8. Let $n \in \mathbb{N}$. Then, the map

$$\begin{aligned} \mathbb{K}^{n \times 1} &\to \mathbb{K}^n, \\ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} &\mapsto (a_1, a_2, \ldots, a_n) \end{aligned}$$

is a $\mathbb{K}$-module isomorphism.

The previous two examples show that

$$\mathbb{K}^{1 \times n} \cong \mathbb{K}^{n \times 1} \cong \mathbb{K}^n \qquad \text{as } \mathbb{K}\text{-modules.}$$

Example 6.10.9. Let $n, m \in \mathbb{N}$. Then, we define a map

$$\begin{aligned} \operatorname{vec} : \mathbb{K}^{n \times m} &\to \mathbb{K}^{nm}, \\ \left(a_{i,j}\right)_{1 \le i \le n,\ 1 \le j \le m} &\mapsto \left(a_{1,1}, a_{1,2}, \ldots, a_{1,m}, a_{2,1}, a_{2,2}, \ldots, a_{2,m}, \ldots, a_{n,1}, a_{n,2}, \ldots, a_{n,m}\right). \end{aligned}$$

For example, if $n = 2$ and $m = 3$, then

$$\operatorname{vec} \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} = (a, b, c, d, e, f).$$

This map vec is called *row reading* or *row vectorization*.

This map vec is a $\mathbb{K}$-module isomorphism.

[79] Indeed:

- The set $\mathbb{C}$ becomes an $\mathbb{R}$-module by defining scaling as multiplication (and addition as addition, and the zero vector as 0), whereas
- the set $\mathbb{R} \times \mathbb{R}$ becomes an $\mathbb{R}$-module according to Definition 6.5.3 (so its scaling is defined entrywise: that is, $\lambda (u, v) = (\lambda u, \lambda v)$ for all $\lambda \in \mathbb{R}$ and $(u, v) \in \mathbb{R} \times \mathbb{R}$).

Example 6.10.10. Let M be any $\mathbb{K}$-module. Let $\lambda \in \mathbb{K}$. Define the map

$$\begin{aligned} L_\lambda : M &\to M, \\ a &\mapsto \lambda a. \end{aligned}$$

(This is called "scaling by λ".) As we know from Example 6.8.3 **(b)**, this map L_λ is $\mathbb{K}$-linear, i.e., a $\mathbb{K}$-module homomorphism. When is it an isomorphism?

(a) If $\lambda \in \mathbb{K}$ is invertible, then L_λ is a $\mathbb{K}$-module isomorphism.

(b) If $M = \mathbb{K}$ and L_λ is a $\mathbb{K}$-module isomorphism, then λ is invertible.

(c) If $\mathbb{K} = \mathbb{Z}$ and $M = \mathbb{Z}/n$ for some integer n, then L_λ is a $\mathbb{K}$-module isomorphism whenever $\lambda \perp n$.

Remark 6.10.11. Fix any $\mathbb{K}$-module M. Then, the map

$$\begin{aligned} \mathbb{K} &\to \operatorname{End} M, \\ \lambda &\mapsto L_\lambda \end{aligned}$$

is a ring homomorphism.

We talked for a while about the meaning and use of ring isomorphisms. The same can be said about $\mathbb{K}$-module isomorphisms. So, in particular, two isomorphic $\mathbb{K}$-modules can be viewed as being "the same $\mathbb{K}$-module up to renaming its elements", and any property of one can be transferred to the other. For example, two isomorphic $\mathbb{K}$-modules must have the same size; their endomorphism rings must be isomorphic; etc.

Proposition 6.10.12. Let $n, m \in \mathbb{N}$. The map

$$\begin{aligned} \mathbb{K}^{n\times m} &\to \operatorname{Hom}\left(\mathbb{K}^{m\times 1}, \mathbb{K}^{n\times 1}\right), \\ A &\mapsto L_A \end{aligned}$$

(where L_A is defined as in Theorem 6.8.4) is a $\mathbb{K}$-module isomorphism.

So $\mathbb{K}^{n\times m} \cong \operatorname{Hom}\left(\mathbb{K}^{m\times 1}, \mathbb{K}^{n\times 1}\right)$ as $\mathbb{K}$-modules whenever $n, m \in \mathbb{N}$. This means that **$\mathbb{K}$-linear maps between $\mathbb{K}^{m\times 1}$ and $\mathbb{K}^{n\times 1}$ are "the same as" $n \times m$-matrices**. This says that the "matrix" way of doing linear algebra can be embedded into the "$\mathbb{K}$-module" way of doing linear algebra.

Multiplication of matrices is directly connected to composition of linear maps:

Proposition 6.10.13. Let $n, m, p \in \mathbb{N}$. Let $A \in \mathbb{K}^{n\times m}$ and $B \in \mathbb{K}^{m\times p}$. Then, $L_{AB} = L_A \circ L_B$.

Corollary 6.10.14. Let $n \in \mathbb{N}$. The map

$$\begin{aligned} \mathbb{K}^{n\times n} &\to \operatorname{End}\left(\mathbb{K}^{n\times 1}\right), \\ A &\mapsto L_A \end{aligned}$$

(where L_A is defined as in Theorem 6.8.4 for $m = n$) is a ring isomorphism.

6.11. Linear independence, spans, bases

Now, let us generalize Definition 6.1.4 to arbitrary $\mathbb{K}$-modules (where $\mathbb{K}$ is still an arbitrary commutative ring):

Definition 6.11.1. Let M be a $\mathbb{K}$-module. Let $v_1, v_2, \ldots, v_k$ be some vectors in M.

(a) A *linear combination* of $v_1, v_2, \ldots, v_k$ means a vector of the form

$$\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k, \qquad \text{with } \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}. \tag{84}$$

(b) The *span* of $v_1, v_2, \ldots, v_k$ is defined to be the subset

$$\begin{aligned} &\{\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k \mid \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathbb{K}\} \\ &= \{\text{linear combinations of } v_1, v_2, \ldots, v_k\} \end{aligned}$$

of M. This span is a $\mathbb{K}$-submodule of M. (This is easy to check.)

(c) The vectors $v_1, v_2, \ldots, v_k$ are said to be *linearly independent* if the only k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $\lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k = 0$ is $\left(\underbrace{0, 0, \ldots, 0}_{k \text{ times}}\right)$.

(d) Let U be a $\mathbb{K}$-submodule of M. We say that $v_1, v_2, \ldots, v_k$ form a *basis* of U (or, more formally, $(v_1, v_2, \ldots, v_k)$ is a basis of U) if and only if the vectors $v_1, v_2, \ldots, v_k$ are linearly independent and their span is U.

(e) Let U be a $\mathbb{K}$-submodule of M. We say that the list $(v_1, v_2, \ldots, v_k)$ *spans* U if and only if the span of $v_1, v_2, \ldots, v_k$ is U. (More informally, instead of saying "the list $(v_1, v_2, \ldots, v_k)$ *spans* U", we can say "the vectors $v_1, v_2, \ldots, v_k$ *span* U"; of course, this is not the same as saying that each of these k vectors on its own spans U.)

(f) All the terminology we have just introduced depends on $\mathbb{K}$. Whenever the ring $\mathbb{K}$ is not clear from the context, you can insert it into this terminology to make it unambiguous: e.g., say "$\mathbb{K}$-linear combination" instead of "linear combination", and "$\mathbb{K}$-span" instead of "span".

The following proposition gives an equivalent criterion for a list of vectors to be a basis of a $\mathbb{K}$-module:

Proposition 6.11.2. Let M be a $\mathbb{K}$-module. Let $v_1, v_2, \ldots, v_k$ be some vectors in M. Then, $(v_1, v_2, \ldots, v_k)$ is a basis of M if and only if each vector in M can be **uniquely** written in the form (84).[80]

Definition 6.11.3. Let M be a $\mathbb{K}$-module. Then, we say that M is *finitely generated* if there exists a $k \in \mathbb{N}$ and k vectors $v_1, v_2, \ldots, v_k$ that span M.

Finitely generated $\mathbb{K}$-modules are a generalization of finite-dimensional $\mathbb{K}$-vector spaces. A classical result from linear algebra says the following:

Theorem 6.11.4. If $\mathbb{K}$ is a field, then every finitely generated $\mathbb{K}$-module (= $\mathbb{K}$-vector space) has a basis.

A version of Theorem 6.11.4 exists for vector spaces that are not finitely generated; however, stating it would require us to define a more general notion of "basis" that would allow for infinite bases (and even then, this version would require the Axiom of Choice).

Theorem 6.11.4 fails horribly when $\mathbb{K}$ is not a field. For example, the $\mathbb{Z}$-module $\mathbb{Z}/2$ has no basis. Indeed, the only $\mathbb{Z}$-linearly independent list of vectors in $\mathbb{Z}/2$ is the empty list $()$, since any vector in $\mathbb{Z}/2$ becomes 0 when scaled by the nonzero integer 2. More generally, if $\mathbb{K}$ is not a field, then there is a $\mathbb{K}$-module spanned by a single vector that has no basis.

Submodules of $\mathbb{K}^{1\times n}$ fare only somewhat better than arbitrary $\mathbb{K}$-modules in terms of having bases. It can be shown that every $\mathbb{Z}$-submodule of $\mathbb{Z}^{1\times n}$ (or, more generally, of a $\mathbb{Z}$-module that has a basis) must have a basis; thus, Theorem 6.1.5 **(a)** does hold for $\mathbb{K} = \mathbb{Z}$. Theorem 6.1.5 **(a)** also holds for $\mathbb{K} = \mathbb{Z}[i]$. (These facts are particular cases of [ConradS, Theorem 2.1].) However, Theorem 6.1.5 **(a)** does not hold for $\mathbb{K} = \mathbb{Z}\left[\sqrt{-3}\right]$ or for $\mathbb{K} = \mathbb{Z}/4$; in both of these cases, we can find $\mathbb{K}$-submodules **of** $\mathbb{K}$ **itself** that have no basis[81].

Thus, Theorem 6.1.5 **(a)** becomes false when $\mathbb{K}$ is allowed to be an arbitrary ring. The same can be said of parts **(d)** and **(e)** of Theorem 6.1.5; indeed, they become false even for $\mathbb{K} = \mathbb{Z}$, $n = 1$ and $U = \mathbb{Z}^{1\times 1}$. Here are examples of their failure (where, for the sake of simplicity, we are working not in the $\mathbb{Z}$-module $\mathbb{Z}^{1\times 1}$, but in the $\mathbb{Z}$-module $\mathbb{Z}$, which is isomorphic to it):

- The 1-element list (2) of vectors in the $\mathbb{Z}$-module $\mathbb{Z}$ (consisting of just the single vector $2 \in \mathbb{Z}$) is $\mathbb{Z}$-linearly independent (because if $\lambda_1 \in \mathbb{Z}$ satisfies

[80] We say that a vector $v \in M$ can be **uniquely** written in the form (84) if there is a **unique** k-tuple $(\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{K}^k$ satisfying $v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_k v_k$.

[81] If $\mathbb{K} = \mathbb{Z}/4$, then this is easy: Just take the $\mathbb{K}$-submodule $2\mathbb{K} = \{[0]_4, [2]_4\}$ of $\mathbb{K}$; it has no basis, since scaling by 2 sends all of its elements to 0.

If $\mathbb{K} = \mathbb{Z}\left[\sqrt{-3}\right]$, then the subset $\left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z} \text{ satisfying } a \equiv b \mod 2\right\}$ of $\mathbb{K}$ is a $\mathbb{K}$-submodule having no basis. This is closely connected to the fact that division with remainder and unique factorization into primes do not work in the ring $\mathbb{Z}\left[\sqrt{-3}\right]$.

$\lambda_1 \cdot 2 = 0$, then $\lambda_1 = 0$); but you cannot extend it to a basis of $\mathbb{Z}$ (since adding any further vector to it would break linear independence). Thus, Theorem 6.1.5 **(d)** fails for $\mathbb{K} = \mathbb{Z}$, $n = 1$ and $U = \mathbb{Z}^{1\times 1}$.

- The integers 2 and 3 are coprime. Hence, Bezout's theorem says that 1 is a $\mathbb{Z}$-linear combination of 2 and 3. (This can be proven more directly: $1 = 1 \cdot 3 + (-1) \cdot 2$.) This entails that **every** integer is a $\mathbb{Z}$-linear combination of 2 and 3. In other words, the span of the 2-element list $(2, 3)$ of vectors in $\mathbb{Z}$ is $\mathbb{Z}$. But neither of these two vectors alone suffices: The span of the 1-element list (2) is just $\{\text{multiples of } 2\}$, whereas the span of the 1-element list (3) is just $\{\text{multiples of } 3\}$. So the 2-element list $(2, 3)$ spans the $\mathbb{Z}$-module $\mathbb{Z}$, but cannot be "shrunk" to a basis of $\mathbb{Z}$. Therefore, Theorem 6.1.5 **(e)** fails for $\mathbb{K} = \mathbb{Z}$, $n = 1$ and $U = \mathbb{Z}^{1\times 1}$.

Does Theorem 6.1.5 **(b)** survive the generalization from fields to commutative rings? Literally speaking, the answer is "no". Indeed, if $\mathbb{K}$ is the zero ring, then there is only one $\mathbb{K}$-module (namely, $\{0\}$), but it has bases of all sizes (indeed, for each $n \in \mathbb{N}$, the n-element list $(0, 0, \ldots, 0)$ is a basis of this $\mathbb{K}$-module). So two bases of this module can have different sizes.

However, surprisingly, this turns out to be the only counterexample for Theorem 6.1.5 **(b)**! More precisely, Theorem 6.1.5 **(b)** holds whenever the ring $\mathbb{K}$ has more than one element. More generally, we have:

Theorem 6.11.5. Let $\mathbb{K}$ be a commutative ring with $|\mathbb{K}| > 1$. Let U be a $\mathbb{K}$-module. Then, any two bases of U have the same size.

This is much harder to prove than the analogue for fields! There is an argument using determinants.

More generally, Theorem 6.1.5 **(c)** also holds over commutative rings $\mathbb{K}$ such that $|\mathbb{K}| > 1$.

These results and counterexamples illustrate the fact that $\mathbb{K}$-modules (where $\mathbb{K}$ is a commutative ring) are a much richer structure than just $\mathbb{K}^{n\times 1}$'s for $n \in \mathbb{N}$.

6.12. $\mathbb{K}$-submodules from linear maps

We defined the kernel of a matrix; we can similarly define the kernel of a linear map, and a slightly more general notion:

Proposition 6.12.1. Let $\mathbb{K}$ be a commutative ring. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a $\mathbb{K}$-module homomorphism (i.e., a $\mathbb{K}$-linear map).

(a) The set

$$\{v \in M \mid f(v) = 0\}$$

is a $\mathbb{K}$-submodule of M. This set is called the *kernel* of f, and is written $\operatorname{Ker} f$ (or $\ker f$).

(b) Let V be a $\mathbb{K}$-submodule of N. Then, the set

$$\{v \in M \mid f(v) \in V\}$$

is a $\mathbb{K}$-submodule of M. This set is called the *preimage of V under f*, and is written $f^{-1}(V)$.

A second way to construct $\mathbb{K}$-submodules out of linear maps generalizes the column space of a matrix:

Proposition 6.12.2. Let $\mathbb{K}$ be a commutative ring. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a $\mathbb{K}$-module homomorphism (i.e., a $\mathbb{K}$-linear map).
(a) The set $f(M) = \{f(v) \mid v \in M\}$ is a $\mathbb{K}$-submodule of N. This is called the *image* of f.
(b) Let U be a $\mathbb{K}$-submodule of M. Then, the set $f(U) = \{f(v) \mid v \in U\}$ is a $\mathbb{K}$-submodule of N. This is called the *image of U under f*.

How do the kernel and the image of a linear map generalize the kernel and the column space of a matrix? Again, this comes from the correspondence between matrices and linear maps:

Remark 6.12.3. Let $\mathbb{K}$ be a commutative ring. Let $n, m \in \mathbb{N}$. Let $A \in \mathbb{K}^{n \times m}$ be an $n \times m$-matrix. Consider the $\mathbb{K}$-linear map L_A defined in Theorem 6.8.4. Then:
(a) The kernel of the map L_A is the kernel of the matrix A.
(b) The image of the map L_A is the column space of the matrix A.
(Here, we are defining the kernel and the column space of a matrix as we did in Definition 6.1.12 and Definition 6.1.8, but without requiring $\mathbb{K}$ to be a field.)

The reader may wonder, after we have stressed certain parallels between rings and $\mathbb{K}$-modules a few times, whether kernels and images can be defined for ring homomorphisms in the same way as we have defined them for $\mathbb{K}$-module homomorphisms. The answer is "yes", of course (after all, rings also have a 0, just as modules do), but the outcome is perhaps somewhat surprising. First, let us show the analogue of Proposition 6.12.2 for rings:

Proposition 6.12.4. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism.
(a) The set $f(\mathbb{K}) = \{f(v) \mid v \in \mathbb{K}\}$ is a subring of $\mathbb{L}$. This is called the *image* of f.
(b) Let $\mathbb{U}$ be a subring of $\mathbb{K}$. Then, the set $f(\mathbb{U}) = \{f(v) \mid v \in \mathbb{U}\}$ is a subring of $\mathbb{L}$. This is called the *image of $\mathbb{U}$ under f*.

Next, we can define the kernel of a ring homomorphism by imitating Proposition 6.12.1; but this kernel will almost never be a subring (as it will almost never contain 1). Instead, it will be a special sort of subset of $\mathbb{K}$: a so-called *ideal*. Let us define ideals:

Definition 6.12.5. Let $\mathbb{K}$ be a ring. An *ideal* of $\mathbb{K}$ is defined to be a subset I of $\mathbb{K}$ that satisfies the following four conditions:

- The subset I is closed under addition (i.e., we have $a+b \in I$ for all $a \in I$ and $b \in I$).
- The subset I contains $0_{\mathbb{K}}$.
- We have $\lambda a \in I$ for all $\lambda \in \mathbb{K}$ and $a \in I$.
- We have $a\lambda \in I$ for all $\lambda \in \mathbb{K}$ and $a \in I$.

It is easy to see that any ring $\mathbb{K}$ is an ideal of itself; furthermore, the 1-element subset $\{0_{\mathbb{K}}\}$ of $\mathbb{K}$ is an ideal of $\mathbb{K}$ as well. But there can be many further ideals:

Example 6.12.6. Let $\mathbb{K}$ be a commutative ring. Let $u \in \mathbb{K}$. Then, the subset

$$u\mathbb{K} := \{uz \mid z \in \mathbb{K}\}$$

of $\mathbb{K}$ is an ideal of $\mathbb{K}$. Such an ideal is called a *principal ideal*. Note that $\{0_{\mathbb{K}}\}$ is a principal ideal (since $\{0_{\mathbb{K}}\} = 0\mathbb{K}$), and $\mathbb{K}$ itself is a principal ideal (since $\mathbb{K} = 1\mathbb{K}$).

Let us see what this results in for some specific rings $\mathbb{K}$:

- The principal ideals of the ring $\mathbb{Z}$ are the subsets $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\} = \{\text{all multiples of } n\}$ with $n \in \mathbb{Z}$. For example, $2\mathbb{Z} = \{\text{all even numbers}\}$ is an ideal of $\mathbb{Z}$. It is not hard to show that all ideals of $\mathbb{Z}$ are principal ideals.
- It can also be shown that all ideals of $\mathbb{Z}[i]$ are principal ideals. The same holds for $\mathbb{D}$ (the ring of dual numbers), for $\mathbb{Z}\left[\sqrt{-2}\right]$ (the ring of "2-Gaussian integers"), and $\mathbb{Q}[x]$ (the ring of polynomials with rational coefficients, to be formally defined in Definition 7.4.10 below).
- However, there exist some rings that have non-principal ideals as well. For example, if $\mathbb{K}$ is the ring $\mathbb{Z}\left[\sqrt{-3}\right]$, then the subset $\left\{a+b\sqrt{-3} \mid a,b \in \mathbb{Z} \text{ satisfying } a \equiv b \mod 2\right\}$ of $\mathbb{K}$ is an ideal but not a principal ideal. For another example, if $\mathbb{K}$ is the ring $\mathbb{Z}[x]$ (the ring of polynomials with integer coefficients, to be formally defined in Definition 7.4.10 below), then the subset of $\mathbb{K}$ consisting of all polynomials with even constant term is an ideal but not a principal ideal.

When $\mathbb{K}$ is a commutative ring, the third and fourth conditions in Definition 6.12.5 actually say the same thing (because $\lambda a = a\lambda$ for all $\lambda \in \mathbb{K}$ and $a \in \mathbb{K}$). From this, it is not hard to see the following:

Proposition 6.12.7. Let $\mathbb{K}$ be a commutative ring. Then, an ideal of $\mathbb{K}$ is the same thing as a $\mathbb{K}$-submodule of $\mathbb{K}$. (Remember that $\mathbb{K}$ itself is a $\mathbb{K}$-module!).

Now, we can state an analogue of Proposition 6.12.1 is the following:

Proposition 6.12.8. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism.

(a) The set

$$\{v \in \mathbb{K} \mid f(v) = 0\}$$

is an ideal of $\mathbb{K}$. This set is called the *kernel* of f, and is written $\operatorname{Ker} f$ (or $\ker f$).

(b) Let V be an ideal of $\mathbb{L}$. Then, the set

$$\{v \in \mathbb{K} \mid f(v) \in V\}$$

is an ideal of $\mathbb{K}$. This set is called the *preimage of V under f*, and is written $f^{-1}(V)$.

So the kernel of a ring homomorphism is always an ideal. (And conversely, every ideal can be written as the kernel of a ring homomorphism; this will follow from Proposition 8.2.6 **(g)** further below.)

Kernels can also help in checking whether a ring homomorphism or a module homomorphism is injective. To wit, for ring homomorphisms, the following criterion for injectivity holds:

Proposition 6.12.9. Let $\mathbb{K}$ and $\mathbb{L}$ be two rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism. Then, f is injective if and only if $\operatorname{Ker} f = \{0_{\mathbb{K}}\}$.

An analogous statement holds for $\mathbb{K}$-module homomorphisms:

Proposition 6.12.10. Let M and N be two $\mathbb{K}$-modules. Let $f : M \to N$ be a $\mathbb{K}$-module homomorphism (i.e., a $\mathbb{K}$-linear map). Then, f is injective if and only if $\operatorname{Ker} f = \{0_M\}$.

A curious (and useful) consequence of Proposition 6.12.9 is the following property of fields:

Corollary 6.12.11. Let $\mathbb{K}$ be a field, and let $\mathbb{L}$ be a ring such that $\mathbb{L}$ is not trivial (i.e., we have $|\mathbb{L}| > 1$). Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism. Then, f is injective.

7. Polynomials and formal power series

7.1. Motivation

Back in our proof of Theorem 2.17.14, we have used a vague notion of polynomials. Let us try and formalize this notion. While at that, we shall also try to generalize it

from polynomials with rational coefficients to polynomials with coefficients in an arbitrary commutative ring.

The most "naive" notion of polynomials is that of a polynomial function:

Definition 7.1.1. Let $\mathbb{K}$ be a commutative ring. A function $f : \mathbb{K} \to \mathbb{K}$ is said to be a *polynomial function* if there exist some elements $a_0, a_1, \ldots, a_n \in \mathbb{K}$ such that every $u \in \mathbb{K}$ satisfies

$$f(u) = a_0 u^0 + a_1 u^1 + \cdots + a_n u^n.$$

For example, the function

$$\mathbb{R} \to \mathbb{R}, \qquad u \mapsto 6u^3 - \frac{1}{2}u + \sqrt{3}$$

is a polynomial function.

Definition 7.1.1 has its uses. In particular, when you are working with real or complex numbers, it is sufficient for most of what you would want from a polynomial. (This is why numerous authors, particularly with backgrounds in analysis, simply define a polynomial to be a polynomial function.) But when we want polynomials with coefficients from other rings, this definition starts showing weaknesses. In what sense?

Here is an example. In Section 5.6, we constructed a field with 4 elements by adjoining a j satisfying $j^2 = j + 1$ to $\mathbb{Z}/2$. In other words, we adjoined a root of "the polynomial $x^2 - x - 1$" (whatever this may mean) to $\mathbb{Z}/2$. It would be helpful to generalize this: How can we adjoin a root of a polynomial to a ring? In particular, if we can do this with polynomials of higher degree than 2, we may hope to be able to construct larger finite fields. For example, how do we find a field of size 8 ? We would hope to get it by adjoining to $\mathbb{Z}/2$ a root of a degree-3 polynomial.

So we need a notion of polynomials over $\mathbb{Z}/2$, and we need there to be infinitely many of them, ideally at least one of each degree. With polynomial functions, we cannot get this. In fact, there are only 4 functions from $\mathbb{Z}/2$ to $\mathbb{Z}/2$.

Even for our above construction of a field with 4 elements, polynomial functions are not suited. In fact, the polynomial function

$$\mathbb{Z}/2 \to \mathbb{Z}/2, \qquad x \mapsto x^2 - x - 1$$

is actually just the constant-1 function. So when we adjoined a root of this polynomial, did we just adjoin a root of 1 ? Hardly. (A root of 1 would be a j satisfying $1 = 0$; "adjoining" such a thing would yield the zero ring, not a field with 4 elements.)

The moral of the story for now is that when we adjoin a root of a polynomial to a field, we certainly are not adjoining a root of a polynomial function. So we have at least one reason to want a concept of polynomials that is finer than that of polynomial functions.

Here is another reason: Polynomial functions from $\mathbb{K}$ to $\mathbb{K}$ can only be applied to elements of $\mathbb{K}$ (because they are defined as functions from $\mathbb{K}$), but we want a notion of polynomials that can be applied to more general things (such as square matrices or other polynomials).

For example, in linear algebra, it is extremely useful to apply polynomials to square matrices. With polynomial functions, this makes no sense: A polynomial function over $\mathbb{R}$ is defined only on $\mathbb{R}$, so how can you apply it to a 2×2-matrix? Once again, the discrepancy becomes the most obvious over a finite field: The two polynomial functions $\mathbb{Z}/2 \to \mathbb{Z}/2,\ x \mapsto x^2$ and $\mathbb{Z}/2 \to \mathbb{Z}/2,\ x \mapsto x$ are identical (since $x^2 = x$ for all $x \in \mathbb{Z}/2$); but the matrix $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in (\mathbb{Z}/2)^{2\times 2}$ does not satisfy $A^2 = A$. So if there was a way to apply these two identical polynomial functions to A, then we should obtain two different results, which is absurd. Thus, it makes no sense to apply a polynomial function $\mathbb{Z}/2 \to \mathbb{Z}/2$ to a square matrix over $\mathbb{Z}/2$.

Hence, we need a finer definition of a polynomial which doesn't just remember its values on the elements of $\mathbb{K}$, but remembers all its coefficients. So we need to bake the coefficients into the definition.

We already gave a hint of such a definition in Subsection 2.17.3, where we said that a polynomial (in 1 variable x, with rational coefficients) is an "expression" (whatever this means) of the form $a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$, where $a_k, a_{k-1}, \ldots, a_0$ are (fixed) rational numbers and where x is an "indeterminate" (a symbol that itself does not stand for a number, but we can substitute a number for). This was vague (what exactly is an "expression"?) but a step in the right direction. We can, of course, generalize this informal definition to an arbitrary commutative ring $\mathbb{K}$ by replacing "rational numbers" by "elements of $\mathbb{K}$". But how do we make the notion of "expression" rigorous?

The idea is to forget (at first) about the specific form of the expression $a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ and simply store the coefficients $a_0, a_1, \ldots, a_k$ appearing in it in a list.

For example, let us consider polynomials of degree ≤ 1 over $\mathbb{R}$. These always have the form $a_0 + a_1 x$ (with $a_0, a_1 \in \mathbb{R}$), so we can simply define them as **pairs** (a_0, a_1) of real numbers a_0 and a_1. (This is analogous to Definition 4.1.1, where we defined complex numbers as pairs of real numbers rather than trying to treat them as "expressions involving i".) Next, we define an addition operation $+$ on polynomials of degree ≤ 1 by setting

$$(a_0, a_1) + (b_0, b_1) = (a_0 + b_0, a_1 + b_1),$$

which of course imitates the informal computation

$$(a_0 + a_1 x) + (b_0 + b_1 x) = (a_0 + b_0) + (a_1 + b_1)\, x.$$

Furthermore, we define a multiplication on these polynomials by setting

$$(a_0, a_1) \cdot (b_0, b_1) = (a_0 b_0, a_0 b_1 + a_1 b_0, a_1 b_1),$$

which imitates the "FOIL" rule

$$(a_0 + a_1 x) \cdot (b_0 + b_1 x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)\, x + a_1 b_1 x^2.$$

However, this multiplication yields a triple, not a pair, so it is not a binary operation. So our polynomials of degree ≤ 1 do not form a ring; their multiplication takes us out of their set.

We can likewise consider polynomials of degree ≤ 2, which can be defined as triples (a_0, a_1, a_2), but then multiplication yields a 5-tuple rather than a triple.

More generally: For each $n \in \mathbb{N}$, we can define polynomials of degree $\leq n$ as $(n+1)$-tuples $(a_0, a_1, \ldots, a_n)$, and define addition and multiplication on them, but the multiplication will result in $(2n+1)$-tuples rather than $(n+1)$-tuples.

Hence, if we want to define polynomials in such a way that they form a ring, we should define them not as pairs or triples or $(n+1)$-tuples, but rather as infinite sequences. In other words, we should define a polynomial as an infinite sequence $(a_0, a_1, a_2, \ldots)$, which will encode the "expression" $a_0 + a_1 x + a_2 x^2 + \cdots$. However, not every sequence stands for a polynomial; after all, we want polynomials to be **finite** expressions, so the sum $a_0 + a_1 x + a_2 x^2 + \cdots$ needs to be finite (in the sense that all but finitely many of its addends are 0) in order for it to qualify as a polynomial. Thus, our polynomials should be defined as infinite sequences $(a_0, a_1, a_2, \ldots)$ that have only finitely many nonzero entries.

An upside of this strategy is that with such a definition, we get a second object for free: the *formal power series*. Those are just going to be **all** infinite sequences $(a_0, a_1, a_2, \ldots)$, including the ones that have infinitely many nonzero entries. We will see that the same rules by which we define addition and multiplication of polynomials can be used to define these operations on formal power series.

7.2. The definition of formal power series and polynomials

Let us now explicitly state the definitions we have been working towards. We shall only define polynomials (and formal power series) in 1 indeterminate; there is a version that involves multiple indeterminates, but for now we restrict ourselves to one.

Convention 7.2.1. For the rest of this chapter, we fix a commutative ring $\mathbb{K}$.

Definition 7.2.2. **(a)** A *formal power series* (in 1 indeterminate over $\mathbb{K}$) is defined to be a sequence $(a_0, a_1, a_2, \ldots) = (a_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$ of elements of $\mathbb{K}$.

We abbreviate the words "formal power series" as "*FPS*".

We let $\mathbb{K}[[x]]$ be the set of all FPSs.

(b) A *polynomial* (in 1 indeterminate over $\mathbb{K}$) is defined to be an FPS $(a_0, a_1, a_2, \ldots)$ such that

$$\text{all but finitely many } i \in \mathbb{N} \text{ satisfy } a_i = 0$$

(that is, only finitely many $i \in \mathbb{N}$ satisfy $a_i \neq 0$).

We let $\mathbb{K}[x]$ be the set of all polynomials.

So far, our FPSs are just sequences, with no other meaning. We will later see why they can be viewed as "power series", what the x in "$\mathbb{K}[[x]]$" means, and why we can write a sequence $(a_0, a_1, a_2, \ldots)$ as $a_0 + a_1 x + a_2 x^2 + \cdots$.

First, let us give two examples to illustrate the above definition:

Example 7.2.3. In this example, let $\mathbb{K} = \mathbb{Z}$.

(a) The sequence $(1, 2, 3, 4, 5, \ldots)$ is an FPS, but not a polynomial. We will later write this FPS as $1 + 2x + 3x^2 + 4x^3 + 5x^4 + \cdots$.

(b) The sequence $\left(3, 0, 2, 5, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}}\right)$ is a polynomial. We will later write this polynomial as $3 + 2x^2 + 5x^3$.

Definition 7.2.4. The goal of this definition is to make $\mathbb{K}[[x]]$ into a $\mathbb{K}$-algebra.

(a) We define a binary operation $+$ (called *addition*) on $\mathbb{K}[[x]]$ by

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots).$$

(That is, we define an entrywise addition.)

(b) We define a scaling map $\cdot : \mathbb{K} \times \mathbb{K}[[x]] \to \mathbb{K}[[x]]$ by

$$\lambda (a_0, a_1, a_2, \ldots) = (\lambda a_0, \lambda a_1, \lambda a_2, \ldots).$$

(That is, we define an entrywise scaling.)

(c) We define a binary operation $\cdot$ (called *multiplication*) on $\mathbb{K}[[x]]$ by

$$(a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots),$$

where

$$c_n = \sum_{i=0}^{n} a_i b_{n-i} = \sum_{\substack{i,j \in \mathbb{N}; \\ i+j=n}} a_i b_j = a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 \qquad \text{for all } n \in \mathbb{N}.$$

(d) For each $a \in \mathbb{K}$, we define an FPS $\underline{a} \in \mathbb{K}[[x]]$ by

$$\underline{a} = \left(a, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right).$$

This is called a *constant* FPS.

For example,

$$\begin{aligned}
(0,1,2,3,4,\ldots)+(1,1,1,1,1,\ldots) &= (1,2,3,4,5,\ldots) && \text{and} \\
(1,1,1,1,1,\ldots)+(1,1,1,1,1,\ldots) &= (2,2,2,2,2,\ldots) && \text{and} \\
8\cdot(1,1,1,1,1,\ldots) &= (8,8,8,8,8,\ldots) && \text{and} \\
(1,1,1,1,1,\ldots)\cdot(1,1,1,1,1,\ldots) &= (1,2,3,4,5,\ldots) && \text{and} \\
\left(1,-1,\underbrace{0,0,0,\ldots}_{\text{zeroes}}\right)\cdot(1,1,1,1,1,\ldots) &= \left(1,\underbrace{0,0,0,\ldots}_{\text{zeroes}}\right) = \underline{1}. && (85)
\end{aligned}$$

Theorem 7.2.5. **(a)** Equip the set $\mathbb{K}[[x]]$ with the addition $+$ defined in Definition 7.2.4 **(a)**, the multiplication $\cdot$ defined in Definition 7.2.4 **(c)**, the scaling $\cdot$ defined in Definition 7.2.4 **(b)**, the zero $\underline{0}$ and the unity $\underline{1}$. Then, $\mathbb{K}[[x]]$ is a $\mathbb{K}$-algebra, a commutative ring and a $\mathbb{K}$-module.

(b) The subtraction $-$ that comes from the $\mathbb{K}$-algebra structure on $\mathbb{K}[[x]]$ is entrywise; in other words, any two FPSs $(a_0,a_1,a_2,\ldots)$ and $(b_0,b_1,b_2,\ldots)$ satisfy

$$(a_0,a_1,a_2,\ldots)-(b_0,b_1,b_2,\ldots)=(a_0-b_0,a_1-b_1,a_2-b_2,\ldots).$$

(c) We have

$$\lambda\mathbf{a}=\underline{\lambda}\cdot\mathbf{a} \qquad \text{for each } \lambda\in\mathbb{K} \text{ and } \mathbf{a}\in\mathbb{K}[[x]].$$

(d) Consider the map

$$\begin{aligned}
\iota:\mathbb{K}&\to\mathbb{K}[[x]],\\
a&\mapsto\underline{a}
\end{aligned}$$

(sending each element $a\in\mathbb{K}$ to the corresponding constant FPS $\underline{a}=\left(a,\underbrace{0,0,0,\ldots}_{\text{zeroes}}\right)$). This map ι is a $\mathbb{K}$-algebra homomorphism[82].

Before we outline a proof of this theorem, let us introduce a helpful notation (used often in enumerative combinatorics):

Definition 7.2.6. Let $n\in\mathbb{N}$. Let $\mathbf{a}=(a_0,a_1,a_2,\ldots)\in\mathbb{K}[[x]]$. Then, we define an element $[x^n]\,\mathbf{a}\in\mathbb{K}$ by

$$[x^n]\,\mathbf{a}=a_n.$$

This element $[x^n]\,\mathbf{a}$ is called *the coefficient of x^n in* $\mathbf{a}$, or the *n-th coefficient* of $\mathbf{a}$. (The letter "x" is so far considered just as a symbolic part of this notation, with no standalone meaning.)

[82] Recall that the notion of a $\mathbb{K}$-algebra homomorphism was introduced in Definition 6.9.5; it means "map that is a ring homomorphism and a $\mathbb{K}$-module homomorphism at the same time".

Be careful with this notation: What you would normally call "the first entry" of the sequence $(a_0, a_1, a_2, \ldots)$ is called its 0-th (not 1-st) coefficient.

Example 7.2.7. We have $\left[x^0\right](1,2,3,4,5,\ldots) = 1$ and $\left[x^3\right](1,2,3,4,5,\ldots) = 4$.

Definition 7.2.6 has a tautological consequence: Each FPS $\mathbf{a}$ satisfies

$$\mathbf{a} = \left(\left[x^0\right]\mathbf{a}, \left[x^1\right]\mathbf{a}, \left[x^2\right]\mathbf{a}, \ldots\right). \tag{86}$$

Thus, an FPS $\mathbf{a}$ is uniquely determined by its coefficients $\left[x^0\right]\mathbf{a}, \left[x^1\right]\mathbf{a}, \left[x^2\right]\mathbf{a}, \ldots$. Hence, if two FPSs $\mathbf{a}$ and $\mathbf{b}$ satisfy $[x^n]\,\mathbf{a} = [x^n]\,\mathbf{b}$ for all $n \in \mathbb{N}$, then $\mathbf{a} = \mathbf{b}$.

The definition of the sum of two FPSs (Definition 7.2.4 **(a)**) rewrites as follows:

$$[x^n](\mathbf{a}+\mathbf{b}) = [x^n]\,\mathbf{a} + [x^n]\,\mathbf{b} \qquad \text{for all } \mathbf{a},\mathbf{b} \in \mathbb{K}[[x]] \text{ and } n \in \mathbb{N}. \tag{87}$$

(Here, the expression "$[x^n]\,\mathbf{a} + [x^n]\,\mathbf{b}$" should be read as "$([x^n]\,\mathbf{a}) + ([x^n]\,\mathbf{b})$".) Furthermore, the definition of scaling on FPSs (Definition 7.2.4 **(b)**) rewrites as follows:

$$[x^n](\lambda\mathbf{a}) = \lambda \cdot [x^n]\,\mathbf{a} \qquad \text{for all } \lambda \in \mathbb{K} \text{ and } \mathbf{a} \in \mathbb{K}[[x]] \text{ and } n \in \mathbb{N}. \tag{88}$$

Moreover, the definition of the product of two FPSs (Definition 7.2.4 **(c)**) rewrites as follows:

$$[x^n](\mathbf{ab}) = \sum_{i=0}^{n} \left(\left[x^i\right]\mathbf{a}\right) \cdot \left(\left[x^{n-i}\right]\mathbf{b}\right) \tag{89}$$

$$= \sum_{\substack{i,j\in\mathbb{N};\\ i+j=n}} \left(\left[x^i\right]\mathbf{a}\right) \cdot \left(\left[x^j\right]\mathbf{b}\right) \tag{90}$$

$$= \left(\left[x^0\right]\mathbf{a}\right) \cdot ([x^n]\,\mathbf{b}) + \left(\left[x^1\right]\mathbf{a}\right) \cdot \left(\left[x^{n-1}\right]\mathbf{b}\right) + \cdots + ([x^n]\,\mathbf{a}) \cdot \left(\left[x^0\right]\mathbf{b}\right)$$
$$\text{for all } \mathbf{a},\mathbf{b} \in \mathbb{K}[[x]] \text{ and } n \in \mathbb{N}.$$

Thus, any $\mathbf{a}, \mathbf{b} \in \mathbb{K}[[x]]$ and $n \in \mathbb{N}$ satisfy

$$[x^n](\mathbf{ab}) = \sum_{i=0}^{n} \left(\left[x^i\right]\mathbf{a}\right) \cdot \left(\left[x^{n-i}\right]\mathbf{b}\right)$$
$$= \sum_{j=0}^{n} \left(\left[x^{n-j}\right]\mathbf{a}\right) \cdot \left(\left[x^j\right]\mathbf{b}\right) \tag{91}$$

(here, we have substituted $n-j$ for i in the sum). Applying (89) to $n = 0$, we conclude that

$$\left[x^0\right](\mathbf{ab}) = \sum_{i=0}^{0} \left(\left[x^i\right]\mathbf{a}\right) \cdot \left(\left[x^{0-i}\right]\mathbf{b}\right) = \left(\left[x^0\right]\mathbf{a}\right) \cdot \left(\left[x^{0-0}\right]\mathbf{b}\right)$$
$$= \left(\left[x^0\right]\mathbf{a}\right) \cdot \left(\left[x^0\right]\mathbf{b}\right) \tag{92}$$

for all $\mathbf{a}, \mathbf{b} \in \mathbb{K}[[x]]$. (But of course, $[x^n](\mathbf{ab})$ is not generally equal to $([x^n]\mathbf{a}) \cdot ([x^n]\mathbf{b})$ when $n > 0$.)

Finally, using the Iverson bracket notation (introduced in Exercise 2.17.2), we can rewrite the definition of the constant FPSs $\underline{a}$ (Definition 7.2.4 **(d)**) as follows:

$$[x^n](\underline{a}) = \begin{cases} a, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases} \tag{93}$$

$$= \underbrace{\begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases}}_{=[n=0]} \cdot a$$

$$= [n = 0] \cdot a \qquad \text{for all } a \in \mathbb{K} \text{ and } n \in \mathbb{N}. \tag{94}$$

We are now ready to prove Theorem 7.2.5:

Convention 7.2.8. From now on, we shall identify each $a \in \mathbb{K}$ with the FPS $\underline{a} = (a, 0, 0, 0, \ldots) \in \mathbb{K}[[x]]$.

This identification is harmless, due to Theorem 7.2.5 **(d)** and to the fact that the map

$$\begin{aligned} \iota : \mathbb{K} &\to \mathbb{K}[[x]], \\ a &\mapsto \underline{a} \end{aligned}$$

is injective (since $a = \left[x^0\right](\underline{a})$ for all $a \in \mathbb{K}$). Note that if $a \in \mathbb{K}$, then the FPS $\underline{a}$ is actually a polynomial (since $\underline{a} = (a, 0, 0, 0, 0, \ldots)$ has at most one nonzero entry), i.e., belongs to $\mathbb{K}[x]$.

The identification we have made in Convention 7.2.8 turns $\mathbb{K}$ into a subset of $\mathbb{K}[[x]]$, and more precisely into a $\mathbb{K}$-subalgebra of $\mathbb{K}[[x]]$ (by Theorem 7.2.5 **(d)**).

Theorem 7.2.5 shows that $\mathbb{K}[[x]]$ is a $\mathbb{K}$-algebra and a commutative ring, so that differences, powers, finite sums, and finite products of FPSs are well-defined. But more can be said. Indeed, sometimes, infinite sums of FPSs make sense. For example, it is reasonable to write

$$\begin{aligned} &(1, 1, 1, 1, 1, \ldots) \\ &+ (0, 1, 1, 1, 1, \ldots) \\ &+ (0, 0, 1, 1, 1, \ldots) \\ &+ (0, 0, 0, 1, 1, \ldots) \\ &+ (0, 0, 0, 0, 1, \ldots) \\ &+ \cdots \\ &= (1, 2, 3, 4, 5, \ldots), \end{aligned}$$

even though the sum on the left hand side has infinitely many nonzero[83] addends! The addition of $\mathbb{K}[[x]]$ is entrywise, so it stands to reason that infinite sums of

[83] As usual, "nonzero" means "different from $0_{\mathbb{K}[[x]]} = (0, 0, 0, 0, \ldots)$".

FPSs should be defined entrywise as well, and whenever such entrywise sums are well-defined, it makes sense to call them the sum of the FPSs. Thus, we make the following definition:

Definition 7.2.9. A (possibly infinite) family $(\mathbf{a}_i)_{i\in I}$ of FPSs (where I is an arbitrary set) is called *summable* if for each $n \in \mathbb{N}$, the following requirement holds:

$$\text{only finitely many } i \in I \text{ satisfy } [x^n](\mathbf{a}_i) \neq 0. \tag{95}$$

In this case, the *sum* $\sum_{i\in I} \mathbf{a}_i$ of the family $(\mathbf{a}_i)_{i\in I}$ is defined as the FPS whose coefficients are given by

$$[x^n]\left(\sum_{i\in I} \mathbf{a}_i\right) = \sum_{i\in I} [x^n](\mathbf{a}_i) \qquad \text{for all } n \in \mathbb{N}.$$

(The sum on the right hand side of this equality is well-defined in $\mathbb{K}$, since it is a sum with only finitely many nonzero addends.)

We notice that the condition (95) is **not** equivalent to saying "infinitely many $i \in I$ satisfy $[x^n](\mathbf{a}_i) = 0$".

Remark 7.2.10. If you work in constructive logic, you should read the condition (95) as "all but finitely many $i \in I$ satisfy $[x^n](\mathbf{a}_i) = 0$" (that is, "there exists a finite subset S of I such that each $i \in I \setminus S$ satisfies $[x^n](\mathbf{a}_i) = 0$").

Proposition 7.2.11. Sums of summable families of FPSs satisfy the usual rules for summation, as long as all families involved are summable. For example:

- If $(\mathbf{a}_i)_{i\in I}$ and $(\mathbf{b}_i)_{i\in I}$ are two summable families of FPSs, then the family $(\mathbf{a}_i + \mathbf{b}_i)_{i\in I}$ is summable as well and its sum is
$$\sum_{i\in I} (\mathbf{a}_i + \mathbf{b}_i) = \sum_{i\in I} \mathbf{a}_i + \sum_{i\in I} \mathbf{b}_i.$$
- If $(\mathbf{a}_i)_{i\in I}$ is a summable family of FPSs, and if J is a subset of I, then the families $(\mathbf{a}_i)_{i\in J}$ and $(\mathbf{a}_i)_{i\in I\setminus J}$ are summable as well and we have
$$\sum_{i\in I} \mathbf{a}_i = \sum_{i\in J} \mathbf{a}_i + \sum_{i\in I\setminus J} \mathbf{a}_i.$$
- The family $(0)_{i\in I}$ (where 0 stands for the FPS $0_{\mathbb{K}[[x]]}$) is always summable (no matter how large I is), and its sum is $\sum_{i\in I} 0 = 0$.
- If $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is a summable family of FPSs indexed by **pairs** $(i,j) \in I \times J$, then
$$\sum_{i\in I}\sum_{j\in J} \mathbf{a}_{i,j} = \sum_{(i,j)\in I\times J} \mathbf{a}_{i,j} = \sum_{j\in J}\sum_{i\in I} \mathbf{a}_{i,j}. \tag{96}$$

Remark 7.2.12. Caveat: The equality (96) implies, in particular, that the summation signs $\sum\limits_{i\in I}$ and $\sum\limits_{j\in J}$ can be interchanged. However, the condition that the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is summable is needed for this! If we drop this condition, and merely require the (weaker!) condition that all the families $\left(\mathbf{a}_{i,j}\right)_{j\in J}$ (for each fixed i), $\left(\mathbf{a}_{i,j}\right)_{i\in I}$ (for each fixed j), $\left(\sum\limits_{j\in J}\mathbf{a}_{i,j}\right)_{i\in I}$ and $\left(\sum\limits_{i\in I}\mathbf{a}_{i,j}\right)_{j\in J}$ are summable, then the equality

$$\sum_{i\in I}\sum_{j\in J}\mathbf{a}_{i,j}=\sum_{j\in J}\sum_{i\in I}\mathbf{a}_{i,j} \tag{97}$$

may be false. For an example where it is false, consider the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ with $I=\{1,2,3,\ldots\}$ and $J=\{1,2,3,\ldots\}$ and $\mathbf{a}_{i,j}$ given by the following table:

$\mathbf{a}_{i,j}$	1	2	3	4	5	$\cdots$
1	1	-1				$\cdots$
2		1	-1			$\cdots$
3			1	-1		$\cdots$
4				1	-1	$\cdots$
5					1	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

(where all the entries not shown are 0). Note that the elements of this family belong to $\mathbb{K}$, and thus can be considered as FPSs via Convention 7.2.8. For this specific family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$, the equality (97) rewrites as $0=1$, which is not a good sign. But this does not contradict the rule (96), since the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is not summable (it contains infinitely many 1's).

The upshot of this caveat is that if you want to interchange two summation signs as in (97), you must check not only that the sums involved are all well-defined, but also that the sum $\sum\limits_{(i,j)\in I\times J}\mathbf{a}_{i,j}$ is well-defined (i.e., the family $\left(\mathbf{a}_{i,j}\right)_{(i,j)\in I\times J}$ is summable). This is automatically satisfied when the sets I and J are finite, but in the case of infinite sets can be a serious restriction as we have just seen.

We shall use standard notations for infinite sums over certain subsets of $\mathbb{Z}$. For instance, the summation sign "$\sum\limits_{i=0}^{\infty}$" shall mean "$\sum\limits_{i\in\mathbb{N}}$"; more generally, if $a\in\mathbb{Z}$, then the summation sign "$\sum\limits_{i=a}^{\infty}$" shall mean "$\sum\limits_{i\in\{a,a+1,a+2,\ldots\}}$". Also, the summation sign

"$\sum\limits_{i>0}$" shall mean "$\sum\limits_{i=1}^{\infty}$", which is the same as "$\sum\limits_{i\in\{1,2,3,\ldots\}}$".

Definition 7.2.13. We let x denote the FPS $\left(0, 1, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}}\right)$.

Thus, we have

$$\left[x^1\right] x = 1, \qquad \text{and} \tag{98}$$

$$[x^n]\, x = 0 \qquad \text{for all } n \in \mathbb{N} \text{ satisfying } n \neq 1. \tag{99}$$

In other words, for all $n \in \mathbb{N}$, we have

$$[x^n]\, x = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n \neq 1 \end{cases} \tag{100}$$

$$= \underbrace{\begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{if } n \neq 1 \end{cases}}_{=[n=1]} \cdot 1_{\mathbb{K}} = [n = 1] \cdot 1_{\mathbb{K}} \tag{101}$$

(using the Iverson bracket notation).

Lemma 7.2.14. Let $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]]$ be an FPS. Then,

$$x\,(a_0, a_1, a_2, \ldots) = (0, a_0, a_1, a_2, \ldots).$$

In other words, Lemma 7.2.14 says that multiplying an FPS by x shifts all entries of the FPS to the right by 1 step, while filling the now-empty 0-th slot with a 0.

Proposition 7.2.15. For each $k \in \mathbb{N}$, we have

$$x^k = \left(\underbrace{0, 0, \ldots, 0}_{k \text{ zeroes}}, 1, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}}\right).$$

Proposition 7.2.15 can be restated as follows:

$$[x^n]\left(x^k\right) = \begin{cases} 1, & \text{if } n = k; \\ 0, & \text{if } n \neq k \end{cases} \qquad \text{for all } n, k \in \mathbb{N}. \tag{102}$$

Corollary 7.2.16. Let $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]]$ be any FPS. Then, the family $\left(a_k x^k\right)_{k \in \mathbb{N}}$ is summable, so that the sum $\sum_{k \in \mathbb{N}} a_k x^k$ is well-defined. Moreover,

$$(a_0, a_1, a_2, \ldots) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots = \sum_{k \in \mathbb{N}} a_k x^k.$$

So now we are justified in computing "formally" with FPSs as if they were infinite sums of powers of x times scalars, because we have now constructed a ring with an actual element x in it and we have shown that these infinite sums are well-defined and just encode the sequences of their coefficients. This is the rigorous answer to the question "what is an indeterminate in a polynomial or FPS". This also explains why we refer to the entries of an FPS $(a_0, a_1, a_2, \ldots)$ as its "coefficients".

Exercise 7.2.1. Let $\mathbf{b} \in \mathbb{K}[[x]]$ and $u, v \in \mathbb{N}$. Prove the following:
(a) If $u \geq v$, then $[x^u](x^v \mathbf{b}) = [x^{u-v}]\,\mathbf{b}$.
(b) If $u < v$, then $[x^u](x^v \mathbf{b}) = 0$.

7.3. Inverses in the ring $\mathbb{K}[[x]]$

7.3.1. The invertibility criterion for power series

The equation (85) is not just an example of multiplying two FPSs. It is also an example of a multiplicative inverse in the ring $\mathbb{K}[[x]]$. Indeed, we can rewrite it as

$$(1 - x) \cdot \left(1 + x + x^2 + x^3 + \cdots\right) = \underline{1}$$

(since $\left(1, -1, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) = 1 - x$ and $(1, 1, 1, 1, 1, \ldots) = 1 + x + x^2 + x^3 + \cdots$).
Since the ring $\mathbb{K}[[x]]$ is commutative, we also have $(1 - x) \cdot \left(1 + x + x^2 + x^3 + \cdots\right) = \left(1 + x + x^2 + x^3 + \cdots\right) \cdot (1 - x)$. Thus,

$$(1 - x) \cdot \left(1 + x + x^2 + x^3 + \cdots\right) = \left(1 + x + x^2 + x^3 + \cdots\right) \cdot (1 - x) = \underline{1}.$$

Since $\underline{1}$ is the unity $1_{\mathbb{K}[[x]]}$ of the ring $\mathbb{K}[[x]]$, we thus conclude that the FPS $1 + x + x^2 + x^3 + \cdots$ is a multiplicative inverse of $1 - x$. Thus, the FPS $1 - x$ is invertible, and its multiplicative inverse is

$$\frac{1}{1 - x} = 1 + x + x^2 + x^3 + \cdots.$$

This, of course, looks exactly like the well-known geometric series formula from analysis, which states that $\dfrac{1}{1 - r} = 1 + r + r^2 + r^3 + \cdots$ for each real $r \in (-1, 1)$.

But keep in mind that our x is an indeterminate over an arbitrary commutative ring, while the r in the latter formula is a real number between -1 and 1; there are ways to transfer identities between these two worlds, but they are not a-priori the same.

Thus we have seen that $1-x$ is an invertible FPS. Let us ask a more general question: When is an FPS invertible? Quite often, as it turns out:

Theorem 7.3.1. Let $\mathbf{a} \in \mathbb{K}[[x]]$. Then, $\mathbf{a}$ is invertible (in the ring $\mathbb{K}[[x]]$) if and only if the coefficient $[x^0]\,\mathbf{a}$ is invertible in $\mathbb{K}$.

7.3.2. Newton's binomial formula

In Definition 4.1.19, we have defined negative powers (i.e., powers of the form α^n with n being a negative integer) of any nonzero complex number α. All that we needed from α in that definition was that α has a multiplicative inverse α^{-1}. Thus, we can straightforwardly extend this definition to any invertible element α of any ring:

Definition 7.3.2. Let $\mathbb{L}$ be a ring. Let $\alpha \in \mathbb{L}$ be invertible. For any negative $n \in \mathbb{Z}$, we define an element $\alpha^n \in \mathbb{L}$ (called the *n-th power of α*) by $\alpha^n = \left(\alpha^{-1}\right)^{-n}$. (This is well-defined, since $\left(\alpha^{-1}\right)^{-n}$ is already defined by Definition 5.4.10 (because n is negative and thus $-n \in \mathbb{N}$).)

When the ring $\mathbb{L}$ is commutative, the powers of its elements satisfy the same rules as the powers of complex numbers (see Proposition 4.1.20), except that we have to replace "nonzero" by "invertible" (since negative powers are defined only for invertible elements of $\mathbb{L}$). For example, if $\mathbb{L}$ is a commutative ring, then

$$(\alpha\beta)^n = \alpha^n \beta^n \qquad \text{for all invertible } \alpha, \beta \in \mathbb{L} \text{ and all } n \in \mathbb{Z}.$$

We can apply this to $\mathbb{L} = \mathbb{K}[[x]]$ (which is a commutative ring). Recall that the FPS $1-x$ is invertible, and its multiplicative inverse is

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots = \sum_{k \in \mathbb{N}} x^k.$$

A similar argument shows that the FPS $1+x$ is invertible, and its multiplicative inverse is

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 \pm \cdots = \sum_{k \in \mathbb{N}} (-1)^k x^k.$$

Thus, negative powers of $1+x$ are well-defined. We can explicitly compute not just the multiplicative inverse of $1+x$ (as we just did), but also all powers of $1+x$. As far as the nonnegative powers are concerned (that is, $(1+x)^u$ for $u \in \mathbb{N}$), this can easily be done by the binomial formula, and the result can be written either as

$\sum\limits_{k=0}^{u} \binom{u}{k} x^k$ or as the infinite sum $\sum\limits_{k \in \mathbb{N}} \binom{u}{k} x^k$. (The second sum differs from the first sum only in the presence of addends for $k > u$; but all these addends are 0, and thus do not actually affect the sum.) Interestingly, however, the formula

$$(1+x)^u = \sum_{k \in \mathbb{N}} \binom{u}{k} x^k$$

is also valid for negative integers u – even though there is no binomial formula for negative exponents any more! This result is called *Newton's (generalized) binomial theorem for integers*; let us state it as follows:

Theorem 7.3.3. (a) The FPS $1 + x$ is invertible (in $\mathbb{K}[[x]]$). Thus, $(1+x)^u$ is defined for each $u \in \mathbb{Z}$ (by Definition 7.3.2).

(b) In the ring $\mathbb{K}[[x]]$, we have

$$(1+x)^u = \sum_{k \in \mathbb{N}} \binom{u}{k} x^k \qquad \text{for each } u \in \mathbb{Z}.$$

In particular, the sum $\sum\limits_{k \in \mathbb{N}} \binom{u}{k} x^k$ is well-defined (i.e., the family $\left(\binom{u}{k} x^k \right)_{k \in \mathbb{N}}$ is summable) for each $u \in \mathbb{Z}$.

To prove this, we begin by showing a simple corollary of the binomial formula:

Lemma 7.3.4. Let $u \in \mathbb{N}$. Let $\mathbb{K}$ be any ring, and let $a \in \mathbb{K}$. Then,

$$(1+a)^u = \sum_{k \in \mathbb{N}} \binom{u}{k} a^k.$$

(Here, the sum $\sum\limits_{k \in \mathbb{N}} \binom{u}{k} a^k$ is well-defined, since it has only finitely many nonzero addends.)

Lemma 7.3.4 easily implies that Theorem 7.3.3 **(b)** holds for $u \in \mathbb{N}$; but proving Theorem 7.3.3 **(b)** for negative integers u requires more work. Here is ours:

7.4. Polynomials and their degrees

Recall that polynomials have been defined as a special case of FPSs: Namely, a polynomial is just an FPS with only finitely many nonzero entries (= coefficients). But polynomials are, in many ways, better behaved than arbitrary FPSs; in particular, polynomials (unlike FPSs) can be evaluated at elements of $\mathbb{K}$ (by plugging these elements for the "x" in the polynomial), and even at more general things, whereas FPSs don't (in general).

We shall now study polynomials in more detail. To that aim, it helps to look a bit closer and define some smaller classes of polynomials. Namely, we know that each polynomial has only finitely many nonzero coefficients; we can thus ask what its last nonzero coefficient is. This leads to the following definition:

Definition 7.4.1. (a) For each $n \in \mathbb{Z}$, we define a subset $\mathbb{K}[x]_{\leq n}$ of $\mathbb{K}[[x]]$ by

$$\mathbb{K}[x]_{\leq n} = \{(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]] \mid a_k = 0 \text{ for all } k > n\} \tag{103}$$

$$= \left\{\mathbf{a} \in \mathbb{K}[[x]] \mid \left[x^k\right]\mathbf{a} = 0 \text{ for all } k > n\right\}. \tag{104}$$

(Here, of course, "for all $k > n$" means "for all $k \in \mathbb{N}$ satisfying $k > n$".)

(b) Let $\mathbf{a} = (a_0, a_1, a_2, \ldots)$ be a polynomial. Then, all but finitely many $i \in \mathbb{N}$ satisfy $a_i = 0$ (by the definition of a polynomial); in other words, only finitely many $i \in \mathbb{N}$ satisfy $a_i \neq 0$. The *degree* of $\mathbf{a}$ is defined to be the largest $i \in \mathbb{N}$ such that $a_i \neq 0$. (If no such i exists, then we define it to be $-\infty$, which is a symbolic quantity that is understood to be smaller than every integer and to satisfy $(-\infty) + m = -\infty$ for all m.)

The degree of the polynomial $\mathbf{a}$ will be denoted $\deg \mathbf{a}$.

Example 7.4.2. (a) We have

$$\begin{aligned}
\mathbb{K}[x]_{\leq 0} &= \{(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]] \mid a_k = 0 \text{ for all } k > 0\} \\
&= \{(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]] \mid a_1 = a_2 = a_3 = \cdots = 0\} \\
&= \left\{\left(a_0, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) \mid a_0 \in \mathbb{K}\right\} \\
&= \left\{\left(a, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) \mid a \in \mathbb{K}\right\} \\
&= \{\underline{a} \mid a \in \mathbb{K}\} \qquad \left(\text{since } \left(a, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) = \underline{a} \text{ for each } a \in \mathbb{K}\right).
\end{aligned}$$

This is the set of all constant FPSs; these are also known as the *constant polynomials*. Convention 7.2.8 lets us identify these constant polynomials to the elements of $\mathbb{K}$; thus, $\mathbb{K}[x]_{\leq 0}$ simply is $\mathbb{K}$.

(b) We have

$$\begin{aligned}
\mathbb{K}[x]_{\leq 1} &= \{(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]] \mid a_k = 0 \text{ for all } k > 1\} \\
&= \{(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]] \mid a_2 = a_3 = a_4 = \cdots = 0\} \\
&= \left\{\left(a_0, a_1, \underbrace{0, 0, 0, \ldots}_{\text{zeroes}}\right) \mid a_0, a_1 \in \mathbb{K}\right\} \\
&= \{a_0 + a_1 x \mid a_0, a_1 \in \mathbb{K}\}.
\end{aligned}$$

The elements of this set are called the *linear polynomials* (at least in one sense of this word).

(c) If $n \in \mathbb{Z}$ is negative, then

$$\begin{aligned}\mathbb{K}[x]_{\leq n} &= \{(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]] \mid a_k = 0 \text{ for all } k > n\} \\ &= \{(a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]] \mid a_0 = a_1 = a_2 = \cdots = 0\} \\ &= \{(0, 0, 0, \ldots)\} = \{\underline{0}\}.\end{aligned}$$

(d) The FPS $\left(3, 0, 2, 5, \underbrace{0, 0, 0, 0, \ldots}_{\text{zeroes}}\right)$ is a polynomial of degree 3.

Parts **(a)** and **(b)** of Definition 7.4.1 are essentially two different ways to look at the same thing (viz., at what point the coefficients of a polynomial become 0); the precise relation is captured by the following lemma:

Lemma 7.4.3. Let $n \in \mathbb{Z}$. Let $\mathbf{a} \in \mathbb{K}[[x]]$ be an FPS. Then:

(a) We have the following equivalence:

$$\left(\mathbf{a} \in \mathbb{K}[x]_{\leq n}\right) \iff \left(\left[x^k\right]\mathbf{a} = 0 \text{ for all } k > n\right).$$

(b) We have the following equivalence:

$$\left(\mathbf{a} \text{ is a polynomial of degree } \leq n\right) \iff \left(\mathbf{a} \in \mathbb{K}[x]_{\leq n}\right).$$

Note that n is allowed to be negative in Lemma 7.4.3; in this case, Lemma 7.4.3 **(b)** is simply saying that $\mathbf{a}$ is a polynomial of degree $-\infty$ if and only if all its coefficients $a_0, a_1, a_2, \ldots$ are 0 (because the only negative degree that a polynomial can have is $-\infty$).

Lemma 7.4.3 is an easy consequence of Definition 7.4.1, but the proof grows long on paper:

Remark 7.4.4. If you work in constructive logic, then Lemma 7.4.3 **(b)** cannot be proven. In fact, in constructive logic, you cannot prove that each polynomial has a well-defined degree (since you cannot generally prove that each $i \in \mathbb{N}$ satisfies either $a_i = 0$ or $a_i \neq 0$). Thus, the notion of "the degree of a polynomial" is not well-behaved in constructive mathematics. It is also not well-behaved in other ways – e.g., it is not preserved by ring homomorphisms, and leads to nuisances when $\mathbb{K}$ is a trivial ring, as witnessed in Theorem 7.4.11 **(d)** below. Thus, I shall avoid this notion wherever I can help it, and instead use the notion of $\mathbb{K}[x]_{\leq n}$ (where $n \in \mathbb{Z}$). This is a bit less familiar but hopefully more "philosophically right" (while being essentially equivalent to the notion of degree under classical logic, because of Lemma 7.4.3 **(b)**). (The notion of a degree does become useful again when $\mathbb{K}$ is a field, but I will first study a more general setup.)

Corollary 7.2.16 has shown that we can write each FPS as an infinite sum; likewise, we can write each polynomial as a finite sum:

Theorem 7.4.5. Let $n \in \mathbb{Z}$. Let $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]_{\leq n}$. Then,

$$(a_0, a_1, a_2, \ldots) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{k=0}^{n} a_k x^k.$$

Note that n is allowed to be negative in Theorem 7.4.5; in this case, the sum $\sum_{k=0}^{n} a_k x^k$ is empty (and thus equals $0_{\mathbb{K}[[x]]}$), and this should not be surprising (because in this case, we have $(a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]_{\leq n} = \{\underline{0}\}$ (by Example 7.4.2 **(c)**), so that $(a_0, a_1, a_2, \ldots) = \underline{0} = (\text{empty sum})$).

Exercise 7.4.1. Let $n \in \mathbb{N}$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Prove the following:
(a) If $[x^n]\,\mathbf{a} = 0$, then $\mathbf{a} \in \mathbb{K}[x]_{\leq n-1}$.
(b) If $[x^n]\,\mathbf{a} \neq 0$, then $\deg \mathbf{a} = n$.
(c) We have $\deg \mathbf{a} = n$ if and only if $[x^n]\,\mathbf{a} \neq 0$.

Next, let us prove some basic properties of $\mathbb{K}[x]_{\leq n}$:

Lemma 7.4.6. Let $n \in \mathbb{Z}$.
(a) We have $\underline{0} \in \mathbb{K}[x]_{\leq n}$.
(b) If $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]_{\leq n}$, then $\mathbf{a} + \mathbf{b} \in \mathbb{K}[x]_{\leq n}$.
(c) If $\lambda \in \mathbb{K}$ and $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$, then $\lambda \mathbf{a} \in \mathbb{K}[x]_{\leq n}$.
(d) The subset $\mathbb{K}[x]_{\leq n}$ of $\mathbb{K}[[x]]$ is a $\mathbb{K}$-submodule of $\mathbb{K}[[x]]$.
(e) Any finite sum of elements of $\mathbb{K}[x]_{\leq n}$ belongs to $\mathbb{K}[x]_{\leq n}$.
(f) If $i \in \mathbb{N}$ satisfies $i \leq n$, then $x^i \in \mathbb{K}[x]_{\leq n}$.

Lemma 7.4.6 yields the following converse of Theorem 7.4.5:

Exercise 7.4.2. Let $n \in \mathbb{Z}$. Let $a_0, a_1, \ldots, a_n \in \mathbb{K}$. Prove that $\sum_{k=0}^{n} a_k x^k \in \mathbb{K}[x]_{\leq n}$.

Combining Lemma 7.4.6 with Exercise 7.4.1 **(a)**, we obtain a simple fact: If two polynomials in $\mathbb{K}[x]_{\leq n}$ have the same coefficient of x^n, then their difference belongs to $\mathbb{K}[x]_{\leq n-1}$ (since the subtraction "cancels their leading terms"[84]). This fact is highly useful in induction proofs (specifically, it helps prove properties of polynomials by induction on the degree of a polynomial); let us state it as an exercise:

[84] I am putting this in quotation marks because I am trying to avoid the notion of "leading term". (The *leading term* of a nonzero polynomial $\mathbf{a} = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ of degree n is defined to be $a_n x^n$. But beware that if $\mathbf{a} = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$ is merely in $\mathbb{K}[x]_{\leq n}$, then $\deg \mathbf{a}$ may be smaller than n, in which case its leading term is not $a_n x^n$ but rather $a_i x^i$ for $i = \deg \mathbf{a}$. Thus there is a discrepancy between the definition of "leading term" and what we typically want to say when we use this word.)

Exercise 7.4.3. Let $n \in \mathbb{N}$. Let $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]_{\leq n}$ be such that $[x^n]\,\mathbf{a} = [x^n]\,\mathbf{b}$. Then, $\mathbf{a} - \mathbf{b} \in \mathbb{K}[x]_{\leq n-1}$.

Theorem 7.4.7. **(a)** If $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$ satisfy $u \leq v$, then $\mathbb{K}[x]_{\leq u} \subseteq \mathbb{K}[x]_{\leq v}$.
(b) If $n \in \mathbb{Z}$, then $\mathbb{K}[x]_{\leq n}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$.
(c) If $\mathbf{a} \in \mathbb{K}[x]$, then there exists some $n \in \mathbb{N}$ such that $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$.
(d) If $a \in \mathbb{K}$, then $\underline{a} \in \mathbb{K}[x]_{\leq 0}$.
(e) We have $x \in \mathbb{K}[x]_{\leq 1}$.
(f) Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$ and $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$. Then, $\mathbf{a} + \mathbf{b} \in \mathbb{K}[x]_{\leq \max\{n,m\}}$ and $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$.

We shall prove Theorem 7.4.7 in Exercise 7.4.4 below. The hardest part of this theorem is the claim $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$ in its part **(f)**; we can strengthen this part as follows:

Lemma 7.4.8. Let $n, m \in \mathbb{N}$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$ and $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$. Then:
(a) We have $\left[x^{n+i}\right](\mathbf{ab}) = \left([x^n]\,\mathbf{a}\right) \cdot \left(\left[x^i\right]\mathbf{b}\right)$ for each integer $i \geq m$.
(b) We have $\mathbf{ab} \in \mathbb{K}[x]_{\leq n+m}$.
(c) We have $[x^{n+m}](\mathbf{ab}) = \left([x^n]\,\mathbf{a}\right) \cdot \left([x^m]\,\mathbf{b}\right)$.

Exercise 7.4.4. Prove Theorem 7.4.7.

Corollary 7.4.9. **(a)** The subset $\mathbb{K}[x]$ of $\mathbb{K}[[x]]$ is a $\mathbb{K}$-subalgebra of $\mathbb{K}[[x]]$.
(b) We have $x \in \mathbb{K}[x]$.
(c) We have

$$\mathbb{K}[x] = \bigcup_{n \in \mathbb{N}} \mathbb{K}[x]_{\leq n}.$$

Here, $\bigcup_{n \in \mathbb{N}} \mathbb{K}[x]_{\leq n}$ means the union of the sets $\mathbb{K}[x]_{\leq n}$ over all $n \in \mathbb{N}$ (in other words,

$$\begin{aligned}\bigcup_{n \in \mathbb{N}} \mathbb{K}[x]_{\leq n} &= \mathbb{K}[x]_{\leq 0} \cup \mathbb{K}[x]_{\leq 1} \cup \mathbb{K}[x]_{\leq 2} \cup \cdots \\ &= \left\{\mathbf{a} \mid \text{there exists some } n \in \mathbb{N} \text{ such that } \mathbf{a} \in \mathbb{K}[x]_{\leq n}\right\}).\end{aligned}$$

Exercise 7.4.5. Prove Corollary 7.4.9.

Definition 7.4.10. Corollary 7.4.9 **(a)** yields that $\mathbb{K}[x]$ is a $\mathbb{K}$-algebra. This $\mathbb{K}$-algebra is called the *polynomial ring over* $\mathbb{K}$ *in the indeterminate* x (or the *algebra of polynomials in* x *over* $\mathbb{K}$).

Exercise 7.4.6. Let $n \in \{-1, 0, 1, \ldots\}$. Theorem 7.4.7 **(b)** shows that $\mathbb{K}[x]_{\leq n}$ is a $\mathbb{K}$-submodule of $\mathbb{K}[x]$. Prove that the list $\left(x^0, x^1, \ldots, x^n\right)$ is a basis of this $\mathbb{K}$-submodule $\mathbb{K}[x]_{\leq n}$. (See Definition 6.11.1 **(d)** for the definition of a basis of a $\mathbb{K}$-submodule.)

We can restate some of Theorem 7.4.7 in terms of degrees:

Theorem 7.4.11. **(a)** If $a \in \mathbb{K}$, then $\underline{a} \in \mathbb{K}[x]$ and $\deg \underline{a} \leq 0$.
(b) If $a \in \mathbb{K}$ is nonzero, then $\deg \underline{a} = 0$.
(c) We have $x \in \mathbb{K}[x]$ and $\deg x \leq 1$.
(d) If $|\mathbb{K}| > 1$, then $\deg x = 1$.
(e) If $\mathbf{a}$ and $\mathbf{b}$ are two polynomials, then $\mathbf{a} + \mathbf{b}$ and $\mathbf{ab}$ are two polynomials satisfying

$$\deg(\mathbf{a} + \mathbf{b}) \leq \max\{\deg \mathbf{a}, \deg \mathbf{b}\} \qquad \text{and} \qquad \deg(\mathbf{ab}) \leq \deg \mathbf{a} + \deg \mathbf{b}.$$

(f) If $\mathbb{K}$ is a field, and if $\mathbf{a}$ and $\mathbf{b}$ are two polynomials, then $\deg(\mathbf{ab}) = \deg \mathbf{a} + \deg \mathbf{b}$.

We shall prove this in Exercise 7.4.7. The condition "$|\mathbb{K}| > 1$" in Theorem 7.4.11 **(d)** is a homage to the possibility that $\mathbb{K}$ may be a trivial ring (i.e., a ring with only one element). If $\mathbb{K}$ is a trivial ring, then all coefficients of the polynomial x are 0 (because all elements of $\mathbb{K}$ are 0), and thus $\deg x = -\infty$ rather than $\deg x = 1$. The zero ring is generally responsible for lots of exceptions in rules about degrees; thus it is better to speak of "polynomials of degree $\leq n$" than of the exact degree of a polynomial.

Note also that Theorem 7.4.11 **(f)** would not be true without the "$\mathbb{K}$ is a field" requirement. For example, if $\mathbb{K} = \mathbb{Z}/4$ and $\mathbf{a} = 1 + 2x$ and $\mathbf{b} = 1 + 2x$ (using the standard shorthand notations $1 = [1]_4$ and $2 = [2]_4$ etc.), then the polynomial

$$\mathbf{ab} = (1 + 2x)(1 + 2x) = 1 + \underbrace{4x + 4x^2}_{\substack{=0 \\ \text{(since } 4=0 \text{ in } \mathbb{K}\text{)}}} = 1 \tag{105}$$

has degree < 2.

Our next lemma is a generalization of Theorem 7.4.11 **(f)**: Instead of requiring $\mathbb{K}$ to be a field, we will merely require that the coefficient $[x^m]\,\mathbf{b}$ of $\mathbf{b}$ be invertible (which is automatically satisfied when $\mathbb{K}$ is a field and $m = \deg \mathbf{b}$).

Lemma 7.4.12. Let $m \in \mathbb{N}$. Let $\mathbf{a}$ and $\mathbf{b}$ be two polynomials with $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$. Assume that $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible. Then, $\deg(\mathbf{ab}) = \deg \mathbf{a} + m$.

Exercise 7.4.7. Prove Theorem 7.4.11 and Lemma 7.4.12.

Proposition 7.4.13. Let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k \in \mathbb{K}[x]$.
(a) Then,

$$\deg(\mathbf{a}_1\mathbf{a}_2\cdots\mathbf{a}_k) \leq \deg(\mathbf{a}_1) + \deg(\mathbf{a}_2) + \cdots + \deg(\mathbf{a}_k).$$

(b) If $\mathbb{K}$ is a field, then this is an equality.

The following exercise will be useful to us later on:

Exercise 7.4.8. Let $m \in \mathbb{N}$. Let $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ be such that $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible. Let $\mathbf{q} \in \mathbb{K}[x]$ be such that $\mathbf{qb} \in \mathbb{K}[x]_{\leq m-1}$. Prove that $\mathbf{q} = \underline{0}$.

7.5. Division with remainder

7.5.1. The general case

Polynomials, in many senses, are like numbers. In particular, we can study their divisibility, congruence and remainder classes just as we did with integers and Gaussian integers. We will not go deeply into this, but we shall see some of the very basic properties.

The first basic fact is a version of division with remainder for polynomials (compare with Theorem 2.6.1 and Theorem 4.2.26):

Theorem 7.5.1. Let $m \in \mathbb{N}$. Let $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ be such that $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible. Let $\mathbf{a} \in \mathbb{K}[x]$ be any polynomial.
(a) Then, there exists a **unique** pair $(\mathbf{q}, \mathbf{r})$ of polynomials such that $\mathbf{a} = \mathbf{qb} + \mathbf{r}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$.
(b) Moreover, if $n \in \mathbb{N}$ satisfies $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$, then this pair satisfies $\mathbf{q} \in \mathbb{K}[x]_{\leq n-m}$.

We shall give an example for Theorem 7.5.1 in a moment (and then prove the theorem after a while); but first, let us comment on the condition that $[x^m]\,\mathbf{b}$ be invertible. Indeed, if $\mathbb{K}$ is a field, then this condition is equivalent to the requirement that $[x^m]\,\mathbf{b}$ be nonzero; and this latter requirement is equivalent to requiring that $\deg \mathbf{b} = m$ (by Exercise 7.4.1 **(c)**). Hence, if $\mathbb{K}$ is a field, then Theorem 7.5.1 can be applied to any nonzero polynomial $\mathbf{b} \in \mathbb{K}[x]$ (as long as m is chosen to be $\deg \mathbf{b}$). Thus, if $\mathbf{b}$ is a nonzero polynomial over a field $\mathbb{K}$, then any polynomial $\mathbf{a}$ can be uniquely divided with remainder by $\mathbf{b}$ (in such a way that the remainder will have degree $< \deg \mathbf{b}$). But if $\mathbb{K}$ is not a field, then not every polynomial can play the role of $\mathbf{b}$ in Theorem 7.5.1. For example, the polynomial $1 + 2x$ over $\mathbb{K} = \mathbb{Z}$ cannot, because its coefficient of x^1 is not invertible (it equals 2). And unsurprisingly, many polynomials over $\mathbb{Z}$ cannot be divided with remainder by $1 + 2x$ (for example, x^2 cannot – unless you allow remainders of degree > 1).

Example 7.5.2. For this example, set $\mathbb{K} = \mathbb{Z}$ and $m = 2$ and $\mathbf{b} = x^2 + x + 1$. Then, $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$.

Let $n = 4$ and $\mathbf{a} = x^4 - x^2$; thus, $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Then, Theorem 7.5.1 **(a)** says that there exists a **unique** pair $(\mathbf{q}, \mathbf{r})$ of polynomials such that

$$\mathbf{a} = \mathbf{q}\mathbf{b} + \mathbf{r} \qquad \left(\text{that is, } x^4 - x^2 = \mathbf{q} \cdot \left(x^2 + x + 1\right) + \mathbf{r}\right) \qquad \text{and}$$

$$\mathbf{r} \in \mathbb{K}[x]_{\leq m-1} \qquad \left(\text{that is, } \deg \mathbf{r} \leq \underbrace{m}_{=2} - 1 = 1\right).$$

Theorem 7.5.1 **(b)** says that this pair satisfies

$$\mathbf{q} \in \mathbb{K}[x]_{\leq n-m} \qquad \left(\text{that is, } \deg \mathbf{q} \leq \underbrace{n}_{=4} - \underbrace{m}_{=2} = 2\right).$$

How can we find this pair?

Consider this, so far unknown, pair. Comparing the coefficients of x^4 in the equality

$$x^4 - x^2 = \mathbf{q} \cdot \left(x^2 + x + 1\right) + \mathbf{r} = \left(x^2 + x + 1\right)\mathbf{q} + \mathbf{r}, \tag{106}$$

we obtain $1 = 1 \cdot [x^2]\,\mathbf{q}$ (because $\deg \mathbf{r} \leq 1$ and $\deg \mathbf{q} \leq 2$, so the only contribution to the coefficient of x^4 on the right hand side of (106) comes from picking the "x^2" from the "$x^2 + x + 1$" factor and the "$([x^2]\,\mathbf{q})\,x^2$" from the expansion of $\mathbf{q}$). Hence, $[x^2]\,\mathbf{q} = 1$. Since $\deg \mathbf{q} \leq 2$, we can thus write $\mathbf{q}$ in the form

$$\mathbf{q} = x^2 + \mathbf{q}_1 \qquad \text{for some polynomial } \mathbf{q}_1 \text{ with } \deg \mathbf{q}_1 \leq 1.$$

Consider this $\mathbf{q}_1$. Now, (106) can be transformed as follows:

$$\begin{aligned}
&\left(x^4 - x^2 = \left(x^2 + x + 1\right) \underbrace{\mathbf{q}}_{=x^2+\mathbf{q}_1} + \mathbf{r}\right) \\
&\iff \left(x^4 - x^2 = \underbrace{\left(x^2 + x + 1\right)\left(x^2 + \mathbf{q}_1\right)}_{=(x^2+x+1)x^2+(x^2+x+1)\mathbf{q}_1} + \mathbf{r}\right) \\
&\iff \left(x^4 - x^2 = \left(x^2 + x + 1\right)x^2 + \left(x^2 + x + 1\right)\mathbf{q}_1 + \mathbf{r}\right) \\
&\iff \left(\underbrace{x^4 - x^2 - \left(x^2 + x + 1\right)x^2}_{=-x^3-2x^2} = \left(x^2 + x + 1\right)\mathbf{q}_1 + \mathbf{r}\right) \\
&\iff \left(-x^3 - 2x^2 = \left(x^2 + x + 1\right)\mathbf{q}_1 + \mathbf{r}\right).
\end{aligned} \tag{107}$$

Comparing the coefficients of x^3 in the last equality here, we obtain $-1 = 1 \cdot [x^1]\,\mathbf{q}_1$ (because $\deg \mathbf{r} \leq 1$ and $\deg \mathbf{q}_1 \leq 1$). Hence, $[x^1]\,\mathbf{q}_1 = -1$. Since $\deg \mathbf{q}_1 \leq 1$, we can thus write $\mathbf{q}_1$ in the form

$$\mathbf{q}_1 = -x + \mathbf{q}_2 \qquad \text{for some polynomial } \mathbf{q}_2 \text{ with } \deg \mathbf{q}_2 \leq 0.$$

Consider this $\mathbf{q}_2$. Now, the last equality of (107) can be transformed as follows:

$$\begin{aligned}
&\left(-x^3 - 2x^2 = \left(x^2+x+1\right) \underbrace{\mathbf{q}_1}_{=-x+\mathbf{q}_2} + \mathbf{r} \right) \\
\iff &\left(-x^3 - 2x^2 = \underbrace{\left(x^2+x+1\right)(-x+\mathbf{q}_2)}_{=(x^2+x+1)(-x)+(x^2+x+1)\mathbf{q}_2} + \mathbf{r} \right) \\
\iff &\left(-x^3 - 2x^2 = \left(x^2+x+1\right)(-x) + \left(x^2+x+1\right)\mathbf{q}_2 + \mathbf{r} \right) \\
\iff &\left(\underbrace{-x^3 - 2x^2 - \left(x^2+x+1\right)(-x)}_{=-x^2+x} = \left(x^2+x+1\right)\mathbf{q}_2 + \mathbf{r} \right) \\
\iff &\left(-x^2 + x = \left(x^2+x+1\right)\mathbf{q}_2 + \mathbf{r} \right). \qquad (108)
\end{aligned}$$

Comparing the coefficients of x^2 in the last equality here, we obtain $-1 = 1 \cdot [x^0]\,\mathbf{q}_2$ (because $\deg \mathbf{r} \leq 1$ and $\deg \mathbf{q}_2 \leq 0$). Hence, $[x^0]\,\mathbf{q}_2 = -1$. Since $\deg \mathbf{q}_2 \leq 0$, we can thus write $\mathbf{q}_2$ in the form

$$\mathbf{q}_2 = -1 + \mathbf{q}_3 \qquad \text{for some polynomial } \mathbf{q}_3 \text{ with } \deg \mathbf{q}_3 \leq -1.$$

Consider this $\mathbf{q}_3$. Of course, $\mathbf{q}_3$ must be the zero polynomial (that is, $\underline{0} = 0_{\mathbb{K}[x]}$), since $\deg \mathbf{q}_3 \leq -1$. Now that we have found $\mathbf{q}_3$, we can recover $\mathbf{q}_2, \mathbf{q}_1, \mathbf{q}$ by back-substitution:

$$\begin{aligned}
\mathbf{q}_2 &= -1 + \underbrace{\mathbf{q}_3}_{=\underline{0}} = -1; \\
\mathbf{q}_1 &= -x + \underbrace{\mathbf{q}_2}_{=-1} = -x - 1; \\
\mathbf{q} &= x^2 + \underbrace{\mathbf{q}_1}_{=-x-1} = x^2 - x - 1.
\end{aligned}$$

Finally, we can find $\mathbf{r}$, for instance, by solving the last equality (108):

$$\mathbf{r} = -x^2 + x - \left(x^2+x+1\right)\underbrace{\mathbf{q}_2}_{=-1} = -x^2 + x - \left(x^2+x+1\right)(-1) = 2x + 1.$$

Hence, we have found the pair $(\mathbf{q}, \mathbf{r})$. And we can check that this pair $(\mathbf{q}, \mathbf{r})$ does indeed satisfy $\mathbf{a} = \mathbf{qb} + \mathbf{r}$: Indeed,

$$\underbrace{\mathbf{q}}_{=x^2-x-1}\ \underbrace{\mathbf{b}}_{=x^2+x+1} + \underbrace{\mathbf{r}}_{=2x+1} = \left(x^2 - x - 1\right) \cdot \left(x^2 + x + 1\right) + (2x+1) = x^4 - x^2 = \mathbf{a}.$$

Our next goal is to prove Theorem 7.5.1. You may have already spotted a proof idea in Example 7.5.2; we will essentially follow this idea when proving the "existence" part of Theorem 7.5.1 **(a)**, while the "uniqueness" part will be proven by a direct argument using Exercise 7.4.8.

Let us first combine the "existence" part of Theorem 7.5.1 **(a)** with Theorem 7.5.1 **(b)** in order to prove both simultaneously:

Lemma 7.5.3. Let $m \in \mathbb{N}$. Let $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ be such that $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible. Let $n \in \{-1, 0, 1, \ldots\}$. Let $\mathbf{a} \in \mathbb{K}[x]_{\leq n}$. Then, there exist $\mathbf{q} \in \mathbb{K}[x]_{\leq n-m}$ and $\mathbf{r} \in \mathbb{K}[x]_{\leq m-1}$ such that $\mathbf{a} = \mathbf{qb} + \mathbf{r}$.

7.5.2. The case of a field

When $\mathbb{K}$ is a field, every nonzero polynomial $\mathbf{b} \in \mathbb{K}[x]$ has an invertible leading coefficient (i.e., if $m = \deg \mathbf{b}$, then $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible). Thus, Theorem 7.5.1 **(a)** shows that we can divide (with remainder) any polynomial $\mathbf{a}$ by any nonzero polynomial $\mathbf{b}$ when $\mathbb{K}$ is a field. More precisely, the following holds:

Theorem 7.5.4. Let $\mathbb{K}$ be a field. Let $\mathbf{a}$ and $\mathbf{b} \neq \underline{0}$ be polynomials in $\mathbb{K}[x]$. Then, there exist polynomials $\mathbf{q}$ and $\mathbf{r}$ in $\mathbb{K}[x]$ such that $\mathbf{a} = \mathbf{qb} + \mathbf{r}$ and $\deg \mathbf{r} < \deg \mathbf{b}$.

I have deliberately stated Theorem 7.5.4 in the above form (omitting the uniqueness of the pair $(\mathbf{q}, \mathbf{r})$, which I could have stated but did not) in order to evoke a deja-vu; indeed, in this form, Theorem 7.5.4 is obviously an analogue of Theorem 4.2.26. This analogy can be taken much further. When $\mathbb{K}$ is a field, the ring $\mathbb{K}[x]$ shares many properties with $\mathbb{Z}$ and $\mathbb{Z}[i]$. In particular, there is a good theory of divisibility, congruence, common divisors and gcds in this ring, which parallels the corresponding theory for Gaussian integers. The degree of a polynomial plays the same role in $\mathbb{K}[x]$ that the norm of a Gaussian integer plays in $\mathbb{Z}[i]$; in particular, it can be used for purposes of induction.

In defining the gcd of two polynomials over a field $\mathbb{K}$, we are faced with the same difficulty as in the case of $\mathbb{Z}[i]$: The gcd is not unique on the nose, but only unique up to unit-equivalence. However, for polynomials there is a natural choice: Out of all possible gcds of two polynomials, we pick the gcd whose leading coefficient is 1. (The "leading coefficient" of a polynomial means the coefficient of x^n, where n is the degree of the polynomial.)

There is a Euclidean algorithm for finding gcd's: For example, if $\mathbb{K} = \mathbb{Q}$, then

$$\begin{aligned}
&\gcd\left(x^2-1, x^3-1\right) \\
&= \gcd\left(x^2-1, \underbrace{\left(x^3-1\right) \% \left(x^2-1\right)}_{=x-1}\right) \\
&= \gcd\left(x^2-1, x-1\right) = \gcd\left(x-1, x^2-1\right) \\
&= \gcd\left(x-1, \underbrace{\left(x^2-1\right) \% \left(x-1\right)}_{=0}\right) = \gcd\left(x-1, 0\right) \\
&= \gcd\left(x-1\right) = x-1.
\end{aligned}$$

Here, of course, the notation **a**%**b** for a remainder is defined for polynomials in the same way as for integers (after all, the **q** and **r** in Theorem 7.5.4 are unique, even if we didn't say so!).

7.6. Evaluating polynomials

So far, polynomials have just been sequences of scalars. But recall that the most useful thing about polynomials should be the ability of evaluating them (at numbers, matrices, other polynomials). So how do we evaluate our polynomials?

Definition 7.6.1. Let U be a $\mathbb{K}$-algebra. Let $u \in U$.

Let $\mathbf{a} = (a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]$ be a polynomial over $\mathbb{K}$. (Thus, $\mathbf{a} = \sum_{k \in \mathbb{N}} a_k x^k$.)

Then, we define

$$\mathbf{a}[u] := \sum_{k \in \mathbb{N}} a_k u^k \in U.$$

This sum is well-defined, since all but finitely many of its addends are zero (indeed, $(a_0, a_1, a_2, \ldots)$ is a polynomial, and thus all but finitely many $k \in \mathbb{N}$ satisfy $a_k = 0$).

We shall call $\mathbf{a}[u]$ the *value* of $\mathbf{a}$ at u. This is commonly denoted by $\mathbf{a}(u)$, but that notation is problematic, since expressions like "$\mathbf{a}(x+1)$" could mean different things depending on whether they are interpreted as values or as products. (That said, be careful with the notation "$\mathbf{a}[u]$" as well: The expression "$\mathbf{a}\left[x^2\right]\mathbf{b}$" can mean either $\mathbf{a}$ times the coefficient $\left[x^2\right]\mathbf{b}$ or the value $\mathbf{a}\left[x^2\right]$ times $\mathbf{b}$. Disambiguate such expressions using parentheses or dots.)

Example 7.6.2. Let $\mathbf{a} = (a_0, a_1, a_2, \ldots) \in \mathbb{K}[x]$ be a polynomial.

(a) Taking $U = \mathbb{K}$ and $u = 0$ in Definition 7.6.1, we obtain

$$\mathbf{a}[0] = \sum_{k \in \mathbb{N}} a_k 0^k = a_0 \underbrace{0^0}_{=1} + \sum_{k>0} a_k \underbrace{0^k}_{\substack{=0 \\ (\text{since } k>0)}} = a_0 = \left[x^0\right]\mathbf{a}.$$

(b) Taking $U = \mathbb{K}$ and $u = 1$ in Definition 7.6.1, we obtain

$$\mathbf{a}[1] = \sum_{k \in \mathbb{N}} a_k \underbrace{1^k}_{=1} = \sum_{k \in \mathbb{N}} a_k = a_0 + a_1 + a_2 + \cdots .$$

This is the sum of all coefficients of $\mathbf{a}$.

(c) Taking $U = \mathbb{K}[x]$ and $u = x$ in Definition 7.6.1, we obtain

$$\mathbf{a}[x] = \sum_{k \in \mathbb{N}} a_k x^k = (a_0, a_1, a_2, \ldots) = \mathbf{a}.$$

So $\mathbf{a}[x]$ is another way of saying "$\mathbf{a}$".

(d) Furthermore,

$$\mathbf{a}[-x] = \sum_{k \in \mathbb{N}} a_k \underbrace{(-x)^k}_{=(-1)^k x^k} = \sum_{k \in \mathbb{N}} (-1)^k a_k x^k = (a_0, -a_1, a_2, -a_3, a_4, \ldots) .$$

(e) Furthermore,

$$\mathbf{a}\left[x^2\right] = \sum_{k \in \mathbb{N}} a_k \left(x^2\right)^k = \sum_{k \in \mathbb{N}} a_k x^{2k} = (a_0, 0, a_1, 0, a_2, 0, a_3, 0, \ldots) .$$

In Definition 7.6.1, we have rigorously defined the value $\mathbf{a}[u]$ of a polynomial $\mathbf{a}$ at an element u of a $\mathbb{K}$-algebra. In practice, this value is best understood through the following slogan:

> *Substitution slogan:* Let U be a $\mathbb{K}$-algebra, and let $u \in U$. Let $\mathbf{a} \in \mathbb{K}[x]$ be a polynomial. Then, $\mathbf{a}[u]$ is, roughly speaking, the result of "substituting u for x" into $\mathbf{a}$.

For example,

$$\left(1 + 3x + 8x^2\right)[u] = 1 + 3u + 8u^2 \qquad \text{and} \tag{109}$$

$$\left(x^9 - 2x\right)[u] = u^9 - 2u \qquad \text{and} \tag{110}$$

$$\left(x^4 - (x-1)^2 (x+1)^2\right)[u] = u^4 - (u-1)^2 (u+1)^2 . \tag{111}$$

However, strictly speaking, this is not all obvious at this point yet. While (109) and (110) can easily be checked using Definition 7.6.1[85], it is not so clear how to

[85]Namely: Write the polynomial $1 + 3x + 8x^2$ in the form $(a_0, a_1, a_2, \ldots)$ for some $a_0, a_1, a_2, \ldots \in \mathbb{K}$. Then, $a_0 = 1$ and $a_1 = 3$ and $a_2 = 8$ and $a_k = 0$ for all $k > 2$. But Definition 7.6.1 (applied to

obtain (111) from Definition 7.6.1 without multiplying out both sides[86]. Definition 7.6.1 only justifies the Substitution slogan when the substitution happens in the **expanded form** of $\mathbf{a}$ (that is, in the form $\mathbf{a} = a_0x^0 + a_1x^1 + a_2x^2 + \cdots$), but not when it happens in some other form like $(1+x)(1-x)$ or $x^2 - (x-1)^2$. We shall soon convince ourselves that the Substitution slogan is true for the latter forms as well. First, we need to prove some basic properties of values of polynomials:

Theorem 7.6.3. Let U be a $\mathbb{K}$-algebra. Let $u \in U$.

(a) Any $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$ satisfy

$$(\mathbf{a}+\mathbf{b})[u] = \mathbf{a}[u] + \mathbf{b}[u] \qquad \text{and} \qquad (\mathbf{ab})[u] = \mathbf{a}[u] \cdot \mathbf{b}[u].$$

(b) Any $\lambda \in \mathbb{K}$ and $\mathbf{a} \in \mathbb{K}[x]$ satisfy

$$(\lambda\mathbf{a})[u] = \lambda \cdot \mathbf{a}[u].$$

(c) Any $a \in \mathbb{K}$ satisfies $\underline{a}[u] = a \cdot 1_U$. (This is often written as "$\underline{a}[u] = a$", but keep in mind that the "a" on the right hand side of this equality is understood to be "coerced into U", so it actually means "the element of U corresponding to a", which is $a \cdot 1_U$.)

(d) We have $x[u] = u$.

(e) We have $x^i[u] = u^i$ for each $i \in \mathbb{N}$.

$\mathbf{a} = 1 + 3x + 8x^2$) yields

$$\left(1+3x+8x^2\right)[u] = \sum_{k\in\mathbb{N}} a_k u^k = \underbrace{a_0}_{=1}\underbrace{u^0}_{=1} + \underbrace{a_1}_{=3}\underbrace{u^1}_{=u} + \underbrace{a_2}_{=8}u^2 + \sum_{k>2}\underbrace{a_k}_{=0}u^k$$
$$= 1 + 3u + 8u^2 + \underbrace{\sum_{k>2} 0u^k}_{=0} = 1 + 3u + 8u^2.$$

This proves (109). A similar argument can be used to prove (110).

[86] Of course, if you multiply them out, then (111) becomes obvious: We have $x^4 - (x-1)^2(x+1)^2 = 2x^2 - 1$, so that

$$\left(x^4 - (x-1)^2(x+1)^2\right)[u] = \left(2x^2-1\right)[u] = 2u^2 - 1$$

(this follows from Definition 7.6.1 in the same way as (109) did). Comparing this with

$$u^4 - (u-1)^2(u+1)^2 = 2u^2 - 1,$$

we obtain $\left(x^4 - (x-1)^2(x+1)^2\right)[u] = u^4 - (u-1)^2(u+1)^2$, and thus (111) is proven.

But multiplying out is not always viable. Let's say we want to prove that

$$\left(x^{2n} - (x-1)^n(x+1)^n\right)[u] = u^{2n} - (u-1)^n(u+1)^n$$

for all $n \in \mathbb{N}$. This can no longer be proven as easily, since the coefficients of the polynomial $x^{2n} - (x-1)^n(x+1)^n$ will grow more complicated as n grows larger.

Corollary 7.6.4. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. Then, the map

$$\begin{aligned} \mathrm{ev}_u : \mathbb{K}[x] &\to U, \\ \mathbf{a} &\mapsto \mathbf{a}[u] \end{aligned}$$

is a $\mathbb{K}$-algebra homomorphism.

The map ev_u in Corollary 7.6.4 is called an *evaluation homomorphism* (specifically, the *evaluation homomorphism at u*), since it "evaluates" each polynomial at u.

Corollary 7.6.5. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. Then:

(a) We have $(-\mathbf{a})[u] = -\mathbf{a}[u]$ for each $\mathbf{a} \in \mathbb{K}[x]$.

(b) We have $(\mathbf{a} - \mathbf{b})[u] = \mathbf{a}[u] - \mathbf{b}[u]$ for each $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$.

(c) We have $\left(\sum_{s \in S} \mathbf{a}_s\right)[u] = \sum_{s \in S} (\mathbf{a}_s[u])$ whenever S is a finite set and $\mathbf{a}_s \in \mathbb{K}[x]$ for all $s \in S$.

(d) We have $(\mathbf{a}_1 \mathbf{a}_2 \cdots \mathbf{a}_k)[u] = \mathbf{a}_1[u] \cdot \mathbf{a}_2[u] \cdot \cdots \cdot \mathbf{a}_k[u]$ whenever $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_k \in \mathbb{K}[x]$.

(e) If the ring U is commutative, then $\left(\prod_{s \in S} \mathbf{a}_s\right)[u] = \prod_{s \in S} (\mathbf{a}_s[u])$ whenever S is a finite set and $\mathbf{a}_s \in \mathbb{K}[x]$ for all $s \in S$.

(f) We have $\mathbf{a}^n[u] = (\mathbf{a}[u])^n$ for each $\mathbf{a} \in \mathbb{K}[x]$ and each $n \in \mathbb{N}$.

(g) We have $(n\mathbf{a})[u] = n \cdot \mathbf{a}[u]$ for each $\mathbf{a} \in \mathbb{K}[x]$ and each $n \in \mathbb{Z}$.

Theorem 7.6.3 and Corollary 7.6.5 (or, more abstractly, Corollary 7.6.4) justify the Substitution slogan in general. For example, we can now prove (111) directly,

without multiplying out anything, as follows:

$$\begin{aligned}
&\left(x^4-(x-1)^2(x+1)^2\right)[u] \\
&= \underbrace{x^4[u]}_{\substack{=(x[u])^4 \\ \text{(by Corollary 7.6.5 \textbf{(f)})}}} - \underbrace{\left((x-1)^2(x+1)^2\right)[u]}_{\substack{=(x-1)^2[u]\cdot(x+1)^2[u] \\ \text{(by the second equality of} \\ \text{Theorem 7.6.3 \textbf{(a)})}}} \qquad \text{(by Corollary 7.6.5 \textbf{(b)})} \\
&= \left(\underbrace{x[u]}_{\substack{=u \\ \text{(by Theorem 7.6.3 \textbf{(d)})}}}\right)^4 - \underbrace{(x-1)^2[u]}_{\substack{=((x-1)[u])^2 \\ \text{(by Corollary 7.6.5 \textbf{(f)})}}} \cdot \underbrace{(x+1)^2[u]}_{\substack{=((x+1)[u])^2 \\ \text{(by Corollary 7.6.5 \textbf{(f)})}}} \\
&= u^4 - \left(\underbrace{(x-1)[u]}_{\substack{=x[u]-1[u] \\ \text{(by Corollary 7.6.5 \textbf{(b)})}}}\right)^2 \cdot \left(\underbrace{(x+1)[u]}_{\substack{=x[u]+1[u] \\ \text{(by the first equality of} \\ \text{Theorem 7.6.3 \textbf{(a)})}}}\right)^2 \\
&= u^4 - (x[u]-1[u])^2 \cdot (x[u]+1[u])^2 \\
&= u^4 - \left(\underbrace{x[u]}_{\substack{=u \\ \text{(by Theorem 7.6.3 \textbf{(d)})}}} - \underbrace{\underline{1}[u]}_{\substack{=1 \\ \text{(by Theorem 7.6.3 \textbf{(c)})}}}\right)^2 \cdot \left(\underbrace{x[u]}_{\substack{=u \\ \text{(by Theorem 7.6.3 \textbf{(d)})}}} + \underbrace{\underline{1}[u]}_{\substack{=1 \\ \text{(by Theorem 7.6.3 \textbf{(c)})}}}\right)^2 \\
&\qquad \text{(since our ``1'' here really means ``}\underline{1}\text{'')} \\
&= u^4 - (u-1)^2(u+1)^2.
\end{aligned}$$

This argument was completely straightforward (despite its length); all we did was "opening the parentheses"[87] using whatever part of Theorem 7.6.3 or Corollary 7.6.5 would let us do that.

Thanks to Corollary 7.6.4 (or the Substitution slogan), the polynomial ring $\mathbb{K}[x]$ is a sort of "forge" for identities that concern an arbitrary element u of an arbitrary $\mathbb{K}$-algebra U. For example, if you want to prove the identity

$$u^3 - u = u(u-1)(u+1) \qquad \text{for any } \mathbb{K}\text{-algebra } U \text{ and any } u \in U,$$

then it suffices to prove the identity

$$x^3 - x = x(x-1)(x+1) \qquad \text{in } \mathbb{K}[x]$$

[87] more formally: rewriting an expression of the form "(something complicated) $[u]$" in terms of one or several expressions of the form "(something simpler) $[u]$"

and then apply ev_u to both sides of it (or, less formally, take the values of both sides at u, and simplify them using the Substitution slogan). Indeed, the map ev_u sends x to u and is a $\mathbb{K}$-algebra homomorphism, whence it also sends $x^3 - x$ to $u^3 - u$ and sends $x(x-1)(x+1)$ to $u(u-1)(u+1)$. The Substitution slogan is saying this at a more concrete level: Indeed, applying the map ev_u is tantamount to "substituting u for x" in a polynomial.

Remark 7.6.6. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. We have defined $\mathbf{a}[u]$ for $\mathbf{a} \in \mathbb{K}[x]$. We can try to define it for arbitrary $\mathbf{a} = (a_0, a_1, a_2, \ldots) \in \mathbb{K}[[x]]$ as well. But in general, this will not work, since the sum $\sum_{k \in \mathbb{N}} a_k u^k$ may not be well-defined. However, if u itself is a FPS (that is, $u \in \mathbb{K}[[x]]$) and satisfies $\left[x^0\right] u = 0$, then the family $\left(a_k u^k\right)_{k \in \mathbb{N}}$ is summable (because in this case, we have

$$\left[x^0\right]\left(u^k\right) = \left[x^1\right]\left(u^k\right) = \cdots = \left[x^{k-1}\right]\left(u^k\right) = 0$$

for all $k \in \mathbb{N}$), and therefore $\mathbf{a}[u]$ is well-defined. For example, $\mathbf{a}\left[x^2\right]$ is well-defined, and more generally, $\mathbf{a}\left[x^k\right]$ is well-defined for every positive integer k; but $\mathbf{a}[1]$ is not well-defined.

We now define the concept of a root of a polynomial:

Definition 7.6.7. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. Let $\mathbf{a} \in \mathbb{K}[x]$.
We say that u is a *root* of $\mathbf{a}$ if $\mathbf{a}[u] = 0$.

This is a very general notion of "root" that we have just defined. You may be used to the idea that a polynomial $\mathbf{a} \in \mathbb{K}[x]$ can have roots in the ring $\mathbb{K}$ itself, but we are allowing roots in any arbitrary $\mathbb{K}$-algebra (e.g., in a matrix algebra $\mathbb{K}^{n \times n}$ or even in the polynomial ring $\mathbb{K}[x]$ itself). For example, the roots of the polynomial $x(x-1)$ in a $\mathbb{K}$-algebra U are the idempotent elements of U, because for any element $u \in U$, we have the following equivalence:

$$\begin{aligned}
&(u \text{ is a root of } x(x-1)) \\
&\iff \left(\underbrace{(x(x-1))[u]}_{=x[u]\cdot(x-1)[u]} = 0 \right) \iff \left(\underbrace{x[u]}_{=u} \cdot \underbrace{(x-1)[u]}_{=u-1} = 0 \right) \\
&\iff \left(\underbrace{u \cdot (u-1)}_{=u^2-u} = 0 \right) \iff \left(u^2 - u = 0\right) \iff \left(u^2 = u\right) \\
&\iff (u \text{ is idempotent}).
\end{aligned}$$

If U is a field, then the only idempotent elements of U are 0 and 1 (because $u \cdot (u-1) = 0$ implies that u or $u-1$ is 0). Otherwise, there can be more idempotent elements; for example, $\mathbb{Z}/6$ has the four idempotent elements $[0]_6, [1]_6, [3]_6, [4]_6$.

We now define divisibility of polynomials in the same way as we defined divisibility of integers (Definition 2.2.1) and divisibility of Gaussian integers (Definition 4.2.17):

Definition 7.6.8. Let $\mathbf{a}$ and $\mathbf{b}$ be two polynomials in $\mathbb{K}[x]$. We say that $\mathbf{a} \mid \mathbf{b}$ (or, more precisely, "$\mathbf{a} \mid \mathbf{b}$ in $\mathbb{K}[x]$") if there exists a $\mathbf{c} \in \mathbb{K}[x]$ such that $\mathbf{b} = \mathbf{ac}$.

Be aware that this is a somewhat slippery notion, as its meaning depends on $\mathbb{K}$, which is not reflected in the notation "$\mathbf{a} \mid \mathbf{b}$". For example, the two polynomials $1+x$ and $2+2x$ satisfy $2+2x \mid 1+x$ when $\mathbb{K} = \mathbb{Q}$ (since $1+x = (2+2x) \cdot \frac{1}{2}$), but not when $\mathbb{K} = \mathbb{Z}$. Thus, when ambiguity is possible, $\mathbb{K}$ should be specified (i.e., you should write "$\mathbf{a} \mid \mathbf{b}$ in $\mathbb{K}[x]$" rather than just "$\mathbf{a} \mid \mathbf{b}$").

The roots of a polynomial $\mathbf{a} \in \mathbb{K}[x]$ are closely connected to divisors of $\mathbf{a}$ – specifically, ones of the form $x - u$:

Proposition 7.6.9. Let $\mathbf{a}$ be a polynomial in $\mathbb{K}[x]$. Let $u \in \mathbb{K}$. Then,

$$(u \text{ is a root of } \mathbf{a}) \iff (x - u \mid \mathbf{a}).$$

(Of course, $x - u$ means $x - \underline{u}$.)

Example 7.6.10. Let $\mathbb{K} = \mathbb{Z}/6$ and $\mathbf{a} = x^2 - x$. Then, the roots of $\mathbf{a}$ in $\mathbb{K}$ are precisely the idempotent elements of $\mathbb{K}$; these are $0, 1, 3, 4$. So the previous proposition yields that $x - 0$, $x - 1$, $x - 3$ and $x - 4$ all divide $\mathbf{a}$. However, this does not mean that the product $(x-0)(x-1)(x-3)(x-4)$ divides $\mathbf{a}$. Instead, we have

$$\mathbf{a} = (x-0)(x-1) = (x-3)(x-4) \qquad \text{in } \mathbb{K}[x].$$

If this example appears weird, keep in mind that $\mathbb{Z}/6$ is not a field. When $\mathbb{K}$ is a field, the polynomial ring $\mathbb{K}[x]$ behaves very much like $\mathbb{Z}$ or $\mathbb{Z}[i]$: We have division with remainder by any nonzero polynomial; we have gcds; we have a notion of "primes" (which are called irreducible polynomials); and every nonzero polynomial has a unique factorization into primes (up to units, which are the nonzero constant polynomials). But when $\mathbb{K}$ is merely a commutative ring, this can all break down; in particular, Example 7.6.10 shows that the factorization into primes (when it exists) is not unique.

The following theorem is often called the "*easy half of the Fundamental Theorem of Algebra*":

Theorem 7.6.11. Let $\mathbb{K}$ be a field. Let $n \in \mathbb{N}$. Then, any nonzero polynomial $\mathbf{a} \in \mathbb{K}[x]$ of degree $\leq n$ has at most n roots in $\mathbb{K}$. (We are not counting the roots with multiplicity here.)

When $\mathbb{K}$ is just an arbitrary field, the number of roots of a degree-n nonzero polynomial over $\mathbb{K}$ can be much smaller than n. For example, the polynomial $x^2+1 \in \mathbb{R}[x]$ has 0 roots in $\mathbb{R}$ (but it has 2 roots in $\mathbb{C}$). The "hard half" of the Fundamental Theorem of Algebra says that a nonzero polynomial $\mathbf{a} \in \mathbb{C}[x]$ of degree n has exactly n roots in $\mathbb{C}$, counted with multiplicity. As I said before, this is not a theorem of algebra, since it relies on the fact that $\mathbb{C}$ has a topology and is closed in this topology.

Next comes a little potpourri of properties of polynomials:

Proposition 7.6.12. Let $\mathbf{a}$ and $\mathbf{b}$ be two nonzero polynomials in $\mathbb{K}[x]$.
(a) We have $\deg(\mathbf{a}[\mathbf{b}]) \leq \deg\mathbf{a} \cdot \deg\mathbf{b}$.
(b) If $\mathbb{K}$ is a field, then this inequality is an equality.

Proposition 7.6.13. Let U and V be two $\mathbb{K}$-algebras. Let $f : U \to V$ be a $\mathbb{K}$-algebra homomorphism. Let $u \in U$ and $\mathbf{a} \in \mathbb{K}[x]$. Then,

$$f(\mathbf{a}[u]) = \mathbf{a}[f(u)].$$

Proposition 7.6.14. Let U be a $\mathbb{K}$-algebra. Let $u \in U$. Let $\mathbf{a}, \mathbf{b} \in \mathbb{K}[x]$. Then,

$$\mathbf{a}[\mathbf{b}[u]] = (\mathbf{a}[\mathbf{b}])[u].$$

One more notation is needed for the next section.

Definition 7.6.15. Let $\mathbb{L}$ be a ring that contains $\mathbb{Q}$ as a subring. (For example, $\mathbb{L}$ can be $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{Q}[x]$.)

Recall that in Definition 2.17.1, we have defined the binomial coefficient $\binom{n}{k}$ for all $n \in \mathbb{Q}$ and $k \in \mathbb{Q}$. We extend the very same definition to all $n \in \mathbb{L}$.

Thus, in particular, we have a polynomial $\binom{x}{k} \in \mathbb{Q}[x]$ for each $k \in \mathbb{Q}$. This polynomial $\binom{x}{k}$ is explicitly given by

$$\binom{x}{k} = \frac{x(x-1)(x-2)\cdots(x-k+1)}{k!} \qquad \text{when } k \in \mathbb{N} \tag{112}$$

(and equals 0 when $k \notin \mathbb{N}$). More generally, for each polynomial $\mathbf{a} \in \mathbb{Q}[x]$ and each $k \in \mathbb{N}$, we have a polynomial

$$\binom{\mathbf{a}}{k} = \frac{\mathbf{a}(\mathbf{a}-1)(\mathbf{a}-2)\cdots(\mathbf{a}-k+1)}{k!}. \tag{113}$$

The following is easy:

Corollary 7.6.16. Let $k \in \mathbb{N}$.

(a) Then, $\binom{x}{k}$ is a polynomial of degree k.

(b) For each $u \in \mathbb{Q}$, we have $\binom{x}{k}[u] = \binom{u}{k}$.

(c) For each $\mathbf{a} \in \mathbb{Q}[x]$ and $u \in \mathbb{Q}$, we have $\binom{\mathbf{a}}{k}[u] = \binom{\mathbf{a}[u]}{k}$.

7.7. The polynomial identity trick

Convention 7.7.1. For this whole section, let $\mathbb{K}$ be a field.

7.7.1. Enough equal values make polynomials equal

Corollary 7.7.2. Let $\mathbf{a}$ and $\mathbf{b}$ be two polynomials of degree $\leq n$ over the field $\mathbb{K}$. Assume that at least $n+1$ many elements $u \in \mathbb{K}$ satisfy $\mathbf{a}[u] = \mathbf{b}[u]$. Then, $\mathbf{a} = \mathbf{b}$.

I like to refer to the following corollary as "the *polynomial identity trick*":

Corollary 7.7.3. Let $\mathbf{a}$ and $\mathbf{b}$ be two polynomials over the field $\mathbb{K}$. Assume that infinitely many elements $u \in \mathbb{K}$ satisfy $\mathbf{a}[u] = \mathbf{b}[u]$. Then, $\mathbf{a} = \mathbf{b}$.

Example 7.7.4. Corollary 7.7.3 can be false when $\mathbb{K}$ is not a field. For an example, pick any infinite set S, and let $\mathbb{K}$ be the commutative ring $(\mathcal{P}(S), \triangle, \cap, \varnothing, S)$ constructed in Section 5.2. Let $n = 2$, $\mathbf{a} = x^2 - x$ and $\mathbf{b} = \underline{0}$. Then, **each** $u \in \mathbb{K}$ satisfies $\mathbf{a}[u] = \mathbf{b}[u]$ (because $\mathbf{a}[u] = u^2 - u = \underbrace{u \cap u}_{=u} - u = u - u = \varnothing = 0_{\mathbb{K}} = \underline{0}[u] = \mathbf{b}[u]$); thus, in particular, infinitely many elements $u \in \mathbb{K}$ satisfy $\mathbf{a}[u] = \mathbf{b}[u]$. But it is not true that $\mathbf{a} = \mathbf{b}$.

We can now prove Proposition 2.17.16:

We can now finish our proof of Theorem 2.17.14 by putting on solid ground everything we used about polynomials in that proof:

7.7.2. Lagrange interpolation

Corollary 7.7.2 shows that for any $n \in \mathbb{N}$, a polynomial of degree $\leq n$ over a field $\mathbb{K}$ is uniquely determined by its values on any $n+1$ (given) distinct elements of $\mathbb{K}$. There is a matching existence claim to this uniqueness claim: To any choice of values at any $n+1$ given distinct elements of $\mathbb{K}$, you can find excatly one polynomial of degree $\leq n$ over $\mathbb{K}$ that takes these values at these elements. This polynomial can even be determined explicitly, as the following theorem shows:

Theorem 7.7.5. Let $n \in \mathbb{N}$. Let $a_1, a_2, \ldots, a_{n+1}$ be $n+1$ distinct elements of a field $\mathbb{K}$. Let $b_1, b_2, \ldots, b_{n+1}$ be $n+1$ arbitrary elements of $\mathbb{K}$.

(a) There is a unique polynomial $\mathbf{f} \in \mathbb{K}[x]_{\leq n}$ satisfying

$$\left(\mathbf{f}[a_i] = b_i \qquad \text{for all } i \in \{1, 2, \ldots, n+1\}\right). \tag{114}$$

(b) This polynomial $\mathbf{f}$ is given by

$$\mathbf{f} = \sum_{j=1}^{n+1} b_j \frac{\prod\limits_{k \neq j} (x - a_k)}{\prod\limits_{k \neq j} (a_j - a_k)}$$

(where the "$\prod\limits_{k \neq j}$" signs mean "$\prod\limits_{\substack{k \in \{1,2,\ldots,n+1\}; \\ k \neq j}}$").

Theorem 7.7.5 is known as the *Lagrange interpolation theorem*. Before we prove it, let us remark that it generalizes (and concretizes) Proposition 1.6.6 (which is its particular case for $n = 2$ and $\mathbb{K} = \mathbb{Q}$ or $\mathbb{K} = \mathbb{R}$). After proving it, we will discuss how it helps make Shamir's Secret Sharing Scheme work. We also notice that Theorem 7.7.5 requires $\mathbb{K}$ to be a field; when $\mathbb{K}$ is merely a commutative ring, both the "existence" and "uniqueness" parts of Theorem 7.7.5 **(a)** may fail, and the fractions appearing in Theorem 7.7.5 **(b)** may fail to be well-defined (since their denominators $a_j - a_k$ may fail to be invertible). We have already witnessed the failure of the "existence" part of Theorem 7.7.5 **(a)** in the case when $\mathbb{K} = \mathbb{Z}$: Indeed, if we set

$$\begin{aligned} n = 2, \qquad & a_1 = 0, \qquad a_2 = 1, \qquad a_3 = 2, \\ & b_1 = 0, \qquad b_2 = 0, \qquad b_3 = 1, \end{aligned}$$

then there exists no polynomial $\mathbf{f} \in \mathbb{Z}[x]_{\leq 2}$ satisfying $\mathbf{f}[a_i] = b_i$ for all $i \in \{1, 2, 3\}$. (The polynomial $\binom{x}{2}$ would satisfy this, but it is not a polynomial in $\mathbb{Z}[x]_{\leq 2}$, since its coefficients are not integers. We have already observed this in Example 2.17.24 **(a)**.)

7.7.3. Application: Curve fitting

Theorem 7.7.5 has multiple applications.

The most obvious one is to treat Theorem 7.7.5 as an interpolation theorem: Roughly speaking, it says that $n+1$ values (at distinct points) in a field can always be fit by a unique polynomial of degree $\leq n$. See the Wikipedia pages for Lagrange polynomials and polynomial interpolation, but beware that this is not the kind of interpolation that is a good choice for curve-fitting practical datasets (which rarely follow a polynomial rule). It is best suited for interpolating functions when you can

freely choose the points at which you sample (i.e., the a_i in Theorem 7.7.5); certain choices of a_i fare much better than others. Thus, Lagrange interpolation can also be used in designing numerical quadrature rules. See [Trefet11] for details.

7.7.4. Application: Shamir's Secret Sharing Scheme

Here is another application of Theorem 7.7.5. Shamir's Secret Sharing Scheme (as presented in Subsection 1.6.7 and fixed in Remark 5.6.3) can now finally be implemented concretely. Indeed, consider the setting of Section 1.6 with general n and k, and assume that the secret **a** that we want to distribute is a bitstring of length N. As in Remark 5.6.3, we pick a prime p such that both $p \geq 2^N$ and $p > n$, and we encode **a** as a residue class $\alpha \in \mathbb{Z}/p$. Pick $k-1$ uniformly random elements $\beta_1, \beta_2, \ldots, \beta_{k-1}$ of $\mathbb{Z}/p$, and define the polynomial

$$\mathbf{f} = \beta_{k-1}x^{k-1} + \beta_{k-2}x^{k-2} + \cdots + \beta_1 x^1 + \alpha \in (\mathbb{Z}/p)[x]_{\leq k-1}.$$

Reveal to each person $i \in \{1, 2, \ldots, n\}$ the value $\mathbf{f}\left(\left[i\right]_p\right)$. Then, Theorem 7.7.5 (applied to $k-1$ instead of n) shows that any k of the n people can uniquely reconstruct **f** (since they know the values of **f** at k distinct elements of $\mathbb{Z}/p$ [88]), whereas $k-1$ of the n people cannot gain any knowledge about the secret **a** (since they only know the values of **f** at $k-1$ nonzero elements of $\mathbb{Z}/p$ [89], and these values could be combined with any possible value at $\left[0\right]_p$ to form a valid polynomial in $(\mathbb{Z}/p)[x]_{\leq k-1}$). Thus, both Requirements 1 and 2 from Section 1.6 are satisfied. This is Shamir's Secret Sharing Scheme in its final form.

Instead of $\mathbb{Z}/p$ we could have used any finite field $\mathbb{F}$ whose size is $\geq 2^N$ and $> n$, but we would need to be careful, since the elements $\left[1\right]_p, \left[2\right]_p, \ldots, \left[n\right]_p$ would no longer necessarily be distinct and nonzero. Thus, we would have to use n distinct nonzero elements of $\mathbb{F}$ instead.

7.7.5. Application: Reed–Solomon codes

Finally, here is a far more important application of Theorem 7.7.5.

Assume that you want to send digital data over a noisy channel (e.g., radio). "Noisy" means that the transmission will introduce errors, and you expect (e.g.) that every bit you send has a small probability p of getting corrupted on its way[90]. You want to ensure that the recepient gets the correct bits that you sent him.[91] How can you do this?

[88] Here we are using the fact that the elements $\left[1\right]_p, \left[2\right]_p, \ldots, \left[n\right]_p$ of $\mathbb{Z}/p$ are distinct (since $p > n$).

[89] Here we are using the fact that the elements $\left[1\right]_p, \left[2\right]_p, \ldots, \left[n\right]_p$ of $\mathbb{Z}/p$ are nonzero (since $p > n$).

[90] "Corrupted" means that the recepient will receive a 0 instead of 1, or a 1 instead of a 0. For simplicity, we assume that bits will not be lost, and the order in which they are received is the order in which they are sent (so, e.g., messenger pigeons are not the kind of channel we are considering).

[91] Another, mostly equivalent, version of this problem is long-term storage of data on a medium (e.g., a hard drive, a DVD, paper or a scroll) that gradually decays. Here, the sender is you when

Of course, you cannot guarantee this with complete surety. But there are several schemes that you can use to make it rather likely. They are called *error-correcting codes*.

- For instance, let us assume you have agreed with your recepient that you will be sending each bit **twice** in a row. Then, if the recepient gets two different bits when they expect the same bit sent twice, he can immediately tell that a bit got corrupted on its way. He cannot tell which bit you meant to send him – but at least he knows that he cannot trust the ones he got.[92] Of course, there is a probability that he got the wrong bit twice, in which case he is clueless about it being wrong; but this probability is p^2, which is a lot smaller than p. This is called *error detection*.

- An even better scheme is to send each bit **thrice** in a row. This way, your recipient can not only tell if some bit was corrupted (with an even smaller probability of falsely believing that everything went right – namely, p^3); he can also try to guess which bit is the right one, by the "majority rule" (i.e., among the 3 bits he obtained, he chooses the one that appears more often). This is called *error correction*.

- But sending each bit multiple times is not the only thing you can do; you can also mix several bits together. For example, you can follow every four bits a, b, c, d that you are sending with the three bits

$$a+b+d, \qquad a+c+d, \qquad b+c+d,$$

  where you are regarding bits as elements of $\mathbb{Z}/2$ (so that, for example, $1+1+1=1$). Thus, you are sending 7 bits instead of 4 bits, but the transmission has become a lot safer, because:

  - If at most 2 of the 7 bits get corrupted along the way, the recepient will be able to tell that something went wrong. (In the language of coding theory, this is saying that your code *detects up to* 2 *errors*.)
  - If at most 1 of the 7 bits gets corrupted along the way, the recepient will be able to guess the bits you intended to send[93]. (In the language of coding theory, this is saying that your code *corrects up to* 1 *error*.)

  This scheme is called the Hamming$(7,4)$ code, and was invented by Richard W. Hamming in 1950 as a tool to make error-prone punch card readers less likely to fail.

you are storing the data; the recepient is you (or whoever wants to read it) in the future. That's a noisy channel!

[92] If he can talk back to you, this means he can ask you to resend the correct one.

[93] without having to ask you to re-send them

- Here is yet another error-correcting code, which makes use of finite fields. Fix two integers $d, e \in \mathbb{N}$ such that $d < e$, as well as a finite field $\mathbb{K}$ and e distinct elements $a_1, a_2, \ldots, a_e$ of $\mathbb{K}$. (You have to agree on these in advance with your recepient. Of course, the field must satisfy $|\mathbb{K}| \geq e$.) Now, instead of transmitting bits, you transmit elements of $\mathbb{K}$. (This does not require a different kind of channel; you can always, under the hood, re-encode your elements of $\mathbb{K}$ into bitstrings and send those as bits via the channel that you have.[94]) Now, when you want to send $d+1$ elements $u_0, u_1, \ldots, u_d$ of $\mathbb{K}$ over the channel, you instead form the polynomial

$$\mathbf{f} = u_0 + u_1 x + \cdots + u_d x^d \in \mathbb{K}\left[x\right]_{\leq d},$$

and transmit the e values $\mathbf{f}\left[a_1\right], \mathbf{f}\left[a_2\right], \ldots, \mathbf{f}\left[a_e\right]$ of this polynomial. The recepient will then receive e values of the polynomial $\mathbf{f}$. If all of these values have been transmitted correctly, then he will be able to pick any $d+1$ of these values[95] and use them to reconstruct $\mathbf{f}$ (and therefore, your messages $u_0, u_1, \ldots, u_d$) via Theorem 7.7.5. If at most $e-d-1$ of these e values get corrupted along the way, he will be able to recognize that something is wrong[96]. Thus, this code detects up to $e-d-1$ errors. It furthermore corrects up to $\left\lfloor \dfrac{e-d-1}{2} \right\rfloor$ errors (i.e., there is a way in which the recepient can guess your original messages, and if no more than $\left\lfloor \dfrac{e-d-1}{2} \right\rfloor$ of your e values have gotten corrupted, then his guess will be right).

This is called a *Reed–Solomon code*; such codes were used by the Voyager spacecraft and later in the storage of data on CDs and DVDs (as said above, storing data on a decaying medium is transmitting it through a noisy channel).

See [Childs00, Chapter 29] for more about these codes, and see textbooks on coding theory (e.g., [Garret07]) for much more.[97]

7.8. Generating functions

7.8.1. A binomial identity

Let me show a further application of the "polynomial identity trick", which is interesting in that it uses polynomials in two different ways.

[94] Of course, an element of $\mathbb{K}$ is more likely to get corrupted along the way than a single bit (if $|\mathbb{K}| > 2$), because it will be encoded as several bits (and each of them can get corrupted). But this is par for the course: After all, an element of $\mathbb{K}$ carries more information than a bit, too.

[95] He can do this, since $e \geq d+1$.

[96] e.g., by attempting to recover $\mathbf{f}$ using some $d+1$ of the values, and then checking whether the resulting polynomial also fits the remaining $e-d-1$ values

[97] Be aware that there are several different ways of defining Reed–Solomon codes; the one in [Garret07] is not the same as ours.

Among many properties of Pascal's triangle, one rather famous one is that the sum of all entries in the n-th row is 2^n. That is,

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \qquad \text{for each } n \in \mathbb{N}.$$

This is, in fact, the direct result of applying Theorem 2.17.13 to $x = 1$ and $y = 1$. Likewise, we can apply Theorem 2.17.13 to $x = -1$ and $y = 1$, and conclude that

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0^n = \begin{cases} 1, & \text{if } n = 0; \\ 0, & \text{if } n \neq 0 \end{cases} \qquad \text{for each } n \in \mathbb{N}.$$

In other words, the alternating sum of all entries in the n-th row of Pascal's triangle is 0, unless $n = 0$ (in which case it is 1).

One may wonder what happens if we start summing higher powers of the entries of a row of Pascal's triangle. For example, the sum of their squares has a nice formula:

Proposition 7.8.1. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}.$$

Now, what about the alternating sum of the squares of the elements of the n-th row of Pascal's triangle? Here, the formula turns out to be just as neat, apart from having two cases to distinguish:

Proposition 7.8.2. Let $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}^2 = \begin{cases} (-1)^{n/2} \binom{n}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

Just as we derived Proposition 7.8.1 from Theorem 2.17.14, we are going to derive Proposition 7.8.2 from the following fact:

Theorem 7.8.3. Let $u \in \mathbb{Q}$ and $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} (-1)^k \binom{u}{k} \binom{u}{n-k} = \begin{cases} (-1)^{n/2} \binom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

Theorem 7.8.3 can be proven in an elementary, computational way (see [Grinbe15, Second solution to Exercise 3.22] for this proof). Let us, however, prove it by applying polynomials strategically (this argument is [Grinbe15, First solution to Exercise 3.22], and is folklore). First, we prove the particular case of Theorem 7.8.3 for $u \in \mathbb{N}$:

Lemma 7.8.4. Let $u \in \mathbb{N}$ and $n \in \mathbb{N}$. Then,

$$\sum_{k=0}^{n} (-1)^k \binom{u}{k} \binom{u}{n-k} = \begin{cases} (-1)^{n/2} \binom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}.$$

Our proof of Lemma 7.8.4 is an example of the use of "generating functions": We have proven that two sequences $(a_0, a_1, a_2, \ldots)$ and $(b_0, b_1, b_2, \ldots)$ of numbers were equal[98] by showing that the two FPSs $\sum_{k \in \mathbb{N}} a_k x^k$ and $\sum_{k \in \mathbb{N}} b_k x^k$ are equal. (In our case, these two FPSs were actually the polynomials $\left(1 - x^2\right)^u$ and $(1-x)^u (1+x)^u$. But they don't have to be polynomials in order for the technique of generating functions to be applicable.) This technique is central to enumerative combinatorics, and also has many uses in pure algebra. See [Loehr11, Chapters 7 and 8] and [Wilf94] for (a lot) more about this technique.

We still need to prove Theorem 7.8.3, which generalizes Lemma 7.8.4 from $u \in \mathbb{N}$ to $u \in \mathbb{Q}$. Here, polynomials come useful once again (in the same way as they came useful when we were generalizing Lemma 2.17.15 to Lemma 2.17.17):

Remark 7.8.5. We now know

- the sum of all entries of the n-th row of Pascal's triangle (it is 2^n);
- the alternating sum of all entries of the n-th row of Pascal's triangle (it is 0 if $n \neq 0$, and 1 otherwise);
- the sum of the squares of all entries of the n-th row of Pascal's triangle (it is $\binom{2n}{n}$);
- the alternating sum of the squares of all entries of the n-th row of Pascal's triangle (see Proposition 7.8.2).

How does this pattern continue? We may ask for the sum $\sum_{k=0}^{n} \binom{n}{k}^3$ of all cubes of all entries of the n-th row of Pascal's triangle, as well as their alternating sum.

[98] In our case, the two sequences are given by $a_n = \sum_{k=0}^{n} (-1)^k \binom{u}{k} \binom{u}{n-k}$ and $b_n = \begin{cases} (-1)^{n/2} \binom{u}{n/2}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases}$ for all $n \in \mathbb{N}$.

The numbers $\sum_{k=0}^{n} \binom{n}{k}^3$ are known as the *Franel numbers* (OEIS sequence A000172); no explicit (sum-less) formula for them is known (unlike for the sums of squares).

As for the alternating sum, however, there is a nice formula:

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k}^3 = \begin{cases} (-1)^{n/2} \dfrac{(3n/2)!}{(n/2)!^3}, & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd} \end{cases} \qquad \text{for all } n \in \mathbb{N}.$$

In the case when n is odd, this formula is easy to check (indeed, in the sum $\sum_{k=0}^{n} (-1)^k \binom{n}{k}^3$, the addend for $k = u$ cancels the addend for $k = n - u$). In the case when n is even, it is a particular case of what is known as *Dixon's identity* (see, e.g., [Ward91]). The sequence of these alternating sums is OEIS sequence A245086.

Higher powers are even more complicated. For example, as far as fourth powers are concerned, neither $\sum_{k=0}^{n} \binom{n}{k}^4$ nor $\sum_{k=0}^{n} (-1)^k \binom{n}{k}^4$ has a known explicit form (see OEIS sequences A005260 and A228304).

7.8.2. Proving Lucas's congruence

Recall Lucas's congruence (Theorem 2.17.20), which we have left unproven back when we were studying binomial coefficients. Let us now outline how it can be proven using polynomials and FPSs. We first shall prove a particular case:

Lemma 7.8.6. Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Then, we have the four congruences

$$\binom{2a}{2b} \equiv \binom{a}{b} \bmod 2; \qquad \binom{2a}{2b+1} \equiv 0 \bmod 2;$$
$$\binom{2a+1}{2b} \equiv \binom{a}{b} \bmod 2; \qquad \binom{2a+1}{2b+1} \equiv \binom{a}{b} \bmod 2.$$

Lemma 7.8.6 is a very particular case of Theorem 2.17.20 – namely, the one when $p = 2$ and $a \in \mathbb{N}$ and $b \in \mathbb{N}$. (The four congruences correspond to the four different options for the pair $(c, d) \in \{0, 1, \ldots, p-1\}^2$.) Nevertheless, it is already the reason for a curious pattern: If you plot the first 2^n rows of Pascal's triangle (for some $n \in \mathbb{N}$), and color all odd entries black and all even entries white, then you obtain an (approximation to) Sierpinski's triangle (the fractal). Lemma 7.8.6 can be used to prove this (by induction on n).

Now, how can we extend this proof to a full proof of Theorem 2.17.20? As we know, Lemma 7.8.6 is the particular case of Theorem 2.17.20 for $p = 2$ and $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Thus, we need to lift the three restrictions $p = 2$, $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Here is a rough plan:

- To lift the restriction $b \in \mathbb{N}$, we simply observe that Theorem 2.17.20 is trivial in the case when $b \in \mathbb{Z}$ is negative. Indeed, if $b \in \mathbb{Z}$ is negative, then both $pb + d$ and b are negative (since $d \in \{0, 1, \ldots, p-1\}$ yields $d < p$, but $b < 0$ yields $pb \leq -p$), and therefore Theorem 2.17.20 boils down to the obvious congruence $0 \equiv 0 \binom{c}{d} \bmod p$.

- To lift the restriction $a \in \mathbb{N}$, we have to tweak our above proof so that it works for negative a as well. Of course, the first step is to use FPSs instead of polynomials. There are only two places in our proof where we have used the nonnegativity of a – namely, the two places where we applied Lemma 7.3.4. The first place was (**??**); the second was (**??**). So we have to prove (**??**) and (**??**) without using the requirement that $a \in \mathbb{N}$. But this is easy using Newton's binomial theorem. In fact, (**??**) follows directly from Theorem 7.3.3 **(b)** (applied to $u = 2a + 1$), whereas (**??**) follows by first applying Theorem 7.3.3 **(b)** to $u = a$ and then substituting x^2 for x. (As we explained in Remark 7.6.6, not every element of a $\mathbb{K}$-algebra can be substituted into an FPS; but x^2 can always be substituted into an FPS, and the usual properties of substitution – such as it being a $\mathbb{K}$-algebra homomorphism – are satisfied.)

- Finally, how can we lift the restriction that p be a prime? Recall that we used the identity $(1 + x)^2 = 1 + x^2$ (in $(\mathbb{Z}/2)[x]$) in our above proof. This has to be replaced by the identity

$$(1 + x)^p = 1 + x^p \qquad \text{in } (\mathbb{Z}/p)[x].$$

  This identity is a consequence of Theorem 5.11.1 (applied to $\mathbb{K} = (\mathbb{Z}/p)[x]$, $a = 1$ and $b = x$), since $p \cdot 1_{(\mathbb{Z}/p)[x]} = 0$.

Thus, we obtain the following proof of Theorem 2.17.20 in full generality:

7.9. Invertible and nilpotent polynomials

In Subsection 7.3.1, we have seen when an FPS $\mathbf{a} \in \mathbb{K}[[x]]$ is invertible in the ring $\mathbb{K}[[x]]$. When is a polynomial $\mathbf{a} \in \mathbb{K}[x]$ invertible in the ring $\mathbb{K}[x]$?

The first hint that the answer is different comes from the example of $1 + x$. As we know, the FPS $1 + x$ is invertible in $\mathbb{K}[[x]]$. Since this FPS is actually a polynomial, we might wonder whether it is invertible in $\mathbb{K}[x]$ as well. The answer is "no", unless the ring $\mathbb{K}$ is trivial.[99] More generally, we can easily characterize the invertible elements of $\mathbb{K}[x]$ when $\mathbb{K}$ is a field:

[99] Indeed, if it was invertible in $\mathbb{K}[x]$, then its multiplicative inverse in $\mathbb{K}[x]$ would also be its multiplicative inverse in $\mathbb{K}[[x]]$; but we already know that the latter is $1 - x + x^2 - x^3 \pm \cdots$ and therefore does not belong to $\mathbb{K}[x]$ unless $\mathbb{K}$ is trivial.

Proposition 7.9.1. Let $\mathbb{K}$ be a field. Let $\mathbf{a} \in \mathbb{K}[x]$ be a polynomial. Then, $\mathbf{a}$ is invertible in $\mathbb{K}[x]$ if and only if $\deg \mathbf{a} = 0$ (that is, $\mathbf{a}$ is a nonzero constant polynomial).

If the ring $\mathbb{K}$ is not a field, the situation becomes more interesting: As we have already seen, the polynomial $1 + 2x$ is invertible when $\mathbb{K} = \mathbb{Z}/4$, despite its degree not being 0, so Proposition 7.9.1 would no longer hold here. Instead, we can give a necessary and sufficient criterion based on the notion of *nilpotent elements*. Let us define this notion:

Definition 7.9.2. Let $\mathbb{L}$ be a ring. Let $a \in \mathbb{L}$. We say that a is *nilpotent* if there exists an $r \in \mathbb{N}$ satisfying $a^r = 0$.

In other words, an element a of a ring $\mathbb{L}$ is nilpotent if one of its powers is 0.
For example:

- The element 0 of any ring $\mathbb{L}$ is nilpotent, since $0^r = 0$ holds for $r = 1$.
- If $m \in \mathbb{Z}$ and $k \in \mathbb{N}$, then the element $[m]_{m^k}$ of $\mathbb{Z}/m^k$ is nilpotent, since its k-th power is $\left[m^k\right]_{m^k} = 0$.
- The nilpotent elements of a matrix ring $\mathbb{K}^{n\times n}$ are exactly the nilpotent $n \times n$-matrices. It is well-known that any nilpotent $n \times n$-matrix A over a field $\mathbb{K}$ satisfies $A^n = 0$; but this is not always true when $\mathbb{K}$ is not a field.

If $\mathbb{K}$ is a field, then the only nilpotent element of $\mathbb{K}$ is 0 (this can be easily proven using Exercise 5.5.2).

Let us state two basic and simple properties of nilpotent elements:

Proposition 7.9.3. Let $\mathbb{L}$ be a ring. Let a and b be two nilpotent elements of $\mathbb{L}$ such that $ab = ba$. Then, $a + b$ is also nilpotent.

The requirement $ab = ba$ in Proposition 7.9.3 cannot be removed: e.g., the two matrices $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$ in $\mathbb{Q}^{2\times 2}$ are nilpotent, but their sum $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is not.

Proposition 7.9.4. Let $\mathbb{L}$ be a ring. Let u be an invertible element of $\mathbb{L}$. Let a be a nilpotent element of $\mathbb{L}$ such that $ua = au$. Then, the element $u - a$ of $\mathbb{L}$ is invertible.

Now, when is a polynomial $\mathbf{a} \in \mathbb{K}[x]$ invertible in $\mathbb{K}[x]$? The answer is given by the following result:

Theorem 7.9.5. Let $\mathbf{a} \in \mathbb{K}[x]$ (where $\mathbb{K}$, still, is a commutative ring). Then, $\mathbf{a}$ is invertible in $\mathbb{K}[x]$ if and only if

- its coefficient $[x^0]\,\mathbf{a}$ is invertible in $\mathbb{K}$, **and**
- its coefficients $[x^n]\,\mathbf{a}$ are nilpotent for all positive integers n.

For example, the polynomial $\mathbf{a} = 1 + 2x$ over $\mathbb{K} = \mathbb{Z}/4$ satisfies this condition, since its coefficient $[x^0]\,\mathbf{a} = [1]_4$ is invertible in $\mathbb{Z}/4$ whereas its other coefficients (which are $[2]_4, [0]_4, [0]_4, [0]_4, \ldots$) are nilpotent.

We will not prove Theorem 7.9.5 here. We only notice that its "$\Longleftarrow$" direction is fairly easy (using Proposition 7.9.3 and Proposition 7.9.4), while its "$\Longrightarrow$" direction is proven in `https://math.stackexchange.com/a/392604/` .

Note the stark contrast between Theorem 7.9.5 and Theorem 7.3.1.

Now that we have introduced nilpotent elements, we might also wonder when a polynomial is nilpotent. This can also be answered:

Theorem 7.9.6. Let $\mathbf{a} \in \mathbb{K}[x]$ (where $\mathbb{K}$, still, is a commutative ring). Then, $\mathbf{a}$ is nilpotent if and only if its coefficients $[x^n]\,\mathbf{a}$ are nilpotent for all $n \in \mathbb{N}$.

Again, we omit the proof of this theorem.

Note that Theorem 7.9.6 has no analogue for FPSs: An FPS can fail to be nilpotent even if all its coefficients are nilpotent.

Let us briefly note that the non-invertibility of most polynomials over a field can be amended: We can introduce formal fractions of polynomials over a field in the same way as formal fractions of integers (also known as "rational numbers") were defined. These fractions are called *rational functions*[100].

7.10. Functoriality of power series and polynomial rings

The polynomial ring $\mathbb{K}[x]$, and the ring $\mathbb{K}[[x]]$ of FPSs, are defined for every ring $\mathbb{K}$. How do they depend on $\mathbb{K}$? For example, does $\mathbb{Z}[x]$ lie in $\mathbb{Q}[x]$ in the same way $\mathbb{Z}$ lies in $\mathbb{Q}$? The answer is a "yes", for fairly simple reasons:

Proposition 7.10.1. Let $\mathbb{K}$ be a subring of a commutative ring $\mathbb{L}$. Then:
(a) The polynomial ring $\mathbb{K}[x]$ is a subring of $\mathbb{L}[x]$.
(b) The ring $\mathbb{K}[[x]]$ is a subring of $\mathbb{L}[[x]]$.

So being a subring is "inherited" to polynomial rings and rings of FPSs.

Does a homomorphism between two commutative rings also yield a homomorphism between their polynomial rings or a homomorphism between their FPS rings? The next theorem shows that the answer is "yes" to both questions:

[100] This is a confusing name, because polynomials are not functions. It is an artifact of the history of the subject.

Theorem 7.10.2. Let $\mathbb{K}$ and $\mathbb{L}$ be two commutative rings. Let $f : \mathbb{K} \to \mathbb{L}$ be a ring homomorphism.

(a) Then, the map

$$\mathbb{K}[[x]] \to \mathbb{L}[[x]],$$
$$(a_0, a_1, a_2, \ldots) \mapsto (f(a_0), f(a_1), f(a_2), \ldots)$$

is a ring homomorphism.

(b) Its restriction to $\mathbb{K}[x]$ is a ring homomorphism from $\mathbb{K}[x]$ to $\mathbb{L}[x]$.

8. Quotient constructions

8.1. Residue classes in commutative rings

8.1.1. The general case

We have previously defined

- what it means for an **integer** to divide an integer (Definition 2.2.1);
- what it means for a **Gaussian integer** to divide a Gaussian integer (Definition 4.2.17);
- what it means for a **polynomial** to divide a polynomial (Definition 7.6.8).

These definitions differed only in what kind of "numbers" we were using. So let us generalize them all together:

Definition 8.1.1. Let $\mathbb{L}$ be a commutative ring. Let a and b be two elements of $\mathbb{L}$. We say that $a \mid b$ *in* $\mathbb{L}$ (or "*a divides b in* $\mathbb{L}$" or "*b* is *divisible by a in* $\mathbb{L}$" or "*b* is a *multiple* of *a in* $\mathbb{L}$") if there exists a $c \in \mathbb{L}$ such that $b = ac$.

We furthermore say that $a \nmid b$ *in* $\mathbb{L}$ if a does not divide b *in* $\mathbb{L}$.

We shall omit the words "in $\mathbb{L}$" whenever $\mathbb{L}$ is clear. But keep in mind that $\mathbb{L}$ matters. For example, $2 \nmid 1$ in $\mathbb{Z}$, but $2 \mid 1$ in $\mathbb{Q}$ (since $1 = 2 \cdot \frac{1}{2}$). Of course, when we speak of divisibility between integers, we mean "in $\mathbb{Z}$", since divisibility in $\mathbb{Q}$ is boring[101].

Most of the standard properties of divisibility still work for any commutative ring $\mathbb{L}$. For example:

- we have $a \mid a$ for all $a \in \mathbb{L}$;

[101] More generally: If $\mathbb{F}$ is any field, then divisibility in $\mathbb{F}$ is boring (because $a \mid b$ holds for any $a, b \in \mathbb{F}$ unless we have $a = 0$ and $b \neq 0$).

- if $a, b, c \in \mathbb{L}$ satisfy $a \mid b$ and $b \mid c$, then $a \mid c$,

and so on. (But, for example, the obvious generalization of Exercise 2.2.3 does not work: In general, we cannot conclude $a \mid b$ from $ac \mid bc$ even if $c \neq 0$.)

We can furthermore generalize the concept of congruence (Definition 2.3.1 and Definition 4.2.21) to arbitrary commutative rings:

Definition 8.1.2. Let $\mathbb{L}$ be a commutative ring. Let $w, a, b \in \mathbb{L}$. We say that *a is congruent to b modulo w (in $\mathbb{L}$)* if and only if $w \mid a - b$. We shall use the notation "$a \equiv b \bmod w$" for "a is congruent to b modulo w".

We furthermore shall use the notation "$a \not\equiv b \bmod w$" for "a is not congruent to b modulo w".

Again, the standard properties of congruence all hold. For example, the following analogue of Proposition 2.3.4 holds (and is proven in the same way as Proposition 2.3.4):

Proposition 8.1.3. Let $\mathbb{L}$ be a commutative ring. Let $w \in \mathbb{L}$.

(a) We have $a \equiv a \bmod w$ for every $a \in \mathbb{L}$.

(b) If $a, b, c \in \mathbb{L}$ satisfy $a \equiv b \bmod w$ and $b \equiv c \bmod w$, then $a \equiv c \bmod w$.

(c) If $a, b \in \mathbb{L}$ satisfy $a \equiv b \bmod w$, then $b \equiv a \bmod w$.

(d) If $a_1, a_2, b_1, b_2 \in \mathbb{L}$ satisfy $a_1 \equiv b_1 \bmod w$ and $a_2 \equiv b_2 \bmod w$, then

$$a_1 + a_2 \equiv b_1 + b_2 \bmod w; \tag{115}$$

$$a_1 - a_2 \equiv b_1 - b_2 \bmod w; \tag{116}$$

$$a_1 a_2 \equiv b_1 b_2 \bmod w. \tag{117}$$

(e) Let $m \in \mathbb{L}$ be such that $m \mid w$. If $a, b \in \mathbb{L}$ satisfy $a \equiv b \bmod w$, then $a \equiv b \bmod m$.

Now, we can define the straightforward generalization of residue classes (Definition 3.4.2 and Definition 3.4.3) and of the standard operations (addition, multiplication and scaling) on them (Definition 3.4.12 and Definition 3.4.18):

Definition 8.1.4. Fix a commutative ring $\mathbb{L}$ and an element $w \in \mathbb{L}$.

(a) Define a relation $\underset{w}{\equiv}$ on the set $\mathbb{L}$ by

$$\left(a \underset{w}{\equiv} b\right) \Longleftrightarrow \left(a \equiv b \bmod w\right).$$

This $\underset{w}{\equiv}$ is an equivalence relation. (The proof of this is analogous to the proof of Example 3.2.5.)

(b) A *residue class modulo w* means an equivalence class of the relation $\underset{w}{\equiv}$.

(c) If $a \in \mathbb{L}$, then we denote the residue class $\left[a\right]_{\underset{w}{\equiv}}$ by $\left[a\right]_w$.

(d) The set $\mathbb{L} / \underset{w}{\equiv}$ of all residue classes modulo w is called $\mathbb{L}/w$.

(e) We define a binary operation $+$ on $\mathbb{L}/w$ (called *addition*) by setting

$$[a]_w + [b]_w = [a+b]_w \qquad \text{for all } a, b \in \mathbb{L}.$$

This is well-defined, because of Theorem 8.1.5 **(a)** below.

(f) We define a binary operation $\cdot$ on $\mathbb{L}/w$ (called *multiplication*) by setting

$$[a]_w \cdot [b]_w = [a \cdot b]_w \qquad \text{for all } a, b \in \mathbb{L}.$$

This is well-defined, because of Theorem 8.1.5 **(a)** below.

(g) Fix $r \in \mathbb{L}$. For any $\alpha \in \mathbb{L}/w$, we define a residue class $r\alpha \in \mathbb{L}/w$ by setting

$$\left(r\,[a]_w = [ra]_w \qquad \text{for any } a \in \mathbb{L}\right).$$

(In other words, for any $\alpha \in \mathbb{L}/w$, we let $r\alpha = [ra]_w$, where a is an element of $\mathbb{L}$ satisfying $\alpha = [a]_w$.) This is well-defined, because of Theorem 8.1.5 **(a)** below.

We shall also write $r \cdot \alpha$ instead of $r\alpha$. The map $\mathbb{L} \times (\mathbb{L}/w) \to \mathbb{L}/w$, $(r, \alpha) \mapsto r\alpha$ will be called *scaling*.

If we set $\mathbb{L} = \mathbb{Z}$ in Definition 8.1.4, and let w be an integer n, then we recover our old definitions of residue classes modulo n and of their set $\mathbb{Z}/n$. Note that we are not defining a subtraction on $\mathbb{L}/w$ this time, because we will get it for free once we recognize $\mathbb{L}/w$ as a ring.

Theorem 8.1.5. Fix a commutative ring $\mathbb{L}$ and an element $w \in \mathbb{L}$.

(a) The operations $+$ and $\cdot$ and the "scaling map" $\cdot$ in Definition 8.1.4 are well-defined.

(b) The set $\mathbb{L}/w$, equipped with the addition $+$ (defined in Definition 8.1.4 **(e)**), the multiplication $\cdot$ (defined in Definition 8.1.4 **(f)**) and the zero $[0]_w$ and the unity $[1]_w$, is a commutative ring.

(c) The set $\mathbb{L}/w$, equipped with the addition $+$ (defined in Definition 8.1.4 **(e)**), the scaling $\cdot$ (defined in Definition 8.1.4 **(g)**) and the zero vector $[0]_w$, is an $\mathbb{L}$-module.

(d) The set $\mathbb{L}/w$, equipped with all of these items, is a commutative $\mathbb{L}$-algebra.

(e) The map

$$\begin{aligned} \pi_w : \mathbb{L} &\to \mathbb{L}/w, \\ a &\mapsto [a]_w \end{aligned}$$

is an $\mathbb{L}$-algebra homomorphism.

Definition 8.1.6. Consider the setting of Theorem 8.1.5.

The commutative $\mathbb{L}$-algebra $\mathbb{L}/w$ constructed in Theorem 8.1.5 **(d)** is called "$\mathbb{L}$ *modulo* w" or "$\mathbb{L}$ *divided by* w" or "$\mathbb{L}$ *quotiented by* w". Whenever we speak of "the $\mathbb{L}$-algebra $\mathbb{L}/w$", we shall mean this precise $\mathbb{L}$-algebra.

The reader can easily check the following:

- If we have $w = 0$ in Theorem 8.1.5, then the map π_w is an $\mathbb{L}$-algebra isomorphism, so that $\mathbb{L}/0 \cong \mathbb{L}$ as rings and as $\mathbb{L}$-modules.
- If we have $w = 1$ in Theorem 8.1.5, then the ring $\mathbb{L}/w = \mathbb{L}/1$ is trivial. More generally, if $w \in \mathbb{L}$ is invertible, then the ring $\mathbb{L}/w$ is trivial.

8.1.2. The case of a polynomial ring

The commutative $\mathbb{L}$-algebra $\mathbb{L}/w$ constructed in Theorem 8.1.5 **(d)** generalizes not just the $\mathbb{Z}$-algebras $\mathbb{Z}/n$, but also the $\mathbb{Z}[i]$-algebras $\mathbb{Z}[i]/\alpha$ (where α is a Gaussian integer). But we can apply this construction to other rings $\mathbb{L}$ as well. It will prove particularly useful to apply it to $\mathbb{L} = \mathbb{K}[x]$, where $\mathbb{K}$ is a commutative ring. In particular, this will help us adjoin a root of a polynomial to a commutative ring $\mathbb{K}$. First, let us introduce some standard conventions:

Convention 8.1.7. Let $\mathbb{K}$ be a commutative ring.

(a) Any $\mathbb{K}[x]$-module automatically becomes a $\mathbb{K}$-module: In fact, let M be a $\mathbb{K}[x]$-module. Then, $\mathbf{a}m$ is defined for each $\mathbf{a} \in \mathbb{K}[x]$ and each $m \in M$. But we have identified each element $a \in \mathbb{K}$ with the corresponding constant polynomial $\underline{a} \in \mathbb{K}[x]$. Thus, am is also defined for each $a \in \mathbb{K}$ and each $m \in M$ (because we can treat a as a constant polynomial); explicitly speaking, it is defined by the equality

$$am = \underline{a}m \qquad \text{for all } a \in \mathbb{K} \text{ and } m \in M.$$

Thus, a "scaling" map $\cdot : \mathbb{K} \times M \to M$ is defined. This "scaling" map (along with the addition and the zero vector that M is already equipped with) makes M a $\mathbb{K}$-module. Thus, every $\mathbb{K}[x]$-module M automatically becomes a $\mathbb{K}$-module.

(b) In this way, any $\mathbb{K}[x]$-algebra becomes a $\mathbb{K}$-algebra (because we just explained how it becomes a $\mathbb{K}$-module, and it is easy to see that this $\mathbb{K}$-module structure harmonizes with the ring structure in a way that yields a $\mathbb{K}$-algebra[102]).

(c) Any $\mathbb{K}[x]$-module homomorphism is automatically a $\mathbb{K}$-module homomorphism. (This is easy to check.)

(d) Any $\mathbb{K}[x]$-algebra homomorphism is automatically a $\mathbb{K}$-algebra homomorphism. (This is easy to check.)

Thus, in particular, if $\mathbf{b} \in \mathbb{K}[x]$ is any polynomial, then the $\mathbb{K}[x]$-algebra $\mathbb{K}[x]/\mathbf{b}$ automatically becomes a $\mathbb{K}$-algebra as well.

Proposition 8.1.8. Let $\mathbb{K}$ be a commutative ring. Let $\mathbf{b} \in \mathbb{K}[x]$ be a polynomial.

(a) The projection map

$$\begin{aligned} \pi_{\mathbf{b}} : \mathbb{K}[x] &\to \mathbb{K}[x]/\mathbf{b}, \\ \mathbf{a} &\mapsto [\mathbf{a}]_{\mathbf{b}} \end{aligned}$$

[102] i.e., the "Scale-invariance of multiplication" axiom is satisfied

is a $\mathbb{K}[x]$-algebra homomorphism and thus a $\mathbb{K}$-algebra homomorphism.

(b) The map

$$\begin{aligned} \mathbb{K} &\to \mathbb{K}[x]/\mathbf{b}, \\ a &\mapsto [\underline{a}]_{\mathbf{b}} \end{aligned}$$

is a $\mathbb{K}$-algebra homomorphism.

(c) We have $\mathbf{a}\,[[x]_{\mathbf{b}}] = [\mathbf{a}]_{\mathbf{b}}$ for any $\mathbf{a} \in \mathbb{K}[x]$.

(d) The element $[x]_{\mathbf{b}} \in \mathbb{K}[x]/\mathbf{b}$ is a root of $\mathbf{b}$.

Theorem 8.1.9. Let $\mathbb{K}$ be a commutative ring.

Let $m \in \mathbb{N}$. Let $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ be such that $[x^m]\,\mathbf{b} \in \mathbb{K}$ is invertible. Then:

(a) Each element of $\mathbb{K}[x]/\mathbf{b}$ can be uniquely written in the form

$$\lambda_0 \left[x^0\right]_{\mathbf{b}} + \lambda_1 \left[x^1\right]_{\mathbf{b}} + \cdots + \lambda_{m-1} \left[x^{m-1}\right]_{\mathbf{b}} \qquad \text{with } \lambda_0, \lambda_1, \ldots, \lambda_{m-1} \in \mathbb{K}.$$

(b) The m vectors $\left[x^0\right]_{\mathbf{b}}, \left[x^1\right]_{\mathbf{b}}, \ldots, \left[x^{m-1}\right]_{\mathbf{b}}$ form a basis of the $\mathbb{K}$-module $\mathbb{K}[x]/\mathbf{b}$. (See Definition 6.11.1 **(d)** for what "basis" means.)

(c) Assume that $m > 0$. Then, the $\mathbb{K}$-algebra homomorphism

$$\begin{aligned} \mathbb{K} &\to \mathbb{K}[x]/\mathbf{b}, \\ a &\mapsto [\underline{a}]_{\mathbf{b}} \end{aligned}$$

is injective. Thus, $\mathbb{K}$ can be viewed as a $\mathbb{K}$-subalgebra of $\mathbb{K}[x]/\mathbf{b}$ if we identify each $a \in \mathbb{K}$ with the $[\underline{a}]_{\mathbf{b}} \in \mathbb{K}[x]/\mathbf{b}$.

Note that Theorem 8.1.9 **(c)** really requires m to be > 0 (otherwise, $\mathbb{K}[x]/\mathbf{b}$ is a trivial ring) and $[x^m]\,\mathbf{b}$ to be invertible (we will see an example below where $[x^m]\,\mathbf{b}$ is not invertible, and $\mathbb{K}$ does not inject into $\mathbb{K}[x]/\mathbf{b}$).

We now understand the quotient rings $\mathbb{K}[x]/\mathbf{b}$ well enough at least in the case when the leading coefficient of $\mathbf{b}$ is invertible. Let us use this to see some examples:

Example 8.1.10. We have $\mathbb{C} \cong \mathbb{R}[x]/\left(x^2+1\right)$ (as rings).

Indeed, the map

$$\begin{aligned} \mathbb{C} &\to \mathbb{R}[x]/\left(x^2+1\right), \\ (a,b) = a + bi &\mapsto [a+bx]_{x^2+1} \end{aligned}$$

is a ring homomorphism, and is invertible, with inverse

$$\begin{aligned} \mathbb{R}[x]/\left(x^2+1\right) &\to \mathbb{C}, \\ [\mathbf{a}]_{x^2+1} &\mapsto \mathbf{a}\,[i]. \end{aligned}$$

To see that the latter inverse is well-defined, you have to check that if $\mathbf{a}$ and $\mathbf{b}$ are two polynomials in $\mathbb{R}[x]$ satisfying $\mathbf{a} \equiv \mathbf{b} \bmod x^2+1$, then $\mathbf{a}\,[i] = \mathbf{b}\,[i]$. (LTTR.)

Example 8.1.11. We have $\mathbb{Z}[i] \cong \mathbb{Z}[x] / (x^2+1)$ (as rings).

Example 8.1.12. Recall the dual numbers $\mathbb{D}$ from homework set #4 exercise 3. Each dual number has the form $(a,b) = a + b\varepsilon$ for a unique pair (a,b) of real numbers, and the multiplication of $\mathbb{D}$ satisfies $\varepsilon^2 = 0$.

We have $\mathbb{D} \cong \mathbb{R}[x]/x^2$ (as rings). More precisely, the map

$$\begin{aligned} \mathbb{D} &\to \mathbb{R}[x]/x^2, \\ (a,b) = a + b\varepsilon &\mapsto [a+bx]_{x^2} \end{aligned}$$

is a ring isomorphism.

Moreover, we also have $\mathbb{D} \cong \mathbb{R}[[x]]/x^2$ as rings.

Note, however, that this is unusual: Normally, if $\mathbf{a} \in \mathbb{K}[x]$ is a polynomial, then $\mathbb{K}[[x]]/\mathbf{a}$ is not isomorphic to $\mathbb{K}[x]/\mathbf{a}$. For example, the ring $\mathbb{R}[x] / (x^2+1)$ is isomorphic to $\mathbb{C}$ (as we have seen above), whereas the ring $\mathbb{R}[[x]] / (x^2+1)$ is trivial (since the FPS x^2+1 is invertible, and thus any two FPSs are congruent to each other modulo x^2+1).

Example 8.1.13. In Section 5.6, we constructed a field with 4 elements by adjoining a j satisfying $j^2 = j+1$ to $\mathbb{Z}/2$. This field is isomorphic to

$$(\mathbb{Z}/2)[x] / \left(x^2 - x - 1\right).$$

Example 8.1.14. Let $m \in \mathbb{Z}$ be nonzero. On midterm #2 exercise 1, we defined R_m to be the set of all m-integers (= rational numbers that can be turned into integers by multiplying with m often enough). We proved that R_m is a ring. Each element of R_m can be written in the form $\dfrac{a}{m^k}$ for some $a \in \mathbb{Z}$ and some $k \in \mathbb{N}$ (but these a and k are not unique, since $\dfrac{a}{m^k} = \dfrac{am}{m^{k+1}} = \dfrac{am^2}{m^{k+2}} = \cdots$).

This ring R_m is isomorphic to the ring $\mathbb{Z}[x] / (mx-1)$. Indeed, we have a ring homomorphism

$$\begin{aligned} \mathbb{Z}[x] / (mx-1) &\to R_m, \\ [\mathbf{a}]_{mx-1} &\mapsto \mathbf{a}\left[\frac{1}{m}\right], \end{aligned}$$

and this is invertible, with inverse

$$\begin{aligned} &R_m \to \mathbb{Z}[x] / (mx-1), \\ &\frac{a}{m^k} \mapsto \left[ax^k\right]_{mx-1} \qquad \text{(for } a \in \mathbb{Z} \text{ and } k \in \mathbb{N}\text{)} \end{aligned}$$

(you have to check that this is well-defined).

Note that Theorem 8.1.9 does not apply here (unless $m \in \{1, -1\}$), and the $\mathbb{Z}$-module R_m has no basis (again, unless $m \in \{1, -1\}$).

Note that R_m (the ring of m-integers) is commonly called $\mathbb{Z}\left[\frac{1}{m}\right]$, in analogy to $\mathbb{Z}[i]$.

Example 8.1.15. We have a ring isomorphism

$$(\mathbb{Z}/6)[x] / (2x+1) \cong \mathbb{Z}/3.$$

Thus, if we adjoin a root of $2x+1$ to the ring $\mathbb{Z}/6$, then we get a smaller ring (namely, $\mathbb{Z}/3$). In particular, there is no injective map from $\mathbb{Z}/6$ to the result of this adjunction!

This is no surprise, since $\left[x^1\right](2x+1) = [2]_6$ is not invertible in $\mathbb{Z}/6$, and thus Theorem 8.1.9 does not apply here.

This is similar to how dividing by 0 makes all numbers equal:

$$\mathbb{Z}[x] / (0x-1) \cong \{0\}.$$

Let us summarize: We can always adjoin a root of a polynomial $\mathbf{b}$ to a commutative ring $\mathbb{K}$ by forming the ring $\mathbb{K}[x]/\mathbf{b}$. This latter ring will always be a commutative ring; moreover, if $\mathbf{b}$ is "nice" (that is, there is a positive integer m such that $\mathbf{b} \in \mathbb{K}[x]_{\leq m}$ and such that $[x^m]\,\mathbf{b}$ is invertible), then Theorem 8.1.9 **(c)** shows that this latter ring will contain $\mathbb{K}$ as a subring (at least if we make a natural identification). If $\mathbf{b}$ is not as "nice", then the ring $\mathbb{K}[x]/\mathbf{b}$ may fail to contain $\mathbb{K}$ as a subring (though it is always a $\mathbb{K}$-algebra), and may be smaller than $\mathbb{K}$ and even trivial.

If $\mathbb{K}$ itself is a field, then $\mathbf{b}$ will always be "nice" (unless $\mathbf{b} = 0$), but the ring $\mathbb{K}[x]/\mathbf{b}$ may and may not be a field. What must a polynomial $\mathbf{b}$ satisfy in order for $\mathbb{K}[x]/\mathbf{b}$ to be a field?

Definition 8.1.16. Let $\mathbb{F}$ be a field.

A polynomial $\mathbf{a} \in \mathbb{F}[x]$ is said to be *irreducible* if $\deg \mathbf{a} > 0$ and there exist no two polynomials $\mathbf{b}, \mathbf{c} \in \mathbb{F}[x]$ with $\mathbf{a} = \mathbf{bc}$ and $\deg \mathbf{b} > 0$ and $\deg \mathbf{c} > 0$.

In other words, a polynomial $\mathbf{a} \in \mathbb{F}[x]$ is said to be *irreducible* if it is non-constant but cannot be written as a product of two non-constant polynomials. (Indeed, the non-constant polynomials are precisely the polynomials having degree > 0.)

Irreducible polynomials over a field $\mathbb{F}$ are an analogue of prime numbers (or, to be more precise, of integers of the form $\pm p$ where p is a prime).

Theorem 8.1.17. Let $\mathbb{F}$ be a field. Let $\mathbf{a} \in \mathbb{F}[x]$ be a polynomial.
Then, the ring $\mathbb{F}[x]/\mathbf{a}$ is a field if and only if $\mathbf{a}$ is irreducible.

So, for example, the irreducible polynomial x^2+1 over $\mathbb{R}$ yields the field $\mathbb{R}[x]/\left(x^2+1\right)$ (which is $\cong \mathbb{C}$), but the non-irreducible polynomial x^2 over $\mathbb{R}$ yields the non-field $\mathbb{R}[x]/x^2$ (which is $\cong \mathbb{D}$).

8.2. Quotients modulo ideals

8.2.1. Congruence and quotients modulo ideals

The notion of "congruence modulo w" introduced in Definition 8.1.2 was a generalization of "congruence modulo n" from number theory; but it can be generalized further. Namely, we can replace w by an ideal I of $\mathbb{L}$. (See Definition 6.12.5 for the definition of an ideal.) Here is how this general notion is defined:

Definition 8.2.1. Let $\mathbb{L}$ be a ring. Let I be an ideal of $\mathbb{L}$. Let $a, b \in \mathbb{L}$. We say that *a is congruent to b modulo I (in $\mathbb{L}$)* if and only if $a - b \in I$. We shall use the notation "$a \equiv b \bmod I$" for "a is congruent to b modulo I".

We furthermore shall use the notation "$a \not\equiv b \bmod I$" for "a is not congruent to b modulo I".

Why is this a generalization of "congruence modulo w"? Because congruence modulo w is recovered if we take I to be the principal ideal[103] $w\mathbb{L}$. More precisely, the following holds:

Proposition 8.2.2. Let $\mathbb{L}$ be a commutative ring. Let $w \in \mathbb{L}$. Let $a, b \in \mathbb{L}$. Consider the principal ideal $w\mathbb{L}$ of $\mathbb{L}$, defined as in Example 6.12.6 (that is, by $w\mathbb{L} = \{wz \mid z \in \mathbb{L}\}$). Then, $a \equiv b \bmod w$ holds if and only if $a \equiv b \bmod w\mathbb{L}$.

Knowing that "congruence modulo I" is a generalization of "congruence modulo w" and of "congruence modulo n", we can play the usual game in which we recall properties of the latter and check whether they still hold for the former. For example, the following generalization of Proposition 8.1.3 holds:

Proposition 8.2.3. Let $\mathbb{L}$ be a ring. Let I be an ideal of $\mathbb{L}$.
(a) We have $a \equiv a \bmod I$ for every $a \in \mathbb{L}$.
(b) If $a, b, c \in \mathbb{L}$ satisfy $a \equiv b \bmod I$ and $b \equiv c \bmod I$, then $a \equiv c \bmod I$.
(c) If $a, b \in \mathbb{L}$ satisfy $a \equiv b \bmod I$, then $b \equiv a \bmod I$.
(d) If $a_1, a_2, b_1, b_2 \in \mathbb{L}$ satisfy $a_1 \equiv b_1 \bmod I$ and $a_2 \equiv b_2 \bmod I$, then

$$a_1 + a_2 \equiv b_1 + b_2 \bmod I; \tag{118}$$
$$a_1 - a_2 \equiv b_1 - b_2 \bmod I; \tag{119}$$
$$a_1 a_2 \equiv b_1 b_2 \bmod I. \tag{120}$$

[103] See Example 6.12.6 for the definition of principal ideals.

(e) Let J be an ideal of $\mathbb{L}$ such that $I \subseteq J$. If $a, b \in \mathbb{L}$ satisfy $a \equiv b \bmod I$, then $a \equiv b \bmod J$.

Note how the "$I \subseteq J$" assumption in Proposition 8.2.3 **(e)** is the correct generalization of the "$m \mid w$" assumption in Proposition 8.1.3, because of the following fact:

Proposition 8.2.4. Let $\mathbb{L}$ be a commutative ring. Let $m, w \in \mathbb{L}$. Then, $w\mathbb{L} \subseteq m\mathbb{L}$ holds if and only if $m \mid w$. (Here, the principal ideals $w\mathbb{L}$ and $m\mathbb{L}$ are defined as in Example 6.12.6).

This proposition is so easy it barely needs proof, but it illustrates a useful point of view: Divisibility of elements of $\mathbb{L}$ can be rewritten as containment of ideals of $\mathbb{L}$.

The following definition generalizes Definition 8.1.4 (and thus also generalizes our construction of $\mathbb{Z}/n$ for $n \in \mathbb{Z}$):

Definition 8.2.5. Fix a ring $\mathbb{L}$ and an ideal I of $\mathbb{L}$.

(a) Define a relation $\underset{I}{\equiv}$ on the set $\mathbb{L}$ by

$$\left(a \underset{I}{\equiv} b\right) \Longleftrightarrow \left(a \equiv b \bmod I\right).$$

This $\underset{I}{\equiv}$ is an equivalence relation. (The proof of this is analogous to the proof of Example 3.2.5.)

(b) A *residue class modulo I* means an equivalence class of the relation $\underset{I}{\equiv}$.

(c) If $a \in \mathbb{L}$, then we denote the residue class $\left[a\right]_{\underset{I}{\equiv}}$ by $\left[a\right]_I$.

(d) The set $\mathbb{L}/\underset{I}{\equiv}$ of all residue classes modulo I is called $\mathbb{L}/I$.

(e) We define a binary operation $+$ on $\mathbb{L}/I$ (called *addition*) by setting

$$\left[a\right]_I + \left[b\right]_I = \left[a+b\right]_I \qquad \text{for all } a, b \in \mathbb{L}.$$

This is well-defined, because of Theorem 8.2.6 **(a)** below.

(f) We define a binary operation $\cdot$ on $\mathbb{L}/I$ (called *multiplication*) by setting

$$\left[a\right]_I \cdot \left[b\right]_I = \left[a \cdot b\right]_I \qquad \text{for all } a, b \in \mathbb{L}.$$

This is well-defined, because of Theorem 8.2.6 **(a)** below.

(g) Fix $r \in \mathbb{L}$. For any $\alpha \in \mathbb{L}/I$, we define a residue class $r\alpha \in \mathbb{L}/I$ by setting

$$\left(r\left[a\right]_I = \left[ra\right]_I \qquad \text{for any } a \in \mathbb{L}\right).$$

(In other words, for any $\alpha \in \mathbb{L}/I$, we let $r\alpha = \left[ra\right]_I$, where a is an element of $\mathbb{L}$ satisfying $\alpha = \left[a\right]_I$.) This is well-defined, because of Theorem 8.2.6 **(a)** below.

We shall also write $r \cdot \alpha$ instead of $r\alpha$. The map $\mathbb{L} \times \left(\mathbb{L}/I\right) \to \mathbb{L}/I$, $\left(r, \alpha\right) \mapsto r\alpha$ will be called *scaling*.

Theorem 8.2.6. Fix a ring $\mathbb{L}$ and an ideal I of $\mathbb{L}$.

(a) The operations $+$ and $\cdot$ and the "scaling map" $\cdot$ in Definition 8.2.5 are well-defined.

(b) The set $\mathbb{L}/I$, equipped with the addition $+$ (defined in Definition 8.2.5 **(e)**), the multiplication $\cdot$ (defined in Definition 8.2.5 **(f)**) and the zero $[0]_I$ and the unity $[1]_I$, is a commutative ring.

(c) The set $\mathbb{L}/I$, equipped with the addition $+$ (defined in Definition 8.2.5 **(e)**), the scaling $\cdot$ (defined in Definition 8.2.5 **(g)**) and the zero vector $[0]_I$, is an $\mathbb{L}$-module when $\mathbb{L}$ is commutative.

(d) The set $\mathbb{L}/I$, equipped with all of these items, is an $\mathbb{L}$-algebra when $\mathbb{L}$ is commutative.

(e) The map

$$\begin{aligned} \pi_I : \mathbb{L} &\to \mathbb{L}/I, \\ a &\mapsto [a]_I \end{aligned}$$

is an $\mathbb{L}$-algebra homomorphism.

(f) If the ring $\mathbb{L}$ is commutative, then the ring $\mathbb{L}/I$ is a commutative $\mathbb{L}$-algebra.

(g) The kernel of the $\mathbb{L}$-algebra homomorphism π_I is $\operatorname{Ker}(\pi_I) = I$. (See Proposition 6.12.8 **(a)** for the definition of a kernel.)

Proposition 8.2.2 shows that Definition 8.2.5 generalizes Definition 8.1.4: Namely, if $\mathbb{L}$ is a commutative ring, and if the ideal I in Definition 8.2.5 is a principal ideal $w\mathbb{L}$ (for some $w \in \mathbb{L}$), then the relation $\underset{I}{\equiv}$ and the ring $\mathbb{L}/I$ are precisely the relation $\underset{w}{\equiv}$ and the ring $\mathbb{L}/w$ defined in Definition 8.1.4. Thus, if w is any element of a commutative ring $\mathbb{L}$, then

$$\mathbb{L}/w = \mathbb{L}/w\mathbb{L}.$$

Thus, in particular, $\mathbb{Z}/n = \mathbb{Z}/n\mathbb{Z}$ for any $n \in \mathbb{Z}$. Most authors prefer the notation $\mathbb{Z}/n\mathbb{Z}$ to our notation $\mathbb{Z}/n$ (since it is an instance of the more general construction $\mathbb{L}/I$).

9. Epilogue (UMN Fall 2019 Math 4281)

Here ends our one-semester course on abstract algebra (Fall 2019 at UMN). I will now tie up some loose ends and point into a few directions for further study.

9.1. Roads not taken

During the course of the past semester, we have learned new things about old concepts (such as the integers) as well as new concepts – both concrete (such as the Gaussian integers) and abstract (such as arbitrary rings and fields).

A one-semester course on abstract algebra always has to decide between many things of roughly equal importance; not everything can get its day[104]. The main topics we missed are:

- **Groups** (and monoids, and group homomorphisms, and subgroups, etc.). Many algebra classes **start** with this topic, since much of it can be done with almost no prerequisites. I have kept delaying this topic and, in the end, did not get to it at all. My main excuse is that it would have taken me afield – we haven't needed groups in what we did above (though they would have simplified a few of our proofs). Nevertheless, groups are worth learning about. Readable introductions into groups include [Siksek15], [GalQua17, §4.1–§4.2], [Goodma16, Chapters 1–5] and [Pinter10, Chapter 1–16]; other sources are [Armstr18, Abstract Algebra I] (with a historical perspective), [Artin10, Chapter 2], [Bosch18, Chapter 1], [Carrel17, Chapter 2], [Elman18, Chapters III–IV], [Knapp16a, Chapter IV], [Loehr11, Chapter 9], [Milne17].

  Only a few dozen pages of basic properties of groups will get you ready for the proof of Theorem 3.9.5, which we left unproved. See [GalQua17, §4.1–§4.2] or [Conrad*, "Cyclicity of $(\mathbf{Z}/(p))^\times$"] (for the case $n = p$).

- **Permutations**. The basics of this subject are extremely important throughout mathematics; in particular, the notion of the **sign** of a permutation is needed for the study of determinants of matrices and of signed volumes in geometry. Concerning this notion, see [Strick13, Appendix B] for a quick "from-scratch" introduction, and [Conrad*, "The sign of a permutation"] for an approach using group theory.

  You can learn more about permutations from a textbook on enumerative combinatorics (such as [Loehr11]) or on permutation puzzles (such as [Bump02], [Joyner08] or [Mulhol16]). The latter texts focus on permutation-related puzzles such as Rubik's cube and the 15-game; but in doing so, they motivate and introduce the properties of permutations and even the basics of group theory.

- **Determinants**. Determinants belong equally to combinatorics, abstract algebra and linear algebra. As a consequence, none of these courses covers them well; usually, only the most basic properties are stated, and their proofs outlined as best. Strickland, in [Strick13, §12 and Appendix B], gives a short but rigorous and honest treatment of the fundamentals. Other good introductions are found in Day's [Day16, Chapter 6], Mate's [Mate14], Walker's [Walker87, §5.4], and Pinkham's [Pinkha15, Chapter 11] (but they all limit themselves to the basics). In [Grinbe15, Chapter 6], I prove a variety of results (including some nonstandard ones) in much detail (probably too much). The "bible" on determinants is [MuiMet60] (and, for the particularly bold, [Muir30] is a goldmine of forgotten results).

[104]The alternative is to skimp on proofs; I consider this the worst option.

The determinant used to be one of the central notions in mathematics, and even predated the notion of matrices! (Determinants first appear in a 1693 letter of Leibniz. The word "matrix" was coined in 1850 by J. J. Sylvester, as a "womb" (this is what "matrix" means in Latin) from which determinants spring out.) Determinants have become less central since, thanks to abstract algebra incorporating many ideas that were first stated in their language. Nevertheless, they are still one of the strongest tools on the algebraic side of mathematics.

- **Multivariate polynomials** (i.e., polynomials in several variables). This is a highly useful topic, but it is rarely done justice in one-semester courses on algebra, since it takes some amount of notational work. For example, $3+2x+3x^2y+6y^2$ is a polynomial in the two variables x, y over the ring $\mathbb{Q}$. To define such polynomials rigorously, we recall that we defined FPSs in one variable as infinite sequences of elements of our ring $\mathbb{K}$. Likewise, we can define FPSs in two variables as infinite "2-dimensional sequences" of elements of $\mathbb{K}$, where a "2-dimensional sequence" is a family $\left(a_{i,j}\right)_{(i,j)\in\mathbb{N}^2}$ of elements of $\mathbb{K}$ indexed by pairs of nonnegative integers.[105] Such an FPS is called a polynomial if the family has only finitely many nonzero entries. Then, x is defined to be the family $\left(a_{i,j}\right)_{(i,j)\in\mathbb{N}^2}$ whose only nonzero entry is $a_{1,0}=1$, and y is defined to be the family $\left(a_{i,j}\right)_{(i,j)\in\mathbb{N}^2}$ whose only nonzero entry is $a_{0,1}=1$. The theory of polynomials (and FPSs) in two variables can thus be built up in analogy to our 1-variable theory; details can be found in [Hunger03, Chapter III, §5], [Loehr11, §7.16], [GalQua18, §30.2] and [AmaEsc05, §I.8].

  Eventually, the theory of multivariate polynomials becomes more complicated than the 1-variable theory. The first point where it significantly differs is division with remainder: There is no analogue of Theorem 7.5.1; instead there is a rich and highly useful theory of *Gröbner bases* ([CoLiOs15]). Also, a polynomial f in two variables x and y can be evaluated at two elements u and v of a $\mathbb{K}$-algebra U only if u and v commute (that is, $uv=vu$).

- **Galois theory** (i.e., the theory of field extensions and roots of polynomials). This is the study of *field extensions*. In the simplest case, this is about how a field $\mathbb{K}$ grows when a root of some polynomial is adjoined to it. We saw a small bit of it when we constructed $\mathbb{C}$, or finite fields of size p^2, by adjoining roots of quadratic polynomials; but the game can be played in greater gener-

[105] You can think of such a "2-dimensional sequence" as an infinite table

$$\begin{pmatrix} a_{0,0} & a_{0,1} & a_{0,2} & \cdots \\ a_{1,0} & a_{1,1} & a_{1,2} & \cdots \\ a_{2,0} & a_{2,1} & a_{2,2} & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

ality. When a field $\mathbb{K}$ is a subring of a field $\mathbb{L}$, the pair $(\mathbb{K}, \mathbb{L})$ is called a *field extension* (and is often written as $\mathbb{L}/\mathbb{K}$, a notation that has nothing to do with quotients despite its look). The Galois theory proper studies the $\mathbb{K}$-algebra isomorphisms from $\mathbb{L}$ to $\mathbb{L}$. (For example, there are two $\mathbb{R}$-algebra homomorphisms from $\mathbb{C}$ to $\mathbb{C}$; one of them is simply the identity map, while the other is the conjugation map $z \mapsto \overline{z}$. The dimension of the $\mathbb{R}$-vector space $\mathbb{C}$ also happens to be 2. Coincidence?)

A one-semester class on Galois theory usually covers only the very basics, but undergraduate-level introductions to the theory exist. Two of them are [Stewar15] and [Tignol01]. Some algebra texts centered on Galois theory are [Armstr18], [Goodma16] and [Bosch18].

- **Finite fields** (also known as Galois fields). We have started exploring them by defining the ones of size p and p^2 (for p prime). But as I already mentioned, there exists a finite field of any prime-power size, and it is unique up to isomorphism. Most algebra textbooks that go deeper than a one-semester course will prove this and perhaps say more – Galois theory texts in particular. But there are also books specifically devoted to finite fields, such as [Wan11] and [LidNie97].

Then, there are deeper topics such as representation theory, algebraic number theory and algebraic geometry, which we have grazed at best (see, e.g., [DumFoo04], [Knapp16a] and [Knapp16b]).

9.2. A quick history of algebraic equations

Algebraic equations (i.e., equations of the form $P(x) = 0$, where P is a given polynomial) were the historical origin of much of abstract algebra. Thus, I am going to say a few words about them, even though they eventually lead into topics (like Galois theory and algebraic geometry) which have not been the subject of this course.

The Babylonians knew the quadratic formula: The solutions to a quadratic equation $ax^2 + bx + c = 0$ (say, over $\mathbb{C}$) are $x = \dfrac{-b \pm \sqrt{b^2 - 4ac}}{2a}$. (Of course, the Babylonians did not know $\mathbb{C}$; even the negative numbers only appeared during the Chinese Han Dynasty and took a long time to propagate into the West. But the idea was there.)

The question of solving cubic equations ($ax^3 + bx^2 + cx + d = 0$) and equations of higher degree has puzzled people for centuries, until the case of the cubic was solved by Scipione del Ferro and Niccolò Tartaglia (and written up by Girolamo Cardano) in the early 16th Century. The history of their solution has been amply discussed and dramatized in the literature (even over-dramatized, as if the truth wasn't interesting enough!); see the lecture slides

`https://cs.uwaterloo.ca/~cbruni/CO480Resources/lectures/CO480MayAug2017/lecture11.pdf`

for a highly readable chronology, and see [Rothma15] for some pop-science claims debunked (including some from the slides).

The formula they found is surprising in its practical uselessness. Consider the case of a "depressed" cubic polynomial; this is a polynomial of the form $x^3 + px + q$ (so the coefficient of x^2 is 0). In this particular case, the Cardano formula[106] says that the roots of this polynomial are

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}.$$

The cubic roots here are understood to be *complex* cubic roots[107], which is why you get not 1 but 3 roots[108]. Note that $\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ may be non-real, even if the polynomial has a real root! Ironically, this happens precisely in the case when the cubic polynomial has 3 real roots (which is the maximum possible number); thus, it qualifies as an explicit formula only if we tolerate the presence of cubic roots of complex numbers inside it.

Worse yet: Even if the Cardano formula does not involve any non-real numbers, it is still far from the expression you might be looking for. For instance, let us try to find the roots of the polynomial $x^3 + 3x - 4$ using this formula. By plugging in $p = 3$ and $q = -4$, we get the expression

$$\sqrt[3]{2 + \sqrt{4+1}} + \sqrt[3]{2 - \sqrt{4+1}} = \sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$$

for its roots. To find the real root, we take the usual (i.e., non-complex) cubic roots. Thus we conclude that $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$ is a root of the polynomial $x^3 + 3x - 4$. But a bit of numerical computation suggests that this root is actually the number 1. And this is indeed the case, as you can easily verify by evaluating the polynomial $x^3 + 3x - 4$ at 1; but how could you have guessed this from the cube-root formula? So the Cardano formula gave us a complicated expression for the number 1, and no way to simplify it![109]

[106] The attentive reader will have noticed that this is another instance of an object named for its first expositor, not for its original discoverer. There is a moral here.

[107] If $z \in \mathbb{C}$ is a complex number, then the *complex cubic roots* of z are the complex numbers w satisfying $w^3 = z$. There are three of them (unless $z = 0$), and (in terms of the Argand diagram) they form the vertices of an equilateral triangle with center at 0.

[108] Actually, you get 9 roots if you are not careful (because there are two $\sqrt[3]{}$ signs in the formula). When picking complex cubic roots of $-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ and $-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$, you should choose not all $3 \cdot 3 = 9$ combinations, but only the ones whose product is $-\frac{1}{3}p$.

[109] Actually, you can prove that $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}} = 1$ by showing that $\sqrt[3]{2+\sqrt{5}} = \frac{1}{2}\left(1+\sqrt{5}\right)$ and $\sqrt[3]{2-\sqrt{5}} = \frac{1}{2}\left(1-\sqrt{5}\right)$. But how would you have found these two identities?

Nevertheless, the discovery of the Cardano formula has proven highly useful, as it forced the introduction of complex numbers! While complex numbers already appear as solutions of **quadratic** equations, this has not convinced anyone to define them, because everyone would content themselves with the answer "no solutions". But cubic equations like $x^3 - x + 1 = 0$ tease you with their 3 real roots which, nevertheless, cannot be expressed through $\sqrt[3]{}$ and $\sqrt{}$ signs until complex numbers are defined. Thus, it was the cubic equation that made complex numbers accepted.[110]

Cardano went on and solved the general quartic equation $ax^4 + bx^3 + cx^2 + dx + e = 0$ with an even longer formula. The proofs of these formulas have remained tricky and computational (see, e.g., [Armstr18, Week 1] for the case of the cubic), even as some of the tricks have since been explained using abstract algebra.

For three more centuries, the quintic equation $ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$ stumped mathematicians. Finally, in 1824, Niels Henrik Abel (based on work by Paolo Ruffini) showed that a general formula for the roots of a degree-5 polynomial (using $+$, $-$, $\cdot$, $/$ and $\sqrt{}$ signs only) does not exist (not even an impractical one like Cardano's). A real understanding of the reasons behind this emerged when Évariste Galois introduced the notion of groups, and what later became known as Galois groups, in 1832. This formed the beginning of Galois theory (for which see the references in Section 9.1).

From a modern viewpoint, the question of finding explicit formulas for roots of polynomials appears arbitrary and inconsequential. After all, why exactly are we allowing $\sqrt{}$ signs in these formulas, if computing $\sqrt[n]{a}$ is already tantamount to finding a root of a polynomial (namely, $x^n - a$) ? Why do some roots count as explicit, but the ones we are looking for don't? In the case of quadratic polynomials, at least the formula ends up quite useful; for higher degrees, this is almost never the case. Expressions involving third (and higher) roots are hard to work with (recall our difficulties recognizing $\sqrt[3]{2+\sqrt{5}} + \sqrt[3]{2-\sqrt{5}}$ as 1!), and if one wants numerical results, the standard numerical methods (such as Newton's) are much simpler. Algebraists generally want to compute precisely, but they don't care for the arbitrary limitations of $+$, $-$, $\cdot$, $/$ and $\sqrt{}$ signs; thus, much of the time, they end up formally adjoining their roots (using the $\mathbb{K}[x]/\mathbf{b}$ construction in Theorem 8.1.9) and computing in the resulting rings. Thus, despite giving birth to some of the algebra we know and love, Cardano's formulas eventually became historical footnotes.

9.3. Irreducible polynomials over finite fields

I have told you that there exists a field of any prime-power size; but I only showed this for the sizes p and p^2 (where p is a prime). Let me go one step further and prove this for size p^3 as well, just to illustrate the use of the $\mathbb{K}[x]/\mathbf{b}$ construction from Theorem 8.1.9. More generally, I claim the following:

[110] There may be a moral here as well.

Lemma 9.3.1. Let $\mathbb{F}$ be a finite field.
(a) There exists an irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 2.
(b) There exists an irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 3.

Note that we could not use the same argument to prove the existence of an irreducible polynomial $\mathbf{a} \in \mathbb{F}[x]$ of degree 4. Indeed, if we tried, we would have to deal with the two substantially different possibilities ($\deg \mathbf{b} = 1$ and $\deg \mathbf{c} = 3$) and ($\deg \mathbf{b} = 2$ and $\deg \mathbf{c} = 2$), which would prevent us from obtaining a surjective map from $\mathbb{F} \times \mathbb{F} \times \mathbb{F} \times \mathbb{F}$ to $\{\text{monic polynomials } \mathbf{a} \in \mathbb{F}[x] \text{ of degree } 4\}$.

Corollary 9.3.2. Let $\mathbb{F}$ be a finite field, and let $q = |\mathbb{F}|$. Then, there exist finite fields of sizes q^2 and q^3.

Now, if p is a prime, then Corollary 9.3.2 (applied to $\mathbb{F} = \mathbb{Z}/p$ and $q = p$) shows that there exist finite fields of sizes p^2 and p^3. Moreover, by applying Corollary 9.3.2 twice, we can see that there exists a finite field of size $\left(p^2\right)^2 = p^4$. However, this method fails at proving that there exists a finite field of size p^5.

For a proper proof of the existence of a finite field of size p^n (for any prime p and integer $n \geq 1$), see [LidNie97, Theorem 2.5], [Knapp16a, Theorem 9.14], [Loehr11, Exercise 12.126], [ConradF, Theorem 2.2], [Hunger14, Corollary 11.26], [Hunger03, Chapter V, Proposition 5.6], [Stewar15, Theorem 19.3], [Walker87, Theorem 6.2.11] or [Escofi01, 14.5.1] or [Grinbe19b]. However, each of these proofs, except for the one in [Grinbe19b], uses at least something we have not seen so far. (The proof in [Grinbe19b], on the other hand, is fairly long.)

References

[AigZie18] Martin Aigner, Günter M. Ziegler, *Proofs from the Book*, 6th edition, Springer 2018.

[AloDub93] Noga Alon and Moshe Dubiner, *Zero-sum sets of prescribed size*, in: "Combinatorics, Paul Erdős is Eighty", Bolyai Society, Mathematical Studies, Keszthely, Hungary, 1993, pp. 33–50.
`https://m.tau.ac.il/~nogaa/PDFS/egz1.pdf`

[AmaEsc05] Herbert Amann, Joachim Escher, *Analysis I*, translated from the German by Gary Brookfield, Birkhäuser 2005.

[AndAnd14] Titu Andreescu, Dorin Andrica, *Complex Numbers from A to... Z*, 2nd edition, Springer 2014.

[Armstr18] Drew Armstrong, *Abstract Algebra I & Abstract Algebra II*, 2019.
I: `https://www.math.miami.edu/~armstrong/561fa18.php` ;
II: `https://www.math.miami.edu/~armstrong/562sp19.php`

[Artin10] Michael Artin, *Algebra*, 2nd edition, Pearson 2010.

[Boreic08] Iurie Boreico, *Linear Independence of Radicals*, The Harvard College Mathematics Review 2.1 (2008).
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.630.1024&rep=rep1&type=pdf

[Bosch18] Siegfried Bosch, *Algebra – From the Viewpoint of Galois Theory*, Springer 2018.
https://www.springer.com/la/book/9783319951768

[Bump02] Daniel Bump, *Mathematics of the Rubik's Cube*, lecture notes (in 2 versions).
http://sporadic.stanford.edu/bump/match/rubik.html

[Burton10] David M. Burton, *Elementary Number Theory*, 7th edition, McGraw-Hill 2010.

[Carrel05] James B. Carrell, *Fundamentals of Linear Algebra*, 31 October 2005.
https://www.math.ubc.ca/~carrell/NB.pdf

[Carrel17] James B. Carrell, *Groups, Matrices, and Vector Spaces: A Group Theoretic Approach*, Springer 2017.
https://dx.doi.org/10.1007/978-0-387-79428-0

[Childs00] Lindsay N. Childs, *A Concrete Introduction to Higher Algebra*, 3rd edition, Springer 2009.

[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

[Conrad*] Keith Conrad, *Expository notes ("blurbs")*.
https://kconrad.math.uconn.edu/blurbs/

[ConradD] Keith Conrad, *The dimension of a vector space*.
https://kconrad.math.uconn.edu/blurbs/linmultialg/dimension.pdf

[ConradE] Keith Conrad, *Euler's theorem*.
https://kconrad.math.uconn.edu/blurbs/ugradnumthy/eulerthm.pdf

[ConradF] Keith Conrad, *Finite fields*, 4 February 2018.
https://kconrad.math.uconn.edu/blurbs/galoistheory/finitefields.pdf

[ConradG] Keith Conrad, *The Gaussian integers*.
`https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf`

[ConradI] Keith Conrad, *Examples of proofs by induction*.
`https://kconrad.math.uconn.edu/blurbs/proofs/induction.pdf`

[ConradS] Keith Conrad, *Modules over a PID*.
`https://kconrad.math.uconn.edu/blurbs/linmultialg/modulesoverPID.pdf`

[ConradW] Keith Conrad, *Well-defined functions*.
`https://kconrad.math.uconn.edu/blurbs/proofs/welldefined.pdf`

[Cox13] David A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley, 2nd edition 2013.

[daSilv12] Patrick Da Silva, *Polynomial in $\mathbb{Q}[x]$ sending integers to integers?*, *math.stackexchange answer #108318*.

[Day16] Martin V. Day, *An Introduction to Proofs and the Mathematical Vernacular*, 7 December 2016.
`https://www.math.vt.edu/people/day/ProofsBook/IPaMV.pdf` .

[DumFoo04] David S. Dummit, Richard M. Foote, *Abstract Algebra*, 3rd edition, Wiley 2004.
See `http://www.cems.uvm.edu/~rfoote/errata_3rd_edition.pdf` for errata.

[Dummit16] Evan Dummit, *Mathematical Cryptography, Spring 2016*, handouts.
`https://math.la.asu.edu/~dummit/handouts.html`

[Elman18] Richard Elman, *Lectures on Abstract Algebra*, 17 September 2018.
`https://www.math.ucla.edu/~rse/algebra_book.pdf`

[ErGiZi61] P. Erdős, A. Ginzburg, A. Ziv, *Theorem in the additive number theory*, Bull. Research Council Israel 10F (1961), pp. 41–43.
`https://pdfs.semanticscholar.org/2860/2b7734c115bbab7141a1942a2c974057ddc0.pdf`

[Escofi01] Jean-Pierre Escofier, *Galois Theory*, translated by Leila Schneps, Springer 2001.

[Galvin17] David Galvin, *Basic discrete mathematics*, 13 December 2017.
`http://www-users.math.umn.edu/~dgrinber/comb/60610lectures2017-Galvin.pdf`
(The URL might change, and the text may get updated. In order to reliably obtain the version of 13 December 2017, you can use the archive.org Wayback Machine: `https:`

//web.archive.org/web/20180205122609/http://www-users.math.umn.edu/~dgrinber/comb/60610lectures2017-Galvin.pdf .)

[GalQua17] Jean Gallier, Jocelyn Quaintance, *Notes on Primality Testing And Public Key Cryptography, Part 1*, 27 February 2019.
https://www.cis.upenn.edu/~jean/RSA-primality-testing.pdf

[GalQua18] Jean Gallier and Jocelyn Quaintance, *Algebra, Topology, Differential Calculus, and Optimization Theory For Computer Science and Engineering*, 2 August 2019.
https://www.cis.upenn.edu/~jean/gbooks/geomath.html

[Garret03] Paul Garrett, *Crypto and Number Theory*, slides, 2003.
http://www-users.math.umn.edu/~garrett/crypto/

[Garret07] Paul Garrett, *The Mathematics of Coding: Information, Compression, Error Correction, and Finite Fields*, 2007.
http://www-users.math.umn.edu/~garrett/coding/CodingNotes.pdf

[Goodma16] Frederick M. Goodman, *Algebra: Abstract and Concrete*, edition 2.6, 12 October 2016.
https://homepage.divms.uiowa.edu/~goodman/algebrabook.dir/algebrabook.html

[Granvi05] Andrew Granville, *Binomial coefficients modulo prime powers*, preprint.
https://web.archive.org/web/20181024055320/http://ebooks.bharathuniv.ac.in/gdlc1/gdlc1/EngineeringMergedLibraryv3.0/AndrewGranville/BinomialCoefficientsModuloPrimePowers(5579)/BinomialCoefficientsModuloPrimePowers-AndrewGranville.pdf

[Grinbe15] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
https://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see https://github.com/darijgr/detnotes/releases/tag/2019-01-10 or arXiv:2008.09862v1.

[Grinbe16] Darij Grinberg, *18.781 (Spring 2016): Floor and arithmetic functions*, 13 April 2019.
https://www.cip.ifi.lmu.de/~grinberg/floor.pdf

[Grinbe17] Darij Grinberg, *The Lucas and Babbage congruences*, 10 January 2019.
https://www.cip.ifi.lmu.de/~grinberg/lucascong.pdf

[Grinbe18] Darij Grinberg, *Notes on linear algebra*, version of 13 December 2016.
https://github.com/darijgr/lina

[Grinbe19a] Darij Grinberg, *Regular elements of a ring, monic polynomials and "lcm-coprimality"*, 2019.
https://www.cip.ifi.lmu.de/~grinberg/algebra/regpol.pdf

[Grinbe19b] Darij Grinberg, *The existence of finite fields, again*, 31 May 2019.
https://www.cip.ifi.lmu.de/~grinberg/t/19s/fpnexists.pdf

[GrKnPa94] Ronald L. Graham, Donald E. Knuth, Oren Patashnik, *Concrete Mathematics, Second Edition*, Addison-Wesley 1994.
See https://www-cs-faculty.stanford.edu/~knuth/gkp.html for errata.

[Hammac18] Richard Hammack, *Book of Proof*, 3rd edition 2018.
https://www.people.vcu.edu/~rhammack/BookOfProof/

[Heffer17] Jim Hefferon, *Linear Algebra*, 3rd edition 2017.
http://joshua.smcvt.edu/linearalgebra/

[Hunger03] Thomas W. Hungerford, *Algebra*, 12th printing, Springer 2003.

[Hunger14] Thomas W. Hungerford, *Abstract Algebra: An Introduction*, 3rd edition, Brooks/Cole 2014.

[Jia13] Yan-Bin Jia, *Quaternions and Rotations (Com S 477/577 Notes)*, 10 September 2013.
https://graphics.stanford.edu/courses/cs348a-17-winter/Papers/quaternion.pdf

[Joyner08] W. D. Joyner, *Mathematics of the Rubik's cube*, 19 August 2008.
https://web.archive.org/web/20160304122348/http://www.permutationpuzzles.org/rubik/webnotes/ (link to the PDF at the bottom).

[Knapp16a] Anthony W. Knapp, *Basic Algebra*, digital 2nd edition 2016.
https://www.math.stonybrook.edu/~aknapp/download.html

[Knapp16b] Anthony W. Knapp, *Advanced Algebra*, digital 2nd edition 2016.
https://www.math.stonybrook.edu/~aknapp/download.html

[Knuth98] Donald Ervin Knuth, *The art of computer programming, volume 2*, Addison–Wesley 1998.

[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

[LeLeMe18] Eric Lehman, F. Thomson Leighton, Albert R. Meyer, *Mathematics for Computer Science*, revised Tuesday 6th June 2018.
https://courses.csail.mit.edu/6.042/spring18/mcs.pdf .

[LidNie97] Rudolf Lidl, Harald Niederreiter, *Finite fields*, 2nd edition, Cambridge University Press 1997.

[Loehr11] Nicholas A. Loehr, *Bijective Combinatorics*, Chapman & Hall/CRC 2011.

[Mate14] Attila Maté, *Determinants*, version 1 October 2017.
http://www.sci.brooklyn.cuny.edu/~mate/misc/determinants.pdf

[Muir30] Thomas Muir, *The theory of determinants in the historical order of development*, 5 volumes (1906–1930), later reprinted by Dover.

[MuiMet60] Thomas Muir, *A Treatise on the Theory of Determinants*, revised and enlarged by William H. Metzler, Dover 1960.

[Mestro14] Romeo Meštrović, *Lucas' theorem: its generalizations, extensions and applications (1878–2014)*, arXiv:1409.3820v1.

[Milne17] James S. Milne, *Group theory*, version v3.14, March 17, 2017.
https://www.jmilne.org/math/CourseNotes/gt.html

[Mulhol16] Jamie Mulholland, *Permutation Puzzles: A Mathematical Perspective*,
https://www.sfu.ca/~jtmulhol/math302/

[NiZuMo91] Ivan Niven, Herbert S. Zuckerman, Hugh L. Montgomery, *An Introduction to the Theory of Numbers*, 5th edition 1991.

[Payne09] S. E. Payne, *A Second Semester of Linear Algebra*, 19 January 2009.
https://web.archive.org/web/20161207060453/http://math.ucdenver.edu/~spayne/classnotes/09LinAlg.pdf

[Pinkha15] Henry C. Pinkham, *Linear Algebra*, draft of a textbook, version 10 July 2015.
https://www.math.columbia.edu/~pinkham/HCP_LinearAlgebra.pdf

[Pinter10] Charles C. Pinter, *A book of abstract algebra*, 2nd edition, Dover 2010.
https://www.amazon.com/Book-Abstract-Algebra-Second-Mathematics/dp/0486474178

[Polya19] Georg Pólya, *Über ganzwertige Polynome in algebraischen Zahlkörpern*, Journal für die Reine und Angewandte Mathematik (Crelle's Journal), **149** (1919), pp. 97–116.

[Rothma15] Tony Rothman, *Cardano v Tartaglia: The Great Feud Goes Supernatural*, arXiv:1308.2181v5, published in: The Mathematical Intelligencer, 36(4), pp. 53–66.

[Siksek15] Samir Siksek, *Introduction to Abstract Algebra*, 2015.
https://homepages.warwick.ac.uk/staff/S.Siksek/teaching/aa/aanotes.pdf

[Stewar15] Ian Stewart, *Galois theory*, 4th edition, CRC Press 2015.
http://matematicaeducativa.com/foro/download/file.php?id=1647

[Strick13] Neil Strickland, *Linear mathematics for applications*, 11 February 2020.
https://neilstrickland.github.io/linear_maths/notes/linear_maths.pdf

[Swanso18] Irena Swanson, *Introduction to Analysis*, with construction of the number systems, 19 June 2019.
https://people.reed.edu/~iswanson/analysisconstructR.pdf

[Tignol01] Jean-Pierre Tignol, *Galois' Theory of Algebraic Equations*, World Scientific 2001.

[Trefet11] Lloyd N. Trefethen, *Six Myths of Polynomial Interpolation and Quadrature*, Maths. Today **47** (2011), pp. 184–188.
https://people.maths.ox.ac.uk/trefethen/publication/PDF/2011_139.pdf

[UspHea39] J. V. Uspensky, M. A. Heaslet, *Elementary Number Theory*, McGraw-Hill 1939.

[Vogan07] David Vogan, *The Character Table for E_8*, Notices of the American Mathematical Society 2007/09.

[Waerde91a] B.L. van der Waerden, *Algebra, Volume I*, translated 7th edition, Springer 1991.

[Waerde91b] B.L. van der Waerden, *Algebra, Volume II*, translated 5th edition, Springer 1991.

[Walker87] Elbert A. Walker, *Introduction to Abstract Algebra*, Random House/Birkhauser, New York, 1987.

[Wan11] Zhe-Xian Wan, *Finite fields and Galois rings*, World Scientific 2011.

[Ward91] James Ward, *100 years of Dixon's identity*, Irish Mathematical Society Bulletin **27** (1991), pp. 46–54.
https://www.maths.tcd.ie/pub/ims/bull27/bull27_46-54.pdf

[Warner71] Seth Warner, *Classical Modern Algebra*, Prentice-Hall 1971.

[Wilf94] Herbert S. Wilf, *generatingfunctionology*, 1999.
https://www.math.upenn.edu/~wilf/DownldGF.html