Math 533 Winter 2021, Lecture 1: Rings and ideals

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

0.1. General

We'll follow the book *Abstract Algebra* by Dummit and Foote, 3rd edition (2004). I will refer to this book by [DF].

Most of what we will do is a subset of [DF, Chapters 7–14], although we won't do all of it, we won't proceed in the same order as the book does, and we will (hopefully have time to) insert some extras here and there.

A few administrativa:

- See the website (`https://www.cip.ifi.lmu.de/~grinberg/t/21w/`) for any info you might be looking for.

  We will use gradescope for HW. We won't use Blackboard.

  Grading is all HW, including HW0 (due this Friday). But HW0 is worth fewer points than future HWs. Probably will be 6 HWs in total.

- Please interrupt whenever something is unclear!

  Don't hesitate to email questions either.

0.2. Plan

What we plan to do:

- Basics of rings and fields.
- Basics of modules over rings (and vector spaces over fields). In a way, this is abstract linear algebra, done in a more general setup.
- The Smith normal form and its consequences (including the Jordan normal form you might know from linear algebra).
- Tensor products.
- Gröbner bases.
- Finite fields.
- Maybe a bit of Galois theory.

0.3. Notations

Notations:

- We let $\mathbb{N} = \{0, 1, 2, \ldots\}$.
- Unlike algebraic geometers, we accept noncommutative rings as rings (see below for the definition). Unlike [DF], we don't accept nonunital rings (i.e., rings without a 1) as rings.

1. Rings and ideals

1.1. Defining rings ([DF, §7.1])

You may have seen rings before, but beware – there are at least 4 non-equivalent concepts known by this name, and the one you know might be different from the one we'll use. Let us define this one:

> **Definition 1.1.1.** A **ring** means a set R equipped with
>
> - two binary operations (i.e., maps from $R \times R$ to R) that are called **addition** and **multiplication** and denoted by $+$ and $\cdot$, and
> - two elements of R that are called **zero** and **unity** and denoted by 0 and 1,
>
> such that the following properties (the "**ring axioms**") hold:
>
> - $(R, +, 0)$ is an abelian group. In other words:
>   - The operation $+$ is associative (i.e., we have $a + (b + c) = (a + b) + c$ for any $a, b, c \in R$).
>   - The element 0 is a neutral element for the operation $+$ (i.e., we have $a + 0 = 0 + a = a$ for any $a \in R$).
>   - Each element $a \in R$ has an inverse for the operation $+$ (i.e., an element $b \in R$ satisfying $a + b = b + a = 0$).
>   - The operation $+$ is commutative (i.e., we have $a + b = b + a$ for any $a, b \in R$).
> - $(R, \cdot, 1)$ is a monoid. In other words:
>   - The operation $\cdot$ is associative (i.e., we have $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for any $a, b, c \in R$).
>   - The element 1 is a neutral element for the operation $\cdot$ (i.e., we have $a \cdot 1 = 1 \cdot a = a$ for any $a \in R$).

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

- The **distributive laws** hold in R: That is, for all $a, b, c \in R$, we have
$$(a+b)\cdot c = a\cdot c + b\cdot c \qquad \text{and} \qquad a\cdot(b+c) = a\cdot b + a\cdot c.$$

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

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

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

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

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

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

Definition 1.1.2. A ring R is said to be **commutative** if its multiplication is commutative (i.e., if $ab = ba$ for all $a, b \in R$).

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

- The sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ (endowed with the usual addition, the usual multiplication, the usual 0 and the usual 1) are commutative rings.

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

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

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

- We can define a commutative ring $\mathbb{Z}'$ as follows: We define a binary operation $\widetilde{\times}$ on the set $\mathbb{Z}$ by setting
$$a \mathbin{\widetilde{\times}} b = -ab \qquad \text{for all } (a,b) \in \mathbb{Z}\times\mathbb{Z}.$$

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

Note that I am calling this ring $\mathbb{Z}'$ rather than $\mathbb{Z}$, even though **as a set** it is identical with $\mathbb{Z}$. I do this because I want to refer to a ring by just one single letter instead of having to specify the addition and multiplication every time; but this cannot go well if we use the same letter for different rings.

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

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

satisfies

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

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

- The polynomial rings $\mathbb{Z}[x]$, $\mathbb{Q}[a,b]$ and $\mathbb{C}[z_1, z_2, \ldots, z_n]$ (which we will define soon) are commutative rings.

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

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

  and multiplication is defined by

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

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

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

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

Here are some more examples of rings:

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

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

  Associativity, distributivity, etc. come for "free", or, as we say, are **inherited from** $\mathbb{R}$ (meaning that we already know that they hold for $\mathbb{R}$, so they must automatically hold for $\mathbb{S}$).

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

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

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

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

  Now, let $\mathbb{S}'$ be the set $\mathbb{S}$, endowed with the usual addition $+$ and the (unusual) multiplication $*$, with the (usual) zero $0_{\mathbb{S}'} = 0$ and with the (unusual) unity $1_{\mathbb{S}'} = 1 + \sqrt{5}$ (not the integer 1). It is easy to check that $\mathbb{S}'$ is

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

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

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

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

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

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

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

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

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

- Another famous noncommutative ring is the ring of **Hamilton quaternions** $\mathbb{H}$. Its elements are the "formal expressions" of the form $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{R}$. (To be more rigorous, you can define them to be 4-tuples (a, b, c, d) with $a, b, c, d \in \mathbb{R}$; the "formal" sum $a + bi + cj + dk$

can be viewed as just a fancy way to write such a 4-tuple.) Addition is defined by the distributive law:

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

Multiplication is also defined by the distributive law using the formulas

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

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

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

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

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

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

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

- For every integer n, the residue classes of integers modulo n form a commutative ring, which is called $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}/n$ or $\mathbb{Z}_n$ (depending on the author; beware that $\mathbb{Z}_n$ has two different meanings). You already know its additive group $(\mathbb{Z}/n, +, 0)$, which is classically called the **cyclic group of order** n. The multiplication is defined just as addition is: namely, we set

$$\overline{a}\cdot\overline{b}=\overline{a\cdot b} \qquad \text{for any } a, b\in\mathbb{Z}.$$

(where the overline means "residue class modulo n"). This is all known as **modular arithmetic**.

The ring $\mathbb{Z}/n$ has n elements when $n > 0$. In particular, $\mathbb{Z}/1\mathbb{Z}$ is a trivial ring. In contrast, $\mathbb{Z}/0\mathbb{Z}$ is just $\mathbb{Z}$ with its elements relabelled (since a residue class modulo 0 only contains a single integer[2]).

See homework set #1 (specifically, exercises 1, 4 and 6) for more examples of rings.

Remark 1.1.3. Our above definition of a ring has some redundancies:

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

Second, we can drop the "abelian" in the axiom "$(R, +, 0)$ is an abelian group"; in other words, we can drop the requirement that addition be commutative. This is because this requirement can be derived from the remaining axioms (see [DF, page 223]). But this is a bit artificial. I am aiming not for a minimal set of axioms, but for a reasonable set of axioms that strikes the balance between usefulness (i.e., important things are easy to derive from the axioms) and verifiability (i.e., it is easy to check these axioms in meaningful cases).

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

Definition 1.1.4. A **nonunital ring** is defined in the same way as we defined a ring, except we no longer require a unity, and we replace the axiom "$(R, \cdot, 1)$ is a monoid" by "the operation $\cdot$ is associative". In particular, any ring is a nonunital ring, but not vice versa.

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

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

Beware:

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

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