Math 332 Winter 2023, Lecture 1: Rings

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

0.1. What is this about?

My name is Darij Grinberg.

This is a course on **rings** and **fields**: essentially, the algebraic structures that have both an "addition" and a "multiplication" defined on them, which we assume to behave reasonably well (i.e., we require them to satisfy certain axioms).

In the previous quarter (Math 331), you have learnt about groups, which are structures with a (very) well-behaved single operation. These are good for modelling symmetries and invertible operations in general. Rings and fields, OTOH, model numbers or things made out of numbers (such as polynomials or matrices). So I hope you will feel more at home in rings than you did in groups back when you heard about them for the first time, as I expect you to have a long history of calculating with numbers.

However, the familiarity can also mislead, since not everything that is true for numbers is also true for elements of a ring. For example, matrices A and B don't always satisfy $AB = BA$. When studying rings, we will again encounter surprises like this and worse. This is the price of exploring new places.

0.2. Plans

Everything I'm typing in class will go on the website. The website also serves as a syllabus and will contain all relevant info, references and links. By the end of this week, it should include info about grading and assignments.

The course will be split into 6 chapters:

1. **Rings and ideals.** A ring is like a number system. An ideal is like a normal subgroup.
2. **Modules.** Modules are the natural generalization of vector spaces when the underlying number system is replaced by a ring.
3. **Monoid algebras and polynomials.** This is a generalization of the classical notion of polynomials.
4. **Finite fields.** A finite field is like miniature version of our number system. They have applications galore. This will include some applications.
5. **Polynomials II.** We will study polynomials in more detail, approaching the ancient question of "how do you solve a system of polynomial equations?".

6. **Modules over a PID.** In particular, we will prove the structure theorem for finite abelian groups, and explore the Smith normal form of a matrix. [We will not actually get to this topic in this quarter, but it appears as §7 in our text.]

I will get to some applications, including (hopefully) answers to all HW#0 problems.

1. Rings and ideals

1.1. Defining rings

1.1.1. The definition

You may have seen rings before, but keep in mind that there are 4 different (related but not equivalent) notions of a ring, and the one you know might not be the one I define.

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 are denoted by $+$ and $\cdot$, and
- two elements of R that are called **zero** and **unity** and are denoted by 0 and 1,

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

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

Note that we **do not** require the operation $\cdot$ to be commutative or to have inverses.

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

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

4. 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 are just calling them 0 and 1 since they play similar roles. If things can get ambiguous, we will fall back to the notations 0_R and 1_R for them.

The unity of R is also known as the **identity** or the **one** of R.

The product $a \cdot b$ is also abbreviated ab.

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

If $a, b \in R$, then the **difference** $a - b \in R$ 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., we have $ab = ba$ for all $a, b \in R$).

1.1.2. Some examples of rings

You have certainly seen some rings in your 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 the existence of **multiplicative** inverses – i.e., inverses for the operation $\cdot$ – is not required.)

- The set $\mathbb{N} := \{0, 1, 2, \ldots\}$ of nonnegative integers (again endowed with the usual addition, the usual multiplication, the usual 0 and the usual 1) is **not** a ring: Its elements (other than 0) have no additive inverses in $\mathbb{N}$. It does, however, satisfy all the other ring axioms. Such an object is called a **semiring**.

- 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 $0_{\mathbb{Z}'} = 0$ and the unusual unity $1_{\mathbb{Z}'} = -1$. It is easy to check that $\mathbb{Z}'$ is a commutative ring. It is an example of a ring whose unity is clearly **not** the usual number 1, so we should not be just calling it 1.

Note that the ring $\mathbb{Z}'$ equals $\mathbb{Z}$ **as a set**, but it is a different **ring**. So if you are talking about sets, $\mathbb{Z}' = \mathbb{Z}$. If you are talking about rings (i.e., the entire packages containing a set, a $+$ operation, a $\cdot$ operation, a 0 and a 1), then $\mathbb{Z}' \neq \mathbb{Z}$.

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 will soon introduce the concept of a **ring isomorphism**, and then we will be able to say that $\mathbb{Z}'$ is **isomorphic** to $\mathbb{Z}$, and more concretely, that the map

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

is a ring isomorphism.

- The polynomial rings

$$\begin{aligned}
\mathbb{Z}[x] &= \{\text{all polynomials in one indeterminate } x \text{ with integer coefficients}\}, \\
\mathbb{Q}[x] &= \{\text{all polynomials in one indeterminate } x \text{ with rational coefficients}\}, \\
\mathbb{R}[x,y] &= \{\text{all polynomials in two indeterminates } x,y \text{ with real coefficients}\}, \\
\mathbb{R}[z_1,z_2,\ldots,z_n] &= \{\text{all polynomials in } n \text{ indeterminates } z_1,z_2,\ldots,z_n \text{ with real coefficients}\}
\end{aligned}$$

are commutative rings. We will formally define them soon.

- The set of all functions from $\mathbb{Q}$ 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, and where the unity is the "constant-1" function.

The same construction holds for functions from $\mathbb{Q}$ to $\mathbb{R}$, or from $\mathbb{R}$ to $\mathbb{Q}$, or from $\mathbb{N}$ to $\mathbb{Q}$.

More generally, if R is a ring, and if S is any set, then the set of all functions from S to R is a ring (with $+$, $\cdot$, 0 and 1 defined as above). If R is commutative, then so is this new ring.

When we specify a ring, we don't need to provide its zero 0 and its unity 1 (although they do need to exist); they are uniquely determined by the operations $+$ and $\cdot$. This is because the neutral element for any binary operation is uniquely determined.

Some more examples of rings:

- The set of all real numbers of the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$. More on this next time.