Math 332 Winter 2023, Lecture 2: Rings

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

1. Rings and ideals (cont'd)

1.1. Defining rings (cont'd)

1.1.2. Some examples of rings (cont'd)

Here are some more examples of rings:

- Let $\mathbb{S}$ be the set of all real numbers of the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$.

  For instance, $3 \in \mathbb{S}$ since $3 = 3 + 0\sqrt{5}$.

  Also, $\sqrt{5} \in \mathbb{S}$ since $\sqrt{5} = 0 + 1\sqrt{5}$.

  But also $\dfrac{30}{7} - \dfrac{25}{9}\sqrt{5} \in \mathbb{S}$.

  We claim that $\mathbb{S}$ is a ring (where the addition, multiplication, zero and unity are the usual ones).

  To prove this, we need to show all the ring axioms. Most of them follow immediately from the analogous properties of real numbers (since $\mathbb{S} \subseteq \mathbb{R}$). The only one that could theoretically go wrong is existence of additive inverses, because now you need to show that the additive inverse actually belongs to $\mathbb{S}$ (the fact that $\mathbb{R}$ is a ring only gives you an additive inverse in $\mathbb{R}$, not in $\mathbb{S}$). But this is easy:

  $$-\left(a + b\sqrt{5}\right) = (-a) + (-b)\sqrt{5} \in \mathbb{S}.$$

  But we are not done yet! We also need to prove that addition and multiplication are binary operations on $\mathbb{S}$, that is, maps from $\mathbb{S} \times \mathbb{S}$ to $\mathbb{S}$. In other words, we need to prove that if we add or multiply two numbers of the form $a + b\sqrt{5}$ with $a, b \in \mathbb{Q}$, then you again get a number of this form. It is easy to miss this requirement because we didn't state it as a "ring axiom", but it is nevertheless part of the definition, hidden in plain sight in its first sentence.

  So let us check this requirement. For addition, it follows from

  $$\left(a + b\sqrt{5}\right) + \left(c + d\sqrt{5}\right) = (a + c) + (b + d)\sqrt{5} \in \mathbb{S}.$$

  For multiplication, it follows from

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

Now, we are done proving that $\mathbb{S}$ is a ring.

- We could define a different ring structure on the same set $\mathbb{S}$: specifically, a ring that, as a set, is identical with $\mathbb{S}$, but has a different choice of multiplication and unity. Namely, we define a binary operation $*$ on $\mathbb{S}$ by

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

  This relies on the fact that every element of $\mathbb{S}$ can be written in the form $a+b\sqrt{5}$ for a **unique** pair $(a,b) \in \mathbb{Q} \times \mathbb{Q}$. (And this fact, in turn, follows from the irrationality of $\sqrt{5}$: If we had $a+b\sqrt{5} = c+d\sqrt{5}$ for two distinct pairs $(a,b), (c,d) \in \mathbb{Q} \times \mathbb{Q}$, then we would have $a-c = (d-b)\sqrt{5}$ and thus $\sqrt{5} = \dfrac{a-c}{d-b}$, which would contradict the irrationality of $\sqrt{5}$.)

  Now, consider the set $\mathbb{S}$, endowed with the usual addition, the unusual multiplication $*$, the usual zero and the unusual unity $1+\sqrt{5}$. This is again a ring, although not a very useful one. It is **not** the same ring as $\mathbb{S}$, and not even close; its properties are fairly different.

- Let $\mathbb{S}_3$ be the set of all real numbers of the form $a+b\sqrt[3]{5}$ with $a,b \in \mathbb{Q}$. Is this a ring (endowed with the usual addition, the usual multiplication, the usual zero and the usual unity)?

  No, because multiplication is not a binary operation on $\mathbb{S}_3$:

$$\begin{aligned}\left(a+b\sqrt[3]{5}\right)\left(c+d\sqrt[3]{5}\right) &= ac+ad\sqrt[3]{5}+bc\sqrt[3]{5}+bd\underbrace{\sqrt[3]{5}\sqrt[3]{5}}_{=\sqrt[3]{25}} \\ &= ac+ad\sqrt[3]{5}+bc\sqrt[3]{5}+bd\sqrt[3]{25}.\end{aligned}$$

  There is no way to rewrite the RHS (= right hand side) in the form $u+v\sqrt[3]{5}$ with $u,v \in \mathbb{Q}$, since the $bd\sqrt[3]{25}$ term cannot be simplified. (Strictly speaking, this needs proof, but you can trust me on this.)

So far, all our rings were commutative (i.e., their multiplication was commutative). But there are many noncommutative examples:

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

  More generally: If R is any ring, and if $n \in \mathbb{N}$, then the set $R^{n\times n}$ of all $n \times n$-matrices with entries in R (endowed with matrix addition, matrix multiplication, the zero matrix and the identity matrix) is a ring. This is

called the $n \times n$**-matrix ring** over R; it is denoted by $R^{n\times n}$ or $\mathrm{M}_n(R)$. 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.

Note that $R^{n\times n}$ is not commutative even for $n = 1$ if R itself is not commutative.

At this point, the phrase "endowed with the usual addition, etc." must have gotten quite boring. So we agree that if we don't say what the operations of a ring are, then we just understand that they are the "obvious ones". For example, if our ring R consists of real numbers, then its addition is understood to be the usual addition of real numbers by default (unless we say that we are endowing it with a different addition).

More examples:

- Another famous noncommutative ring is the ring of **Hamilton quaternions** $\mathbb{H}$. Its elements are the "formal expressions" of the form

$$a + bi + cj + dk \qquad \text{with } a, b, c, d \in \mathbb{R}.$$

(To be rigorous, you can define them as 4-tuples (a, b, c, d) of real numbers. The "formal expression" $a + bi + cj + dk$ is then just a fancy way of writing such a 4-tuple.)

We make this set $\mathbb{H}$ into a ring by defining

  - its addition by

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

  - its multiplication by the distributive law and by the formulas

$$\begin{aligned}&i^2 = j^2 = k^2 = -1,\\ &ij = k, \qquad jk = i, \qquad ki = j,\\ &ji = -k, \qquad kj = -i, \qquad ik = -j\end{aligned}$$

(and by the requirement that real numbers commute with i, j, k). For example, the distributive law yields

$$\begin{aligned}(1 + i)(2 + k) &= 2 + k + 2i + \underbrace{ik}_{=-j}\\ &= 2 + k + 2i + (-j)\\ &= 2 + 2i + (-1) j + k.\end{aligned}$$

  - its zero to be $0 = 0 + 0i + 0j + 0k$.

– its unity to be $1 = 1 + 0i + 0j + 0k$.

This $\mathbb{H}$ is indeed a ring. Indeed, all the ring axioms can be checked by brute force (i.e., directly by multiplying things out). Later we will learn a better way.

Back to some simpler examples:

- The **zero ring** is the ring consisting of a single element 0. This element serves both as zero and as unity. (So we have $0 = 1$ in this ring.) Both operations $+$ and $\cdot$ do what they have to do:

$$0 + 0 = 0 \cdot 0 = 0.$$

The zero ring is commutative.

More generally, a **trivial ring** means a ring with only one element. Every trivial ring is just the zero ring with its 0 element renamed.

- Let n be an integer.

Consider the relation $\underset{n}{\equiv}$ on the set $\mathbb{Z}$ defined by

$$a \underset{n}{\equiv} b \iff n \mid a - b.$$

This relation $\underset{n}{\equiv}$ is called **congruence modulo** n, and is an equivalence relation. (We usually write $a \equiv b \bmod n$ instead of $a \underset{n}{\equiv} b$.)

The equivalence classes of this relation are called the **residue classes of integers modulo** n. Explicitly, for every integer a, the residue class that contains a is

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

We denote this class by $\overline{a}$. Two integers a and b satisfy $\overline{a} = \overline{b}$ if and only if $a \underset{n}{\equiv} b$. Thus, working with residue classes of integers modulo n can be viewed as working with integers but pretending that n equals 0 (so that two integers that differ by a multiple of n become equal).

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

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

The set of all residue classes of integers modulo n will be called $\mathbb{Z}/n$ or $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$. When n is positive, this set $\mathbb{Z}/n$ has n elements, which are the residue classes

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

In modular arithmetic ("clock arithmetic"), we have learned how to add and multiply such residue classes: The rules are

$$\begin{aligned}
\overline{a} + \overline{b} &= \overline{a+b}; \\
\overline{a} \cdot \overline{b} &= \overline{ab}
\end{aligned}$$

for all $a, b \in \mathbb{Z}$. This turns the set $\mathbb{Z}/n\mathbb{Z}$ into a commutative ring. Its additive part – i.e., the group $\left(\mathbb{Z}/n\mathbb{Z},\ +,\ \overline{0}\right)$ – is known as the **cyclic group of order** n.