Math 332 Winter 2023, Lecture 3: 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)

Warm-up:

Let's practice computations in $\mathbb{Z}/n$ ("modular arithmetic").

Recall that $\overline{a}$ denotes the residue class of an integer a modulo n. Note that this notation does not mention n, but of course the meaning of $\overline{a}$ does depend on n. So we will rely on context to clarify what the n is. Less ambiguously, we can denote the same residue class $\overline{a}$ as $a + n\mathbb{Z}$, which stands for "coset of a with respect to the subgroup $n\mathbb{Z}$ of the abelian group $\mathbb{Z}$". The residue classes modulo n are precisely the cosets of the subgroup $n\mathbb{Z}$ in $\mathbb{Z}$.

Let us now compute some products of residue classes.

- In $\mathbb{Z}/12$, we have

$$\overline{3} \cdot \overline{7} = \overline{3 \cdot 7} = \overline{21} = \overline{9} \qquad (\text{since } 21 \equiv 9 \bmod 12)$$

and

$$\overline{6} \cdot \overline{8} = \overline{6 \cdot 8} = \overline{48} = \overline{0} \qquad (\text{since } 48 \equiv 0 \bmod 12)\,.$$

- In $\mathbb{Z}/15$, we have

$$\overline{6} \cdot \overline{5} = \overline{6 \cdot 5} = \overline{30} = \overline{0} \qquad (\text{since } 30 \equiv 0 \bmod 15)\,.$$

Note that the $\overline{6}$ here is not the same as the $\overline{6}$ in the previous example. Indeed, the $\overline{6}$ here is $6 + 15\mathbb{Z}$, whereas the previous $\overline{6}$ was $6 + 12\mathbb{Z}$.

Note that there is no such thing as $\overline{6}/\overline{5}$. Nor is there such a thing as $\overline{20}/\overline{5}$. Indeed, it sounds reasonable to define $\overline{20}/\overline{5} = \overline{20/5} = \overline{4}$. By the same logic, it sounds reasonable to define $\overline{50}/\overline{5} = \overline{50/5} = \overline{10}$. However, these two equalities would contradict one another, since their LHSs are equal (since $\overline{20} = \overline{50}$) but their RHSs are not. So division in $\mathbb{Z}/15$ cannot be defined unambiguously in general.

Let's go back to examples of rings. Here is one more:

- Consider a 4-element set with four elements $0, 1, a, b$. We endow this set with two operations $+$ and $\cdot$ defined by the following tables of values:

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

and

xy	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

.

  This turns our set into a ring, which we call F_4. You can check all the ring axioms for it by brute force; it's not fun. We will later see a "conceptual" way to construct this ring F_4, which will render this busywork unnecessary.

We will see many more examples through this course.

1.2. Calculating in rings

1.2.1. What works

The intuition for a commutative ring is essentially "a system of numbers, but built of something other than numbers". So we expect all the standard rules for calculating with numbers to also hold in any commutative ring. For a noncommutative ring, we need to be more careful, since commutativity of multiplication ($ab = ba$) is not required, and therefore any rule that relies on commutativity (e.g., the binomial formula) doesn't have to hold either.

Let us be more precise about what rules we expect to hold.

If $a_1, a_2, \ldots, a_n$ are n elements of a ring, then the sum $a_1 + a_2 + \cdots + a_n$ is well-defined (i.e., you can add its addends from the front or from the back or in any other order, and the results will all be the same). More generally, any finite sum of the form $\sum_{s \in S} a_s$ (with S being a finite set) is well-defined whenever the a_s belong to a ring. Such finite sums behave like usual finite sums of numbers. This is called **generalized commutativity**. (For rigorous proofs, you can find some references in the text.) An empty sum is defined to be the zero of the underlying ring.

If our ring is commutative, then the same is true for finite products of the form $\prod_{s \in S} a_s$. However, this is not the case if our ring is noncommutative, because the order in a product matters even for just 2 factors. But a product with a well-defined order, such as $a_1 a_2 \cdots a_n$, is well-defined in any ring (commutative or not). For example, $abcde$ is well-defined, i.e., the result does not depend on whether you read it as $(a\,(bc))\,(de)$ or as $(((ab)\,c)\,d)\,e$ or in any of the other

possible ways. This is called **generalized associativity**. An empty product is defined to be the unity of the underlying ring.

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

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

Furthermore, for any three elements a, b, c of a ring, we have

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

("**distributivity of subtraction**").

Next, some more definitions.

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

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

Note that this defines multiplying (aka **scaling**) an element of R by an integer. This is not the same as multiplying two elements of R with each other. (However, if R does contain $\mathbb{Z}$ as a subset, then usually the two operations will give the same result, unless the multiplication of R has been rigged to make this false[1].)

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

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

In particular,

$$a^0 = (\text{empty product}) = 1_R \qquad \text{by definition.}$$

Now, we have learned to scale elements of a ring by integers, and take them to nonnegative integer powers. These operations satisfy some of the rules that you would expect. For example, if $a, b \in R$ (with R being a ring), and $n, m \in \mathbb{Z}$, then

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

[1] An example of such a rigged multiplication is the ring $\mathbb{Z}'$ from Lecture 1.

Furthermore, if $a \in R$ and $n, m \in \mathbb{N}$, then

$$a^{n+m} = a^n \cdot a^m;$$
$$a^{nm} = \left(a^n\right)^m.$$

Also,

$$1_R^n = 1_R \qquad \text{for any } n \in \mathbb{N};$$
$$0_R^n = 0_R \qquad \text{for any integer } n > 0;$$
$$0_R^0 = 1_R.$$

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

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

and

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

and the binomial formula

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

All of this is proved just as for numbers (with the exception of $a^i b^j = b^j a^i$, which is unnecessary for numbers, but can be easily proved by a double induction on i and on j).

Warning 1.2.1. None of the latter three identities can be expected to hold if $ab \neq ba$. It is easy to find examples of 2×2-matrices $a, b \in \mathbb{Q}^{2\times 2}$ which violate them all.

1.2.2. What doesn't work

Here are some less familiar features of rings:

- It is not always true that $a \neq 0$ and $b \neq 0$ imply $ab \neq 0$ (when a and b are elements of a ring R). For example, $\overline{6} \cdot \overline{5} = \overline{0} = 0$ in $\mathbb{Z}/15$, but neither $\overline{6}$ nor $\overline{5}$ is 0.
- It is not always true that $ab = 1$ implies $ba = 1$. Counterexamples, however, are hard to find, since "$ab = 1 \implies ba = 1$" holds not just for numbers and residue classes of integers, but also (e.g.) for square matrices with real entries. It will take several weeks until we meet a ring where the "$ab = 1 \implies ba = 1$" implication is false.

1.3. Subrings

1.3.1. Definition

Groups have subgroups; vector spaces have subspaces. Not surprisingly, rings have their substructures too:

Definition 1.3.1. Let R be a ring. A **subring** of R is a subset S of R such that

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

These five conditions are called the "**subring axioms**". They are called "S is closed under addition", "S is closed under multiplication", "S is closed under negation", "S contains 0" and "S contains 1", respectively. Altogether, they ensure that the following proposition holds:

Proposition 1.3.2. Let S be a subring of a ring R. Then, S automatically is a ring in its own right (with its operations $+$ and $\cdot$ obtained by restricting the corresponding operations of R, and with its zero and unity passed down from R).

1.3.2. Examples

Here are some examples of subrings:

- From the classical construction of the number systems, you know that $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$. Each of these three "$\subseteq$" signs can be strengthened to "is a subring of". For instance, $\mathbb{Z}$ is a subring of $\mathbb{Q}$.
- You can extend this chain further to the right: $\mathbb{C}$ is a subring of $\mathbb{H}$ (the Hamilton quaternions).
- However, we **cannot** extend this chain to the left: The only subring of $\mathbb{Z}$ is $\mathbb{Z}$ itself. Indeed, if S is a subring of $\mathbb{Z}$, then $1 \in S$ (by the last subring axiom), therefore $\underbrace{1+1+\cdots+1}_{n \text{ times}} \in S$ for any $n > 0$ (since S is closed under addition), so that $1, 2, 3, \ldots \in S$, therefore $-1, -2, -3, \ldots \in S$ (since S is closed under negation), and finally $0 \in S$ (by an axiom), so that S contains all the integers $\ldots, -2, -1, 0, 1, 2, \ldots$, and therefore $S = \mathbb{Z}$.

- There are lots of rings between $\mathbb{Z}$ and $\mathbb{Q}$ (that is, rings $\mathbb{B}$ such that $\mathbb{Z}$ is a subring of $\mathbb{B}$ and $\mathbb{B}$ is a subring of $\mathbb{Q}$). For example, the set of all rational numbers of the form

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

is such a ring[2]. More such rings you can find on Homework Set #1 exercise 5.

[2]To prove this, you need to show the subring axioms for this set. For example, why is it closed under addition? Well, if we add two such numbers $\frac{a}{b}$ and $\frac{c}{d}$ (with $a, b, c, d \in \mathbb{Z}$ and with b, d odd), then we get $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, which again has an odd denominator. Thus, our set is closed under addition. Closedness under multiplication is similar, and the remaining axioms are almost obvious.