Math 332 Winter 2023, Lecture 7: Rings

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

1. Rings and ideals (cont'd)

1.8. Ideals and kernels

1.8.1. Kernels

Here is a definition that we already made last time:

Definition 1.8.1. Let R and S be rings. Let $f : R \to S$ be a ring morphism. Then, the **kernel** of f is defined to be the set

$$\operatorname{Ker} f := \{r \in R \mid f(r) = 0_S\}.$$

This is a subset of R (but usually not a subring).

Examples:

- Let $n \in \mathbb{Z}$. The kernel of the ring morphism

$$\begin{aligned} \pi : \mathbb{Z} &\to \mathbb{Z}/n, \\ a &\mapsto \overline{a} \end{aligned}$$

  is $n\mathbb{Z} = \{\text{all multiples of } n\}$.

- Let R be a ring. Let S be any set. Recall the ring R^S of all functions from S to R (with pointwise operations). Fix an element $s \in S$. Then, the kernel of the ring morphism

$$\begin{aligned} R^S &\to R, \\ f &\mapsto f(s) \end{aligned}$$

  is the set of all functions $f \in R^S$ that vanish on s.

- The kernel of an injective ring morphism $f : R \to S$ is always $\{0_R\}$. Indeed, any ring morphism $f : R \to S$ sends 0_R to 0_S. If f is furthermore injective, then 0_R must be the **only** element of R that f sends to 0_S (since any other such element a would cause $f(a) = 0_S = f(0_R)$, which would violate injectivity), so we obtain $\operatorname{Ker} f = \{0_R\}$.

1.8.2. Ideals

As we saw, kernels of ring morphisms are usually not subrings. Instead, here is what they are:

Definition 1.8.2. Let R be a ring. An **ideal** of R means a subset I of R such that

- we have $a + b \in I$ for any $a, b \in I$ (that is, I is closed under addition);
- we have $ab \in I$ and $ba \in I$ for any $a \in R$ and $b \in I$ (that is, I is closed under multiplication **by arbitrary elements of** R – not just under multiplication within its own elements);
- we have $0 \in I$ (where 0 means 0_R).

These three requirements are called the **ideal axioms**. The second is called "**absorption axiom**", since it yields that any product that has (at least) one factor in I will belong to I. In other words, it says that lying in I is "infectious" (at least in products). When R is commutative, the requirements $ab \in I$ and $ba \in I$ are equivalent.

Here are some easy consequences of the definition:

Proposition 1.8.3. Let R be a ring. Let I be an ideal of R. Then, I is a subgroup of the additive group $(R, +, 0)$.

Proof. By the first ideal axiom, I is closed under addition. By the third, it contains 0. By the second axiom, it is closed under multiplying by -1, which means that it is closed under negation. □

Theorem 1.8.4. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then, its kernel $\operatorname{Ker} f$ is an ideal of R.

Proof. Let us check the ideal axioms. Specifically, we will check the second, since the other two are easier.

So we need to show that $ab \in \operatorname{Ker} f$ and $ba \in \operatorname{Ker} f$ for any $a \in R$ and $b \in \operatorname{Ker} f$.

To that purpose, we let $a \in R$ and $b \in \operatorname{Ker} f$ be arbitrary. Since f is a ring morphism, we then have

$$f(ab) = f(a) \cdot \underbrace{f(b)}_{\substack{=0_S \\ (\text{since } b \in \operatorname{Ker} f)}} = f(a) \cdot 0_S = 0_S,$$

so that $ab \in \operatorname{Ker} f$. Similarly, $ba \in \operatorname{Ker} f$.

As I said, the other two axioms are similar but easier. □

We will soon see that the theorem we just proved has a converse: Any ideal of a ring R can be written as the kernel of a ring morphism from R to another ring S. Thus, ideals and kernels are "the same thing, viewed from different angles".

1.8.3. Principal ideals

The simplest way to construct ideals in a commutative ring is by fixing an element and taking all its multiples:

Proposition 1.8.5. Let R be a commutative ring. Let $u \in R$. We define uR to be the set $\{ur \mid r \in R\}$. The elements of this set uR are called the **multiples** of u (in R).

Then, uR is an ideal of R. This ideal is known as a **principal ideal** of R. In particular, $0R = \{0\}$ and $1R = R$ are therefore principal ideals of R.

Proof. The only thing we need to prove is that uR is an ideal of R. Let us check the axioms:

- We have $a + b \in uR$ for any $a \in uR$ and $b \in uR$. Indeed, let $a \in uR$ and $b \in uR$. Then, we can write a as $a = ux$ for some $x \in R$ (since $a \in uR$), and likewise we can write b as $b = uy$ for some $y \in R$, and then we have $a + b = ux + uy = u(x + y) \in uR$.
- We have $ab \in uR$ and $ba \in uR$ for any $a \in R$ and $b \in uR$. Indeed, let $a \in R$ and $b \in uR$. Then, we can write b as $b = uy$ for some $y \in R$ (since $b \in uR$), and then we have $ab = auy = uay \in uR$ and $ba = ab \in uR$.
- We have $0 \in uR$, since $0 = u \cdot 0$.

□

For example, $2\mathbb{Z} = \{\text{all even integers}\}$ is a principal ideal of $\mathbb{Z}$.

Principal ideals can also be defined for noncommutative rings, but this is more complicated (for details, see the footnote in §2.8.3 of the text). (Fortunately, uR still works if u is a central element of R.)

1.8.4. Other examples of ideals

In the classical number rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, all ideals are principal (this will be proved below). But some other commutative rings have non-principal ideals as well. For example:

- Consider the set of all polynomials $f \in \mathbb{Q}[x, y]$ that have constant term 0 (equivalently: that vanish when you substitute 0 for x and for y). This set is an ideal of $\mathbb{Q}[x, y]$ (why?), but not a principal ideal (why?).

- Consider the set of all polynomials $f \in \mathbb{Z}[x]$ whose constant term is even. This set is an ideal of $\mathbb{Z}[x]$, but not a principal ideal.

We will come back to this later, as we rigorously define polynomials in one of the next chapters.

See the text (§2.8.4) for more examples of ideals. Here is just one:

Example 1.8.6. Let R be any ring. Recall that

$$R^{2\leq 2} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in R \right\}$$

is the ring of all upper-triangular 2×2-matrices over R. Then,

$$I := \left\{ \begin{pmatrix} 0 & b \\ 0 & d \end{pmatrix} \mid b, d \in R \right\},$$
$$J := \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in R \right\},$$
$$K := \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in R \right\}$$

are ideals of $R^{2\leq 2}$, whereas

$$L := \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in R \right\}$$

is not. Checking this will be a problem on homework set #3.

1.9. Quotient rings

What follows is one of the most abstract topics of this course: the definition of quotient rings, and their basic properties.

Recall the idea behind modular arithmetic: By passing from the integers to their residue classes modulo n (for a given $n \in \mathbb{Z}$), we are essentially equating n with 0: Two integers become "equal" if they differ by a multiple of n. Thus, the residue classes modulo n are "what remains" of the integers if we equate n with 0.

The same passage can be made in greater generality: We can start with any ring R and any ideal I of R, and we can equate all elements of I with 0 (so that two elements of R become "equal" if they differ by an element of I). What remains is again called "residue classes" (now modulo I rather than modulo n), and we can again define addition and multiplication on these classes. The result is a new ring, called the **quotient ring** of R by the ideal I, and denoted by R/I. Working in this quotient ring R/I is a natural generalization of modular

arithmetic to things that are not necessarily integers (but can be matrices or polynomials or any other objects instead).

This was the rough idea behind quotient rings. We will now define them rigorously.

1.9.1. Quotient groups

We don't need to reinvent the wheel: You have already seen residue classes in a first course on groups; in that context, they are known as "**cosets**". We will only have to turn them into a ring.

Let me recall the definition of cosets:

- If H is a subgroup of a group G, then the **left cosets** of H in G are the subsets
$$gH := \{gh \mid h \in H\} \qquad \text{for all } g \in G.$$
There is one left coset gH for each $g \in G$; but different g's can often lead to the same coset. Thus, there are usually fewer left cosets than elements of G. The set of all left cosets of H is called G/H.

- If H is merely a subgroup of a group G, then G/H is not a group, but just a "G-set" (i.e., a set equipped with an action of G). However, when H is a **normal** subgroup of a group G, then G/H becomes a group itself, with group operation defined by
$$(g_1H) \cdot (g_2H) = g_1g_2H \qquad \text{for all } g_1, g_2 \in G. \tag{1}$$
This group G/H is called the **quotient group** of G by H. The left cosets of H in G are just called the **cosets** of H in G in this case.

- If G is an abelian group, then any subgroup H of G is normal, so G/H is always a group.

- Now, assume that G is an **additive** group (which means that its binary operation is written as $+$ instead of $\cdot$). This presupposes that G is abelian. Then, the cosets of H in G are denoted by $g + H$ instead of gH. The quotient group G/H is also written additively (i.e., we denote its operation by $+$ instead of $\cdot$). The equality (1) thus turns into
$$(g_1 + H) + (g_2 + H) = (g_1 + g_2) + H \qquad \text{for all } g_1, g_2 \in G.$$
Thus, on the quotient group G/H, we have an addition operation, not a multiplication operation (but mathematically, the definition is the same as before; it's just the notation that has changed). Note that G/H is again an abelian group.

- The most famous example of a quotient group is when $G = \mathbb{Z}$ and $H = n\mathbb{Z} = \{\text{all multiples of } n\}$ for some fixed integer n. (Here, the group operation is addition.) Then, the quotient group $\mathbb{Z}/n\mathbb{Z}$ is the cyclic group $\mathbb{Z}/n$, and this is precisely how $\mathbb{Z}/n$ is defined.

  (See Samir Siksek, *Introduction to Algebra*, Chapter XII, for more examples of quotient groups.)

1.9.2. Quotient rings

Now, piggybacking on the construction of quotient groups we just recalled, we shall define a similar quotient structure for rings instead of groups. Instead of normal subgroups, we will use ideals this time:

Definition 1.9.1. Let I be an ideal of a ring R. Thus, I is a subgroup of the additive group $(R, +, 0)$, hence a normal subgroup (since $(R, +, 0)$ is abelian). Thus, the quotient group R/I is a well-defined abelian group. Its elements are the cosets $r + I$ of I in R. These cosets are called the **residue classes** modulo I. A coset $r + I$ is also denoted by $\overline{r}$ or $[r]$ or $[r]_I$ or $r \bmod I$. (We will only use the notations $\overline{r}$ and $r + I$.)

Note that the addition on R/I is given by

$$(a + I) + (b + I) = (a + b) + I \qquad \text{for all } a, b \in R.$$

We now define a multiplication operation on R/I by setting

$$(a + I)(b + I) = ab + I \qquad \text{for all } a, b \in R.$$

(See below for a proof that this is well-defined.)

The set R/I, equipped with the addition and the multiplication we just defined, and with the elements $0 + I$ and $1 + I$ playing the roles of zero and unity, is a ring (as we will soon see). This ring is called the **quotient ring** of R by the ideal I, and is denoted by R/I. It is pronounced "R **modulo** I".

Theorem 1.9.2. Let R and I be as in this definition. Then, the multiplication on R/I is well-defined, and R/I becomes a ring when endowed with the operations we just introduced.

We will prove this next time. First, a few examples:

- Let $n \in \mathbb{Z}$. Then, the set $n\mathbb{Z} = \{\text{all multiples of } n\}$ is an ideal of $\mathbb{Z}$ (a principal ideal, in fact). The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is exactly the ring $\mathbb{Z}/n$ of residue classes modulo n that we introduced a while ago.