Math 533 Winter 2021, Lecture 3: Rings and ideals

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

1. Rings and ideals (cont'd)

1.1. Ring morphisms ([DF, §7.3])

Groups have group homomorphisms; vector spaces have vector space homomorphisms (= linear maps); topological spaces have topological space homomorphisms (= continuous maps). No wonder that an analogous concept exists for rings:

Definition 1.1.1. Let R and S be two rings.

(a) A **ring homomorphism** (or, for short, **ring morphism**, or, more informally, **ring homo** or **ring hom** or **ring map**) from R to S means a map $f : R \to S$ that

- **respects addition** (i.e., satisfies $f(a+b) = f(a) + f(b)$ for all $a, b \in R$);
- **respects multiplication** (i.e., satisfies $f(ab) = f(a) \cdot f(b)$ for all $a, b \in R$);
- **respects the zero** (i.e., satisfies $f(0_R) = 0_S$);
- **respects the unity** (i.e., satisfies $f(1_R) = 1_S$).

(b) A **ring isomorphism** (or, informally, **ring iso**) from R to S means an invertible ring morphism $f : R \to S$ whose inverse $f^{-1} : S \to R$ is also a ring morphism.

(c) The rings R and S are said to be **isomorphic** (this is written $R \cong S$) if there exists a ring isomorphism from R to S.

Examples:

- Let $n \in \mathbb{Z}$. The map $\pi : \mathbb{Z} \to \mathbb{Z}/n$, $a \mapsto \overline{a}$ that sends each integer a to its residue class $\overline{a}$ is a ring morphism, because any $a, b \in \mathbb{Z}$ satisfy
$$\overline{a+b} = \overline{a} + \overline{b}, \qquad \overline{a \cdot b} = \overline{a} \cdot \overline{b}, \qquad \overline{0} = 0_{\mathbb{Z}/n}, \qquad \overline{1} = 1_{\mathbb{Z}/n}.$$
- The map $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto 2a$ is **not** a ring morphism. It respects addition and the zero, but not multiplication and the unity.
- The map $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto 0$ is **not** a ring morphism. It respects addition, multiplication and the zero, but not the unity.

- Let S be a subring of a ring R. Let $i : S \to R$ be the **canonical inclusion**; this is simply the map that sends each $a \in S$ to itself. (You can view it as the restriction of the identity map $\operatorname{id}_R : R \to R$ to S.) Then, i is a ring morphism. Indeed, it respects multiplication because the multiplication of S is inherited from R; for similar reasons, it satisfies the other axioms in the definition of a ring morphism.

- Consider the map
$$\begin{aligned} f : \mathbb{C} &\to \mathbb{R}^{2\times 2}, \\ a + bi &\mapsto \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad \text{(for } a, b \in \mathbb{R}\text{)}. \end{aligned}$$

  This map f is a ring morphism. Indeed, it is easy to see that it respects addition, the zero and the unity. To see that it respects multiplication, you need to check that $f(zw) = f(z) \cdot f(w)$ for any $z, w \in \mathbb{C}$. But this is straightforward: Write $z = a + bi$ and $w = c + di$ and multiply out[1].

  This can also be proved using linear algebra: The $\mathbb{R}$-vector space $\mathbb{C}$ has basis $(1, i)$. If $z \in \mathbb{C}$, then $f(z)$ is the 2×2-matrix that represents the "multiply by z" operator (i.e., the map $\mathbb{C} \to \mathbb{C}$, $u \mapsto zu$) in this basis. Since the "multiply by zw" operator is the composition of the "multiply by z" operator with the "multiply by w" operator, it thus follows that $f(zw) = f(z) \cdot f(w)$ (because composition of endomorphisms of a vector space corresponds to multiplication of their representing matrices).

- The map $\mathbb{R}^{2\times 2} \to \mathbb{R}$, $A \mapsto \det A$ is **not** a ring morphism. It respects multiplication but not addition.

- Let R be a commutative ring. Let S be any set. Let R^S be the ring of all functions from S to R (with pointwise addition and multiplication). Fix any $s \in S$. Then, the map $R^S \to R$, $f \mapsto f(s)$ is a ring morphism. This map is known as the **evaluation morphism** at s, since all it does is evaluating a function at the constant s.

[1] In more detail: Writing $z = a + bi$ and $w = c + di$, we have $zw = (a + bi)(c + di) = (ac - bd) + (ad + bc)i$ and thus
$$f(zw) = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}.$$
However,
$$f(z) \cdot f(w) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -(ad + bc) & ac - bd \end{pmatrix}.$$
Comparing these two equalities yields $f(zw) = f(z) \cdot f(w)$.

Time for another warning. You couldn't have guessed, but our definition again differs from [DF] in how it treats unities! Namely, [DF] does not require a ring morphism to respect the unity. Thus, the map $\mathbb{Z} \to \mathbb{Z}$, $a \mapsto 0$ is a ring morphism according to [DF], but not according to us.

Let us show some basic properties of ring morphisms:

Proposition 1.1.2. Let R and S be two rings. Let $f : R \to S$ be an invertible ring morphism. Then, f is a ring isomorphism.

Proof. This is proved using the same reasoning as for groups (but not for topological spaces): You need to show that f^{-1} is a ring morphism. Let me just show that f^{-1} respects addition (the proofs of the other axioms are similar). So let $c, d \in S$; we must show that $f^{-1}(c+d) = f^{-1}(c) + f^{-1}(d)$.

It is clearly sufficient to check that $f\left(f^{-1}(c+d)\right) = f\left(f^{-1}(c) + f^{-1}(d)\right)$. Indeed, if we can show this equality, then we can apply f^{-1} to it and obtain $f^{-1}(c+d) = f^{-1}(c) + f^{-1}(d)$, which is what we want to prove.

Recall that f respects addition. Thus,

$$f\left(f^{-1}(c) + f^{-1}(d)\right) = f\left(f^{-1}(c)\right) + f\left(f^{-1}(d)\right) = c + d = f\left(f^{-1}(c+d)\right).$$

Hence, $f\left(f^{-1}(c+d)\right) = f\left(f^{-1}(c) + f^{-1}(d)\right)$ is proved. □

Incidentally, [DF] defines ring isomorphisms as invertible ring morphisms. Proposition 1.1.2 shows that this is equivalent to our definition.

Proposition 1.1.3. Let R, S and T be three rings. Let $f : S \to T$ and $g : R \to S$ be two ring morphisms. Then, $f \circ g : R \to T$ is a ring morphism.

Proof. This is proved in the same way as for groups. □

Proposition 1.1.4. Let R, S and T be three rings. Let $f : S \to T$ and $g : R \to S$ be two ring isomorphisms. Then, $f \circ g : R \to T$ is a ring isomorphism.

Proof. This is proved in the same way as for groups. □

Proposition 1.1.5. Let R and S be two rings. Let $f : R \to S$ be a ring isomorphism. Then, $f^{-1} : S \to R$ is a ring isomorphism.

Proof. This is proved in the same way as for groups. □

Corollary 1.1.6. The relation $\cong$ for rings is an equivalence relation.

Proof. Transitivity follows from Proposition 1.1.4. Reflexivity follows from the obvious fact that $\text{id} : R \to R$ is a ring isomorphism whenever R is a ring. Symmetry follows from Proposition 1.1.5. □

The next proposition shows that the "respects the zero" condition in the definition of a ring morphism is redundant (even though the "respects the unity" condition is not):

Proposition 1.1.7. Let R and S be two rings. Let $f : R \to S$ be a map that respects addition. Then, f automatically respects the zero.

Proof. Since f respects addition, we have $f(0_R + 0_R) = f(0_R) + f(0_R)$. Rewrite this as $f(0_R) = f(0_R) + f(0_R)$ (since $0_R + 0_R = 0_R$). Now, subtract $f(0_R)$ from both sides to get $0_S = f(0_R)$. In other words, f respects the zero. □

Note that we can restate our definition of a ring morphism as follows:

> A *ring morphism* is a map $f : R \to S$ between two rings R and S that is a group homomorphism from the additive group $(R, +, 0)$ to the additive group $(S, +, 0)$ and simultaneously a monoid homomorphism from the multiplicative monoid $(R, \cdot, 1)$ to the multiplicative group $(S, \cdot, 1)$.

It is easy to see that ring morphisms respect all sorts of operations constructed from $+$, $\cdot$, 0 and 1:

Proposition 1.1.8. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then:

(a) The map f respects finite sums; i.e., we have $f(a_1 + a_2 + \cdots + a_n) = f(a_1) + f(a_2) + \cdots + f(a_n)$ for any $a_1, a_2, \ldots, a_n \in R$.

(b) The map f respects finite products; i.e., we have $f(a_1 a_2 \cdots a_n) = f(a_1) \cdot f(a_2) \cdot \cdots \cdot f(a_n)$ for any $a_1, a_2, \ldots, a_n \in R$.

(c) The map f respects differences; i.e., we have $f(a - b) = f(a) - f(b)$ for any $a, b \in R$.

(d) The map f respects inverses; i.e., if a is a unit of R, then $f(a)$ is a unit of S, with inverse $(f(a))^{-1} = f\left(a^{-1}\right)$.

(e) The map f respects integer multiples; i.e., if $a \in R$ and $n \in \mathbb{Z}$, then $f(na) = nf(a)$.

(f) The map f respects powers; i.e., if $a \in R$ and $n \in \mathbb{N}$, then $f(a^n) = (f(a))^n$.

Proof. This is pretty straightforward, and you have probably seen the idea in group theory already. Details LTTR[2]. □

Recall that the **image** of a map $f : R \to S$ is defined to be the set $f(R) = \{f(r) \mid r \in R\}$; it is often denoted $\operatorname{Im} f$. This makes sense for arbitrary maps f between arbitrary sets R and S, not just for ring morphisms between rings. However, the image of a ring morphism has a special property:

[2] "LTTR" means "left to the reader".

Proposition 1.1.9. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then, $\operatorname{Im} f = f(R)$ is a subring of S.

Proof. Just check the axioms for a subring. For example, let's show that $f(R)$ is closed under multiplication:

Let $x, y \in f(R)$. We must show that $xy \in f(R)$. Since $x \in f(R)$, there exists some $a \in R$ such that $x = f(a)$. Similarly, there exists some $b \in R$ such that $y = f(b)$. Consider these a and b. From $x = f(a)$ and $y = f(b)$, we obtain

$$\begin{aligned} xy &= f(a) \cdot f(b) = f(ab) && \text{(since } f \text{ respects multiplication)} \\ &\in f(R), \end{aligned}$$

qed. □

1.2. Ideals and kernels ([DF, §7.1])

In linear algebra, the kernel (aka nullspace) of a linear map "measures how non-injective it is". The same can be done for ring morphisms:

Definition 1.2.1. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then, the **kernel** of f (denoted $\ker f$ or $\operatorname{Ker} f$) is defined to be the subset

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

of R.

Some examples:

- Let $n \in \mathbb{Z}$. The kernel of the ring morphism $\pi : \mathbb{Z} \to \mathbb{Z}/n,\ a \mapsto \overline{a}$ is $n\mathbb{Z} = \{\text{all multiples of } n\}$.
- Let R be a commutative ring. Let S be any set. Recall the ring R^S of all functions from S to R. Fix an element $s \in S$. Then, the kernel of the ring morphism $R^S \to R,\ f \mapsto f(s)$ 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, if $f : R \to S$ is an injective ring morphism, then f sends 0_R to 0_S (since f is a ring morphism), and therefore f cannot send any other element to 0_S (since f is injective).

As we see here, the kernel of a ring morphism is not usually a subring of R, since it normally does not contain 1_R. However, it satisfies all the other axioms for a subring (which is why [DF] considers it a subring of R). We can say more, however. The type of a subset that kernels of ring morphisms are has its own name:

Definition 1.2.2. Let R be a ring. An **ideal** of R is a subset I of R such that

- $a+b \in I$ for any $a, b \in I$;
- $ab \in I$ and $ba \in I$ for any $a \in R$ and $b \in I$;
- $0 \in I$ (where the 0 means the zero of R).

When R is commutative, of course, the "$ab \in I$" and "$ba \in I$" conditions are equivalent.

The three conditions in the definition of an ideal are called the "**ideal axioms**". The first and the third of them are familiar (they already appeared in the definition of a subring). The second is new – it is saying that if a factor in a product belongs to I, then the whole product belongs to I, no matter what the other factors are.

Proposition 1.2.3. Let R be a ring. Let I be an ideal of R. Then, I is a subgroup of the additive group $(R, +, 0)$.

Proof. The first and third "ideal axioms" reveal that I is closed under addition and contains 0. It remains to show that I is closed under negation – i.e., that we have $-b \in I$ for each $b \in I$. But this is easy: If $b \in I$, then the second "ideal axiom" (applied to $a = -1$) yields $(-1)\,b \in I$ and $b\,(-1) \in I$. But this rewrites as $-b \in I$, qed. □

Theorem 1.2.4. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then, the kernel $\operatorname{Ker} f$ of f is an ideal of R.

Proof. We need to prove the three "ideal axioms". Let me only show the second, as the other two are similar. So let $a \in R$ and $b \in \operatorname{Ker} f$. We must prove that $ab \in \operatorname{Ker} f$ and $ba \in \operatorname{Ker} f$.

We have $b \in \operatorname{Ker} f$, so that $f(b) = 0$ (by the definition of $\operatorname{Ker} f$). Now, the map f is a ring morphism and thus respects multiplication. Hence, $f(ab) = f(a) \cdot \underbrace{f(b)}_{=0} = f(a) \cdot 0 = 0$, so that $ab \in \operatorname{Ker} f$ (by the definition of $\operatorname{Ker} f$). Similarly, $ba \in \operatorname{Ker} f$. Thus we have shown the second ideal axiom. □

We will soon see a converse of this theorem: Every ideal of a ring R is the kernel of some ring morphism from R.

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

Proposition 1.2.5. 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, $0R = \{0_R\}$ and $1R = R$ are therefore principal ideals of R.

Proof. The only thing to prove is that uR is an ideal of R. This is easy:

- We have $a + b \in uR$ for any $a \in uR$ and $b \in uR$. (Indeed, if $a \in uR$ and $b \in uR$, then there exist $x, y \in R$ satisfying $a = ux$ and $b = uy$ (since $a \in uR$ and $b \in uR$), and therefore 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, if $a \in R$ and $b \in uR$, then there exists an $r \in R$ satisfying $b = ur$ (since $b \in uR$), and thus we have $ab = aur = u(ar) \in uR$ and thus $ba = ab \in uR$.)
- We have $0 \in uR$ (since $0 = u \cdot 0$). □

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

Principal ideals can also be defined for noncommutative rings, but this is more complicated[3].

In general, not all ideals of a ring need to be principal. An easy way to construct non-principal ideals is to work with polynomials in several variables over a field, or even with univariate polynomials over $\mathbb{Z}$. For example:

- The ideal of all polynomials $f \in \mathbb{Q}[x, y]$ that have constant term 0 is an ideal of $\mathbb{Q}[x, y]$ that is not principal.
- The ideal of all polynomials $f \in \mathbb{Z}[x]$ whose constant term is even is an ideal of $\mathbb{Z}[x]$ that is not principal.

We will come back to this later when we actually have defined polynomials.

1.3. Quotient rings ([DF, §7.3])

Let me first recall something I assume you have seen: quotient groups.

[3] Some details:

If R is a noncommutative ring, then **in general** neither $uR = \{ur \mid r \in R\}$ nor its mirror analogue $Ru = \{ru \mid r \in R\}$ are ideals of R. (For example, uR may fail the "$ab \in uR$ for any $a \in R$ and $b \in uR$" requirement, because there is no way to move the u to the left of the a.) This suggests considering the set $\{rus \mid r, s \in R\}$, but this is still not an ideal (in general), since it is not always closed under addition.

However, one can define the "principal ideal" RuR to be

$$\{\text{all finite sums of the form } r_1us_1 + r_2us_2 + \cdots + r_nus_n \text{ with } r_i, s_i \in R\}.$$

This is always an ideal of R.

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

- If H is merely a subgroup of a group G, then G/H is merely a "G-set" (i.e., a set with an action of G). However, when H is a **normal** subgroup of G (that is, a subgroup of G satisfying $gng^{-1} \in H$ for each $g \in G$ and $n \in H$), then G/H becomes a **group** as well, with group operation defined by
$$(g_1H)\,(g_2H) = g_1g_2H \qquad \text{for all } g_1, g_2 \in G. \tag{1}$$
The 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 always is a group.

- Now, assume that G is an **additive** group (which means that its binary operation is written as $+$ rather than as $\cdot$). This presupposes that G is abelian, as it is considered gauche to write a non-abelian group additively. Let H be a subgroup of G. Then, the cosets of H in G are denoted by $g + H$ instead of gH (in order to match the additive notation for the group operation). The equality (1) therefore rewrites as
$$(g_1 + H) + (g_2 + H) = (g_1 + g_2) + H \qquad \text{for all } g_1, g_2 \in G.$$
Note that the quotient group G/H is an abelian group.

- The most famous example of quotient groups is when $G = \mathbb{Z}$ and $H = n\mathbb{Z} = \{\text{all multiples of } n\}$ for some fixed integer n. (Here, the group operation on G is addition of integers.) In this case, the quotient group $\mathbb{Z}/n\mathbb{Z}$ is the cyclic group $\mathbb{Z}/n$, also known as Z_n. See Chapter XII of Samir Siksek's *Introduction to Abstract Algebra* (`http://homepages.warwick.ac.uk/~maseap/teaching/aa/aanotes.pdf`) for this and other examples.

We shall now define a similar quotient structure for rings instead of groups. Instead of normal subgroups, we will use ideals this time:

Definition 1.3.1. 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). Therefore, the quotient group R/I itself becomes an abelian group. Its elements are the cosets $r + I$ of I in R. (Note that, since our groups are additive, we are writing $r + I$ for what would normally be written rI in group theory.)

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 $1+I$ (as zero and unity), is a ring (as we will show in a moment). This ring is called the **quotient ring** of R by the ideal I; it is also pronounced "R **modulo** I". It is denoted R/I (so when you hear "the ring R/I", it always means the set R/I equipped with the structure just mentioned).

The cosets $r+I$ are called **residue classes** modulo I, and are often denoted $r \operatorname{mod} I$ or $[r]_I$ or $[r]$ or $\overline{r}$. (The last two notations are used when I is clear from the context.)

Theorem 1.3.2. Let R and I be as in Definition 1.3.1. Then, the multiplication on R/I is well-defined, and R/I does indeed become a ring when endowed with the operations and elements just described.

Before we prove this theorem, let us see some examples:

- Let $n \in \mathbb{Z}$. The set $n\mathbb{Z} = \{\text{all multiples of } n\}$ is a principal ideal of $\mathbb{Z}$. The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is precisely the ring $\mathbb{Z}/n$ we discussed above. Thus, the notion of a quotient ring generalizes the familiar concept of modular arithmetic. (More precisely, modular arithmetic is arithmetic in R/I where $R = \mathbb{Z}$ and $I = n\mathbb{Z}$.)

- Recall the ring $\mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$ of Gaussian integers. Consider its principal ideal

$$\begin{aligned} 3\mathbb{Z}[i] &= \{3r \mid r \in \mathbb{Z}[i]\} = \{3a+3bi \mid a,b \in \mathbb{Z}\} \\ &= \{c+di \mid c,d \in \mathbb{Z} \text{ are multiples of } 3\}. \end{aligned}$$

  What is the quotient ring $\mathbb{Z}[i] \ / \ (3\mathbb{Z}[i])$? The elements of this quotient ring have the form[4] $\overline{a+bi}$ with $a,b \in \{0,1,2\}$ (since any Gaussian integer can be reduced to an $a+bi$ with $a,b \in \{0,1,2\}$ by subtracting an appropriate Gaussian-integer multiple of 3). In other words,

$$\mathbb{Z}[i] \ / \ (3\mathbb{Z}[i]) = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{i},\ \overline{1+i},\ \overline{2+i},\ \overline{2i},\ \overline{1+2i},\ \overline{2+2i}\}.$$

  It is easy to see that this is a 9-element ring (i.e., the residue classes $\overline{0},\ \overline{1},\ \overline{2},\ \overline{i},\ \overline{1+i},\ \overline{2+i},\ \overline{2i},\ \overline{1+2i},\ \overline{2+2i}$ are distinct), and a field (i.e., all the nonzero residue classes are invertible). So we have found a finite field with 9 elements.

[4] We are using $\overline{z}$ to denote the residue class of a Gaussian integer $z \in \mathbb{Z}[i]$. This should not be confused with the complex conjugate of z (which is commonly denoted $\overline{z}$ as well).

For the curious: If we replace 3 by any other positive integer n, then $\mathbb{Z}[i] \ / \ (n\mathbb{Z}[i])$ will be a finite ring with n^2 elements, but not always a field. Understanding when it will be a field is a fruitful question in elementary number theory. (It is a field for some, but not for all, primes n.)

Proof of Theorem 1.3.2. To see that the multiplication on R/I is well-defined, we must prove that a product xy with $x, y \in R/I$ does not depend on how exactly we write x and y as $x = a + I$ and $y = b + I$. In other words, we must show that if $a + I = a' + I$ and $b + I = b' + I$, then $ab + I = a'b' + I$.

So let $a, a', b, b' \in R$ be such that $a + I = a' + I$ and $b + I = b' + I$. From $a + I = a' + I$, we obtain $a - a' \in I$, so that $(a - a')\, b \in I$ (by the second ideal axiom, since I is an ideal). In other words, $ab - a'b \in I$. Hence, $ab + I = a'b + I$. Similarly, we can obtain $a'b + I = a'b' + I$ (from $b + I = b' + I$). Thus, $ab + I = a'b + I = a'b' + I$, which is just what we need.

So the multiplication on R/I is well-defined. Now why is R/I a ring? This we leave to the reader – it's a straightforward consequence of the fact that R is a ring. □

Thus, ideals of rings are somewhat like normal subgroups of groups: You can "quotient them out" (this is slang for "take a quotient by them") and get a ring again.

Now, we are ready to show that any ideal of a ring is the kernel of a ring morphism:

Theorem 1.3.3. Let R be a ring. Let I be an ideal of R. Consider the map

$$\pi : R \to R/I, \qquad r \mapsto r + I.$$

Then, π is a surjective ring morphism with kernel I. This morphism π is called the **canonical projection** from R onto R/I.

Proof. LTTR[5]. □

The following theorem is known as the "universal property of quotient rings". It may appear technical and pointless for now, but its importance will become clear once you start constructing ring morphisms out of quotient rings and realize that the most comfortable way to do so is via this theorem.

Theorem 1.3.4 (Universal property of quotient rings)**.** Let R be a ring. Let I be an ideal of R.

Let S be a ring. Let $f : R \to S$ be a ring morphism. Assume that $f(I) = 0$ (this is shorthand for saying that $f(a) = 0$ for all $a \in I$). Consider the canonical projection $\pi : R \to R/I$. Then, there is a unique ring morphism $f' : R/I \to S$ satisfying $f = f' \circ \pi$.

[5] This abbreviation means "left to the reader".

The equality $f = f' \circ \pi$ in this theorem is oftentimes restated as follows: The diagram

$$\begin{tikzcd}
R \arrow[d, "\pi"'] \arrow[dr, "f"] & \\
R/I \arrow[r, dashed, "f'"'] & S
\end{tikzcd}$$

commutes. In general, a **diagram** is a bunch of sets and a bunch of maps between them, drawn as nodes and arrows; it is said to **commute** (or **be commutative**) if any two ways of going between two nodes yield the same map. In the above diagram, there are two ways of going from the R-node to the S-node: one is direct, while the other goes through R/I. The corresponding maps are f (for the direct way) and $f' \circ \pi$ (for the indirect way). This is the only pair of two different ways that go between the same two nodes; thus, the diagram commutes if and only if $f = f' \circ \pi$. Commutative diagrams become increasingly useful as you go deeper into algebra (and become ubiquitous when you get to category theory or homological algebra); for us here, this diagram is just a convenient aide-mémoire. Note that we have drawn the map f' as a dashed arrow, since this is the map whose existence is claimed, whereas the other two maps are given and thus drawn as regular arrows. This is a common convention and helps you distinguish the things you have from the things you are trying to construct.

Before we prove Theorem 1.3.4, let us give an example:

- Consider the canonical projections

  $$\pi_6 : \mathbb{Z} \to \mathbb{Z}/6 \qquad \text{and} \qquad \pi_3 : \mathbb{Z} \to \mathbb{Z}/3.$$

  Both of them send each integer a to its residue class; but the residue class is $a + 6\mathbb{Z}$ for the first map and $a + 3\mathbb{Z}$ for the second.

  I claim that there is a unique ring morphism $\pi_3' : \mathbb{Z}/6 \to \mathbb{Z}/3$ such that $\pi_3 = \pi_3' \circ \pi_6$. Indeed, this is what Theorem 1.3.4 says when it is applied to $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $\pi = \pi_6$, $S = \mathbb{Z}/3$ and $f = \pi_3$, because the ideal $6\mathbb{Z}$ satisfies $\pi_3(6\mathbb{Z}) = 0$ (check this!).

  How would you construct this π_3' ? The equation $\pi_3 = \pi_3' \circ \pi_6$ is equivalent to saying that $\pi_3(a) = \pi_3'(\pi_6(a))$ for any $a \in \mathbb{Z}$; in other words, it is saying that $a + 3\mathbb{Z} = \pi_3'(a + 6\mathbb{Z})$ for any $a \in \mathbb{Z}$ (since $\pi_3(a) = a + 3\mathbb{Z}$ and $\pi_6(a) = a + 6\mathbb{Z}$). So the map π_3' needs to send the residue classes

  $$\begin{array}{lllllll} 0+6\mathbb{Z}, & 1+6\mathbb{Z}, & 2+6\mathbb{Z}, & 3+6\mathbb{Z}, & 4+6\mathbb{Z}, & 5+6\mathbb{Z} & \text{to} \\ 0+3\mathbb{Z}, & 1+3\mathbb{Z}, & 2+3\mathbb{Z}, & 3+3\mathbb{Z}, & 4+3\mathbb{Z}, & 5+3\mathbb{Z}, & \end{array}$$

  respectively. In other words, it needs to send the residue classes

  $$\begin{array}{lllllll} 0+6\mathbb{Z}, & 1+6\mathbb{Z}, & 2+6\mathbb{Z}, & 3+6\mathbb{Z}, & 4+6\mathbb{Z}, & 5+6\mathbb{Z} & \text{to} \\ 0+3\mathbb{Z}, & 1+3\mathbb{Z}, & 2+3\mathbb{Z}, & 0+3\mathbb{Z}, & 1+3\mathbb{Z}, & 2+3\mathbb{Z}, & \end{array}$$

respectively. This uniquely determines this map. If you want, you can easily check by hand that this map is indeed a ring morphism.

More generally, if n and m are two integers such that $m \mid n$, and if

$$\pi_n : \mathbb{Z} \to \mathbb{Z}/n \qquad \text{and} \qquad \pi_m : \mathbb{Z} \to \mathbb{Z}/m$$

are the canonical projections, then there is a unique ring morphism $\pi'_m : \mathbb{Z}/n \to \mathbb{Z}/m$ such that $\pi'_m \circ \pi_n = \pi_m$. This morphism can be regarded as reducing a modulo-n residue class "further" to a modulo-m residue class.

Let us now prove the universal property of quotient rings:

Proof of Theorem 1.3.4. What does $f = f' \circ \pi$ mean? It means that $f(r) = f'(\pi(r))$ for each $r \in R$. In other words, it means that $f(r) = f'(r+I)$ for each $r \in R$ (since $\pi(r) = r + I$ by the definition of π). But this equality uniquely determines (actually overdetermines) all values of f' (since any element of R/I has the form $r + I$ for some $r \in R$). Thus, if we want to construct a map f' that satisfies $f = f' \circ \pi$, the only thing we can do is to set

$$f'(r+I) = f(r) \qquad \text{for each } r \in R. \tag{2}$$

We now need to show two facts:

1. This map f' is well-defined – i.e., the value $f(r)$ depends only on the coset $r + I$ but not on the specific choice of r. (If this wasn't the case, then the equality (2) would give two conflicting values for a single value of f', which would spell doom for our map f'.)

2. This map f' is a ring morphism.

Let us prove Fact 1 first. So let $r, r' \in R$ be such that $r + I = r' + I$. We must show that $f(r) = f(r')$.

We do what we can: From $r + I = r' + I$, we obtain $r - r' \in I$, so that $f(r - r') = 0$ because $f(I) = 0$. However, f is a ring morphism and thus respects differences; hence, $f(r - r') = f(r) - f(r')$. Thus, $f(r) - f(r') = f(r - r') = 0$, so that $f(r) = f(r')$. This proves Fact 1.

Let us now prove Fact 2. We need to show that f' is a ring morphism. There are four axioms to check; we shall only show that f' respects multiplication (as the other three axioms follow the same mold).

So let $a, b \in R/I$. We must show that $f'(ab) = f'(a) \cdot f'(b)$.

Write the cosets $a, b \in R/I$ as $a = r + I$ and $b = s + I$ for some $r, s \in R$. Then, $ab = (r+I)(s+I) = rs + I$ because of how we defined multiplication on R/I. Hence, $f'(ab) = f'(rs + I) = f(rs)$ (by (2)). On the other hand, $a = r + I$ and thus $f'(a) = f'(r + I) = f(r)$ (by (2)). Similarly, $f'(b) = f(s)$. Thus,

$$\begin{aligned} f'(ab) = f(rs) &= \underbrace{f(r)}_{=f'(a)} \cdot \underbrace{f(s)}_{=f'(b)} \qquad \text{(since } f \text{ is a ring morphism)} \\ &= f'(a) \cdot f'(b), \end{aligned}$$

which is precisely what we wanted to prove. Thus, Fact 2 is proved as well.

So we have constructed a ring morphism $f' : R/I \to S$ that satisfies (2) and therefore satisfies $f = f' \circ \pi$. The uniqueness of such an f' is obvious, since (as we have seen) the equality (2) determines all values of f'. Thus, the theorem is proven. □