Math 332 Winter 2023, Lecture 6: Rings

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

1. Rings and ideals (cont'd)

1.7. Ring morphisms

1.7.1. Definition and examples

Modern mathematics is often a study of (1) sets with some structure, and (2) maps that respect this structure. The maps are just as important as the sets, if not more so. For example: 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 1.7.1. Let R and S be two rings.

(a) A **ring homomorphism** (or, for short, **ring morphism**) 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** 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 $f : R \to S$.

Examples:

- Let $n \in \mathbb{Z}$. The map
$$\pi : \mathbb{Z} \to \mathbb{Z}/n, \quad a \mapsto \overline{a}$$
that sends each integer a to its residue class $\overline{a} = a + n\mathbb{Z}$ 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

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}, \\ a &\mapsto 2a \end{aligned}$$

is not a ring morphism. It respects addition and zero, but it does not respect multiplication and unity.

- The map

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}, \\ a &\mapsto 0 \end{aligned}$$

is not a ring morphism, since it does not respect the unity (although it respects everything else). However, the map

$$\begin{aligned} \mathbb{Z} &\to (\text{the zero ring}), \\ a &\mapsto 0 \end{aligned}$$

is a ring morphism. The target of the map matters!

- The map

$$\begin{aligned} \mathbb{Z} &\to \mathbb{Z}, \\ a &\mapsto a^2 \end{aligned}$$

is not a ring morphism, since it does not respect addition ($(a+b)^2 \neq a^2+b^2$ in general), although its respects everything else.

- 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 element $a \in S$ to itself. Then, i is a ring morphism. For example, it respects addition because $i(a) + i(b) = a + b = i(a+b)$ for all $a, b \in S$ (and this is true because the addition of S is inherited from R).

- Consider the map

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

This map f is a ring morphism. For example, let us check that f respects multiplication: We need to show that

$$f(zw) = f(z) \cdot f(w) \qquad \text{for all } z, w \in \mathbb{C}.$$

We fix $z, w \in \mathbb{C}$, and we write z and w as $z = a + bi$ and $w = c + di$ with $a, b, c, d \in \mathbb{R}$. Then,

$$\begin{aligned} f(zw) &= f((a+bi)(c+di)) = f((ac-bd)+(ad+bc)i) \\ &= \begin{pmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} f(z) \cdot f(w) &= f(a+bi) \cdot f(c+di) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} \\ &= \begin{pmatrix} ac-bd & ad+bc \\ -bc-ad & -bd+ac \end{pmatrix}, \end{aligned}$$

which is the same matrix. Thus, f respects multiplication. All the other morphism axioms are just as easy. So f is a ring morphism.

Since f is injective, you can use the matrix $f(z) \in \mathbb{R}^{2\times 2}$ as a "stand-in" for the complex number z. So instead of calculating with complex numbers, you can work with their images under f instead.

This is not an isolated occurrence. There is also an injective ring morphism

$$\begin{aligned} g : \mathbb{H} &\to \mathbb{R}^{4\times 4}, \\ a+bi+cj+dk &\mapsto \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}. \end{aligned}$$

Several more rings we will study later can be "represented" by matrices, in the sense that we can find injective morphisms from those rings to matrix rings, and thus work with matrices instead of with abstract objects.

- The map

$$\begin{aligned} \mathbb{R}^{2\times 2} &\to \mathbb{R}, \\ A &\mapsto \det A \end{aligned}$$

is not a ring morphism, since it disrespects addition (although it respects everything else).

- Let R be a ring. Let S be any set. Let R^S be the ring of all maps from S to R (with pointwise $+$ and $\cdot$). Fix any $s \in S$. Then, the map

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

is a ring morphism. This is just a roundabout way of saying that any maps $g, h \in R^S$ satisfy

$$\begin{aligned} (g+h)(s) &= g(s) + h(s); \\ (gh)(s) &= g(s) \cdot h(s); \\ 0(s) &= 0; \\ 1(s) &= 1. \end{aligned}$$

But these equalities follow from our definition of how functions in R^S are added and multiplied (namely, pointwise).

See §2.7.1 in the text for more examples of morphisms.

1.7.2. Basic properties of ring morphisms

The composition of two ring morphisms is again a ring morphism. Or, to be more formal:

Proposition 1.7.2. Let R, S, 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. Same as for groups. □

The following proposition simplifies the definition of a ring morphism somewhat:

Proposition 1.7.3. Let R and S be two rings. Let $f : R \to S$ be a map that respects addition. Then, f respects the zero.

Proof. We have $f(0_R + 0_R) = f(0_R) + f(0_R)$ (since f respects addition). In view of $0_R + 0_R = 0_R$, we can rewrite this as

$$f(0_R) = f(0_R) + f(0_R).$$

Now, subtract $f(0_R)$ from both sides, and you get $0_S = f(0_R)$, which means that f respects the zero. □

Thus, the "respects the zero" axiom in the definition of a morphism is redundant. Nevertheless, I have chosen to keep it in, as I think it deserves its place in the definition.

By the way, we can restate the 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 $(R, +, 0)$ to $(S, +, 0)$ and simultaneously a monoid homomorphism from $(R, \cdot, 1)$ and $(S, \cdot, 1)$.

Ring morphisms preserve the basic structures of a ring ($+$, $\cdot$, 0 and 1) by definition. Therefore, they also preserve some of the structures that are derived from these basic structures:

Proposition 1.7.4. 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 all $a_1, a_2, \ldots, a_n \in R$.

(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 all $a_1, a_2, \ldots, a_n \in R$.

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

(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. LTTR (= left to the reader). □

1.7.3. The image of a ring morphism

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 by $\operatorname{Im} f$. This makes sense for any map between any sets, but in particular it makes sense for ring morphisms. Their images are nice:

Proposition 1.7.5. 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. For example, the product of two elements of $\operatorname{Im} f$ belongs to $\operatorname{Im} f$, since $f(a) f(b) = f(ab)$. Thus, $\operatorname{Im} f$ is closed under multiplication. The other subring axioms are similar. □

For instance, recall the ring morphism

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

Its image $\operatorname{Im} f$ is a commutative subring of $\mathbb{R}^{2\times 2}$. It consists of all 2×2-matrices whose diagonal entries are equal and whose off-diagonal entries add up to 0.

1.7.4. Basic properties of ring isomorphisms

When proving that a map f is a ring isomorphism, you have to check (1) that f is a ring morphism, (2) that f has an inverse, and (3) that this inverse f^{-1} is a ring morphism; at least, this is what the definition of a ring isomorphism would require you to do. It turns out, however, that (3) is unnecessary, since it follows from (1) and (2):

Proposition 1.7.6. Let R and S be two rings. Let $f : R \to S$ be an invertible ring morphism. Then, f is a ring isomorphism.

Proof. We need to show that f^{-1} is a ring morphism as well. For instance, we need to check that

$$f^{-1}(c+d) = f^{-1}(c) + f^{-1}(d) \qquad \text{for all } c, d \in S.$$

But this follows easily by setting $a = f^{-1}(c)$ and $b = f^{-1}(d)$ and applying $f(a+b) = f(a) + f(b)$. For details, see Proposition 2.7.7 in the text. □

Here are some further properties of ring isomorphisms:

Proposition 1.7.7. Let R, S, 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. Same as for groups. □

Proposition 1.7.8. 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. Same as for groups. □

Corollary 1.7.9. The relation $\cong$ for rings is an equivalence relation.

Proof. The previous two propositions show that it is transitive and symmetric. Reflexivity is clear, since $\mathrm{id} : R \to R$ is a ring isomorphism. □

The most useful property of ring isomorphisms is the following "meta-theorem":

> **Isomorphism principle for rings:** Let R and S be two isomorphic rings. Then, any "ring-theoretic" property of R (that is, any property that does not refer to specific elements, but can be stated entirely in terms of ring operations) that holds for R must hold for S as well.

This is rather nebulous (what does "ring-theoretic" mean?), so let me give examples. Here are some examples of "ring-theoretic" properties:

- The ring R has 15 elements.
- The ring R is commutative.
- The ring R is a field.
- For any $a, b, c \in R$, we have $3abc\,(a+b+c) = 0$ (where 0 is the zero of R).
- The center of R has 10 elements.
- There exist two nonzero elements $a, b \in R$ such that $a^2 + b^2 = 0$.

So all of these properties can be automatically transported along isomorphisms (i.e., if they hold for one ring R, then they also hold for all rings isomorphic to R).

Here are some non-"ring-theoretic" properties:

- The elements of R are matrices.
- The set R is disjoint from $\mathbb{C}$.
- The set R contains the complex number $i = \sqrt{-1}$.

Clearly, an isomorphism can destroy these properties, since it can send elements to different elements.

A ring isomorphism $f : R \to S$ is like a train that can transport anything back and forth between the rings R and S. The isomorphism principle is just a semi-rigorous way to draw the obvious conclusions from this. I will not state it precisely, but you should be able to rigorously justify any specific application of this principle.

1.7.5. What about kernels?

We have defined the image of a ring morphism, which is somewhat similar to the column space of a matrix. Another standard construction with matrices is the kernel (aka nullspace). This, too, has an analogue for rings:

Definition 1.7.10. 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

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

Is this kernel $\operatorname{Ker} f$ a subring of R ? No, because it rarely contains 1. Nevertheless, it has a bunch of the same properties: It is closed under addition and multiplication and contains 0. And even something stronger. More on that next time!