Math 332 Winter 2023, Lecture 10: Rings

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

1. Rings and ideals (cont'd)

1.9. Quotient rings (cont'd)

1.9.5. The universal property of quotient rings

When trying to understand a quotient ring R/I, it is important to construct ring morphisms into and out of it.

Constructing morphisms $\alpha : S \to R/I$ into a quotient ring R/I is generally easy. (For example, we did so in the proof of Theorem 1.9.5 in Lecture 9.)

Constructing morphisms $\beta : R/I \to S$ out of a quotient ring R/I is harder: Not only do you have to define what $\beta(\overline{r})$ is for any given residue class $\overline{r}$, but you also need to make sure that this value $\beta(\overline{r})$ will depend not on r but only on the residue class $\overline{r}$. This is called "well-definedness", and is usually not immediately obvious, because one and the same residue class in R/I can be written as $\overline{r}$ for different values of $r \in R$. In other words, the well-definedness of β does not come for free if we just define $\beta(\overline{r})$ by some formula for all $r \in R$; we also need to check that the value that this formula gives is unambiguous.

This can be done by hand, but it is extra work (adding to the trouble of proving that β is a ring morphism).

The **universal property of quotient rings** is a theorem that does some of this work for you. It gives a way to define a ring morphism $\beta : R/I \to S$ by providing a ring morphism $f : R \to S$ and showing that $f(I) = 0$ (that is, f sends all elements of I to 0). Once you have done this part, the theorem automatically gives you a ring morphism $f' : R/I \to S$ that sends each residue class $\overline{r} \in R/I$ to $f(r)$. Here is the precise statement:

Theorem 1.9.6 (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 $f(I) = 0$ (by this we mean that $f(i) = 0$ for each $i \in I$). Then, the map

$$\begin{aligned} f' : R/I &\to S, \\ \overline{r} &\mapsto f(r) \qquad \text{(for all } r \in R\text{)} \end{aligned}$$

is well-defined (i.e., the value $f(r)$ depends only on the residue class $\overline{r}$, not on r itself) and is a ring morphism.

Here is an example:

- Consider the canonical projections

$$\begin{aligned} \pi_6 : \mathbb{Z} &\to \mathbb{Z}/6, \\ r &\mapsto r + 6\mathbb{Z} \end{aligned}$$

and

$$\begin{aligned} \pi_3 : \mathbb{Z} &\to \mathbb{Z}/3, \\ r &\mapsto r + 3\mathbb{Z}. \end{aligned}$$

(Each of these two projections sends each integer r to its residue class $\overline{r}$, but the residue class is a modulo-6 class for π_6 and a modulo-3 class for π_3.)

Then, $\pi_3(6\mathbb{Z}) = 0$ (because any $j \in 6\mathbb{Z}$ is a multiple of 6, thus a multiple of 3, and therefore its residue class $j + 3\mathbb{Z}$ is $\overline{0}$, and thus $\pi_3(j) = j + 3\mathbb{Z} = \overline{0} = 0_{\mathbb{Z}/3}$). Thus, by Theorem 1.9.6 (applied to $R = \mathbb{Z}$, $I = 6\mathbb{Z}$, $S = \mathbb{Z}/3$ and $f = \pi_3$), we see that the map

$$\begin{aligned} \pi_3' : \mathbb{Z}/6 &\to \mathbb{Z}/3, \\ \overline{r} &\mapsto \pi_3(r) \qquad (\text{that is, } r + 6\mathbb{Z} \mapsto r + 3\mathbb{Z}) \end{aligned}$$

is well-defined and is a ring morphism. Explicitly, this morphism π_3' sends

$$\begin{aligned} &\text{the modulo-6 residue classes } \overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5} \\ &\text{to the modulo-3 residue classes } \overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}. \end{aligned}$$

In other words, it sends

$$\begin{aligned} &\text{the modulo-6 residue classes } \overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5} \\ &\text{to the modulo-3 residue classes } \overline{0},\ \overline{1},\ \overline{2},\ \overline{0},\ \overline{1},\ \overline{2} \end{aligned}$$

(because in $\mathbb{Z}/3$, we have $\overline{3} = \overline{0}$ and $\overline{4} = \overline{1}$ and $\overline{5} = \overline{2}$). If you want, you can easily check that this is actually a morphism.

More generally, if n and m are two integers such that $m \mid n$, then there is a ring morphism

$$\begin{aligned} \mathbb{Z}/n &\to \mathbb{Z}/m, \\ \overline{r} &\mapsto \overline{r} \qquad (\text{that is, } r + n\mathbb{Z} \mapsto r + m\mathbb{Z}). \end{aligned} \tag{1}$$

This follows from Theorem 1.9.6, applied to $R = \mathbb{Z}$, $I = n\mathbb{Z}$, $S = \mathbb{Z}/m$ and $f = \pi_m$ (the canonical projection from $\mathbb{Z}$ to $\mathbb{Z}/m$).

Incidentally, this accounts for all ring morphisms that go between two quotient rings of $\mathbb{Z}$. That is:

- If m and n are two integers such that $m \mid n$, then there is only one ring morphism $\mathbb{Z}/n \to \mathbb{Z}/m$, and it is the one we just constructed (sending each $r + n\mathbb{Z}$ to $r + m\mathbb{Z}$).
- If m and n are two integers such that $m \nmid n$, then there is no ring morphism $\mathbb{Z}/n \to \mathbb{Z}/m$.

Proving this is a nice (and easy) exercise!

Proof of Theorem 1.9.6. First, we must prove that f' is well-defined (i.e., that the formula $f'(\overline{r}) = f(r)$ does not assign two different output values to one and the same residue class).

In other words, we must show that if two elements a and b of R have the same residue class $\overline{a} = \overline{b}$ (modulo I), then $f(a) = f(b)$.

So let us do this. Let a and b be two elements of R such that $\overline{a} = \overline{b}$. From $\overline{a} = \overline{b}$, we obtain $a - b \in I$. Hence, $f(a - b) = 0$ (because $f(I) = 0$). However, f is a ring morphism and thus respects differences. Hence, $f(a - b) = f(a) - f(b)$. Thus, $f(a) - f(b) = f(a - b) = 0$, and therefore $f(a) = f(b)$, as desired.

Thus, we have proved that the map f' is well-defined, i.e., exists.

It remains to prove that f' is a ring morphism. We have four axioms to check, but we will only check the "respects multiplication" axiom, since the other three axioms are proved similarly.

To check the "respects multiplication" axiom, we must prove that $f'(xy) = f'(x) \cdot f'(y)$ for all $x, y \in R/I$.

Fix $x, y \in R/I$. Then, $x = \overline{a}$ and $y = \overline{b}$ for some $a, b \in R$ (since any element of R/I is a residue class, i.e., has the form $\overline{r}$ for some $r \in R$). Using these a and b, we then have

$$xy = \overline{a} \cdot \overline{b} = \overline{ab} \qquad \text{(by the definition of the multiplication on } R/I\text{)},$$

so that

$$\begin{aligned} f'(xy) &= f'\left(\overline{ab}\right) = f(ab) && \left(\text{by the definition of } f'\right) \\ &= f(a) \cdot f(b) && (\text{since } f \text{ is a ring morphism}) \end{aligned}$$

and

$$f'\left(\underbrace{x}_{=\overline{a}}\right) \cdot f'\left(\underbrace{y}_{=\overline{b}}\right) = \underbrace{f'(\overline{a})}_{\substack{=f(a) \\ \text{(by the} \\ \text{definition of } f')}} \cdot \underbrace{f'\left(\overline{b}\right)}_{\substack{=f(b) \\ \text{(by the} \\ \text{definition of } f')}} = f(a) \cdot f(b).$$

Comparing the last two equalities, we find $f'(xy) = f'(x) \cdot f'(y)$. Thus, we have shown that f' respects multiplication. As we said, the other axioms can be checked in the same way, so we have shown that f' is a ring morphism. This concludes the proof of Theorem 1.9.6. $\square$

So we have proved the universal property of quotient rings.

For various reasons, it is helpful to have an alternative formulation of this property, which does not refer to specific elements but instead "implicitly" describes the morphism f' by an equality:

Theorem 1.9.7 (Universal property of quotient rings, abstract form)**.** Let R be a ring. Let I be an ideal of R. Let $\pi : R \to R/I$ be the canonical projection (sending each $r \in R$ to its residue class $\overline{r}$).

Let S be a ring. Let $f : R \to S$ be a ring morphism. Assume that $f(I) = 0$ (that is, $f(i) = 0$ for each $i \in I$). Then, there is a unique ring morphism $f' : R/I \to S$ that satisfies

$$f = f' \circ \pi.$$

Proof. Theorem 1.9.6 shows that there is a unique ring morphism $f' : R/I \to S$ that satisfies

$$f'(\overline{r}) = f(r) \qquad \text{for all } r \in R. \tag{2}$$

We shall now prove that the equality $f = f' \circ \pi$ is just an equivalent restatement of the condition (2).

Indeed, we have the following chain of equivalences:

$$\begin{aligned}
&\left(f = f' \circ \pi\right) \\
&\iff \left(f(r) = \left(f' \circ \pi\right)(r) \text{ for all } r \in R\right) \qquad \left(\begin{array}{c}\text{since two maps are equal}\\ \text{if and only if they}\\ \text{agree on each input}\end{array}\right) \\
&\iff \left(f(r) = f'(\pi(r)) \text{ for all } r \in R\right) \qquad \left(\text{since } \left(f' \circ \pi\right)(r) = f'(\pi(r)) \text{ for each } r\right) \\
&\iff \left(f(r) = f'(\overline{r}) \text{ for all } r \in R\right) \qquad \left(\text{since } \pi(r) = \overline{r} \text{ for each } r\right) \\
&\iff \left(f'(\overline{r}) = f(r) \text{ for all } r \in R\right).
\end{aligned}$$

In other words, the equality $f = f' \circ \pi$ is equivalent to the condition (2).

Now, recall that there is a unique ring morphism $f' : R/I \to S$ that satisfies the condition (2). In view of the previous sentence, we can reformulate this as follows: There is a unique ring morphism $f' : R/I \to S$ that satisfies $f = f' \circ \pi$. This proves Theorem 1.9.7. □

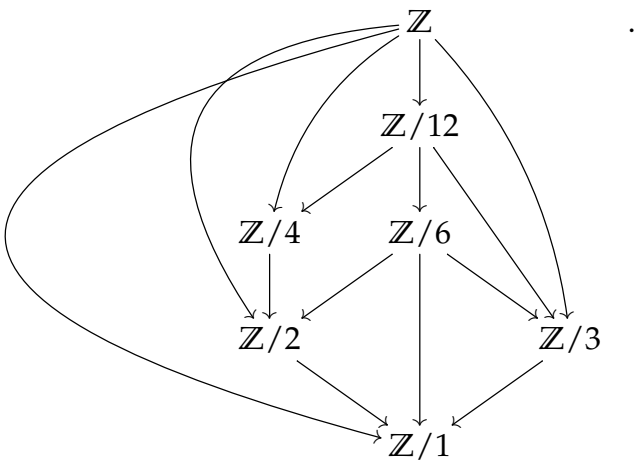
The equality $f = f' \circ \pi$ in Theorem 1.9.7 can be restated in yet another way: Namely, it is restated as "the diagram

$$\begin{array}{ccc} R & & \\ {\scriptstyle\pi}\downarrow & \searrow^{f} & \\ R/I & \xrightarrow[f']{} & S \end{array}$$

commutes". In general, a **diagram** is a bunch of sets (drawn as nodes) and a bunch of maps between these sets (drawn as arrows between these nodes). In

our case, the sets are the rings R, R/I, S and the maps are the ring morphisms f, π, f'. We say that a diagram **commutes** (or **is commutative**) if, for any two nodes in the diagram, all ways of going from the first node to the second (walking along the arrows) result in the same composed map. In our case, there are two ways to go from R to S: one direct way, which gives the map f, and one indirect way (via R/I), which gives the map $f' \circ \pi$. Thus, the commutativity of the above diagram is saying that $f = f' \circ \pi$ (and this is all that it is saying, since there are no two other ways that go between the same two nodes).

In general, diagrams are a good way to visualize situations in which there are several maps going between the same sets. For example, here is a diagram that shows the rings $\mathbb{Z}$, $\mathbb{Z}/12$, $\mathbb{Z}/6$, $\mathbb{Z}/4$, $\mathbb{Z}/3$, $\mathbb{Z}/2$ and $\mathbb{Z}/1$ (the latter ring is trivial) as well as various morphisms between them:



In this diagram, all arrows coming out of the $\mathbb{Z}$ node are canonical projections $\mathbb{Z} \to \mathbb{Z}/n$ (sending each $r \in \mathbb{Z}$ to $\overline{r} \in \mathbb{Z}/n$), whereas all the other arrows are instances of the morphisms (1) constructed above. Note that we have not drawn all possible morphisms (e.g., the morphism $\mathbb{Z}/4 \to \mathbb{Z}/1$ is missing) to avoid crowding the diagram. This diagram commutes, as you can easily see directly by convincing yourself that each of the arrows sends each residue class $\overline{r}$ (or, in the case of $\mathbb{Z}$, each integer r) to the corresponding residue class $\overline{r}$ modulo the respective number.

We do not have any particularly strong need for diagrams in this course, but they can be helpful as visual aids. More advanced courses such as homological algebra and category theory involve diagrams in far more substantial ways.

1.9.6. Injectivity means zero kernel

Let us take a break from abstractions and notations, and prove a simple lemma about injectivity of ring morphisms:

Lemma 1.9.8. Let R and S be two rings. Let $f : R \to S$ be a ring morphism. Then, f is injective if and only if $\operatorname{Ker} f = \{0_R\}$.

Proof. You may have seen analogous results about groups or vector spaces; the proof is essentially the same. Nevertheless, let me prove Lemma 1.9.8 from scratch:

$\Longrightarrow$: If f is injective, then

$$\begin{aligned}
\operatorname{Ker} f &= \{r \in R \mid f(r) = 0_S\} && \text{(by the definition of a kernel)} \\
&= \{r \in R \mid f(r) = f(0_R)\} && \left(\begin{array}{c}\text{since } 0_S = f(0_R) \\ \text{(because } f \text{ is a ring morphism)}\end{array}\right) \\
&= \{r \in R \mid r = 0_R\} && \left(\begin{array}{c}\text{since } f \text{ is injective, and thus } f(r) = f(0_R) \\ \text{can only happen if } r = 0_R\end{array}\right) \\
&= \{0_R\}.
\end{aligned}$$

$\Longleftarrow$: Assume that $\operatorname{Ker} f = \{0_R\}$. We must show that f is injective. In other words, we must show that any $a, b \in R$ that have the same value under f (that is, satisfy $f(a) = f(b)$) must be equal (that is, $a = b$).

So let $a, b \in R$ be two elements satisfying $f(a) = f(b)$. We must prove that $a = b$.

The map f is a ring morphism, hence respects differences. Thus

$$f(a - b) = f(a) - f(b) = 0_S \qquad (\text{since } f(a) = f(b)).$$

In other words, $a - b \in \operatorname{Ker} f = \{0_R\}$, which means that $a - b = 0_R$. In other words, $a = b$. This proves that f is injective. $\square$