Lecture 27: Ideals and quotients

Last time we saw what rings were: They're sets with a notion of addition and multiplication.

Exercise 27.1. (1) Write out the multiplication table for $\mathbb{Z}/4\mathbb{Z}$.

Answer:

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

(2) If R is a ring and $a, b \in R$, show that

$$(-a)b = -(ab).$$

Answer: $ab + (-a)b = (a-a)b = 0b = 0$ So the additive inverse of ab is given by $(-a)b$.

1. Homomorphisms

There's a notion of homomorphism and isomorphism for rings, too.

Definition 27.2. Let R and S be rings, and let $f : R \to S$ be a function. We say that f is a *ring homomorphism* if

(1) f is a group homomorphism for addition,
(2) $f(1) = 1$ (so f sends the multiplicative unit of R to that of S), and
(3) $f(ab) = f(a)f(b)$ for all $a, b \in R$.

We further say f is an *isomorphism* if f is abijection.

Now I wanted to say something more about why $\mathbb{Z}/n\mathbb{Z}$ is a ring. How did we see it was a group? By applying a general principle: If $H \lhd G$, then G/H is a group.

I want to do the same thing with rings. But for this lecture (and for most lectures hereon), when I say ring, I will mean a *commutative* ring.

2. Ideals

You might think something along the lines of: If $S \subset R$ is a "normal" subring, then R/S is going to be some ring. That's the blind analogy to groups. Well, that analogy is wrong.

Definition 27.3. Let R be a commutative ring. A subset $I \subset R$ is called an *ideal* if

(1) I is a subgroup under addition, and
(2) $x \in I$ implies $rx \in I$ for all $r \in R$.

Remark 27.4. Note that (2) implies that if $x, y \in I$, then $xy \in I$. So it looks like a closure condition for being a subobject. But I need not have the multiplicative identity of R, so I is definitely not a subring. What (2) is really saying, heuristically, is that I sucks everr element of R into I via multiplication.

Exercise 27.5. For every non-zero integer n, let $n\mathbb{Z} \subset \mathbb{Z}$ be those integers which are multiples of n. Show that $n\mathbb{Z}$ is an ideal inside the ring $\mathbb{Z}$.

Answer: (1) $n\mathbb{Z}$ contains 0, and if two numbers are divisible by n, so its their sum. Likewise, if a is divisible by n, so is $-a$. So $n\mathbb{Z}$ is a subgroup under addition. (2) Finally, if r is any integer and x is divisible by n, then rx is divisible by n.

Remark 27.6. Since R is abelian, note that any subgroup I is normal. So there is an abelian group R/I.

Proposition 27.7. Let R be a commutative ring, and $I \subset R$ an ideal. Then the operation

$$\times : R/I \times R/I \to R/I, \qquad \overline{r} \cdot \overline{s} = \overline{rs}$$

along with the usual addition on R/I, makes R/I a commutative ring.

Proof. We need to show that this operation doesn't depend on the choice of representative $r \in \overline{r}, s \in \overline{s}$.

So let $r' = r + x$ and $s' = s + y$ where $x, y \in I$. (This just means $\overline{r'} = \overline{r} \in R/I$, and that $\overline{s'} = \overline{s} \in R/I$.)

Then

$$r's' = (r + x)(s + y) = rs + xs + ry + xy.$$

Note the last three terms are in I because I is an ideal, and hence their sum is in I because I is a subgroup. So $\overline{r's'} = \overline{rs}$. That is, the operation is well-defined.

We already know that $(R/I, +)$ is an abelian group. So we need to show that $(R/I, \times)$ is an abelian monoid, and that multiplication distributes over addition.

Well, multiplication is associative because

$$(\overline{a}\overline{b})\overline{c} = \overline{ab}\overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a}(\overline{bc}).$$

Note that the key step there was invoking the fact that $(R, \times)$ is associative.

It is commutative because

$$\overline{a}\overline{b} = \overline{ab} = \overline{ba} = \overline{b}\overline{a}$$

where again, the middle equality is just using that $(R, \times)$ is commutative.

The multiplicative unit is $\overline{1}$:

$$\overline{1}\overline{a} = \overline{1a} = \overline{a}, \qquad \overline{a}\overline{1} = \overline{a1} = \overline{a}.$$

Finally, multiplication distributes over addition because

$$\overline{a}(\overline{b} + \overline{c}) = \overline{a(b+c)} = \overline{ab+bc} = \overline{a}\overline{b} + \overline{b}\overline{c}.$$

$\square$

So to get new and interesting rings, we can look for ideals and then take quotient rings.

Example 27.8. The ring $\mathbb{Z}/n\mathbb{Z}$ is the quotient ring of $\mathbb{Z}$ by the ideal $I = n\mathbb{Z}$.

Non-example 27.9. $\mathbb{Z} \subset \mathbb{Q}$ is a subgroup, and a subring in fact, but it is definitely not an ideal. This is because if x is an integer and r is a rational number, rx need not be an integer. In fact, subrings are usually not ideals.

3. Examples of ideals and quotient rings

Definition 27.10. Let $x \in R$ be an element of a commutative ring. Then *ideal generated by* x is the subset of all elements of the form rx for some $r \in R$. We write (x) for this ideal.

Exercise 27.11. Prove this is an ideal.

Answer: Let $I = (x)$. I is closed under addition because $rx + sx = (r+s)x \in I$. It contains the additive identity since $0x = 0$. It contains inverses because $-(rx) = (-r)x$. So I is a subgroup under addition. Finally, if $s \in R$ and $rx \in I$, we have that $s(rx) = (sr)x \in I$.

Example 27.12. Let $R = \mathbb{R}[t]$ be the ring of polynomials in one variable t. Consider the ideal I generated by the polynomial $t^2 + 1$. So

$$I = \{f(t) \text{ such that } f(t) = g(t)(t^2+1) \text{ for some polynomial } g(t) \in \mathbb{R}[t].\}$$

Then what is the ring R/I?

Proposition 27.13. The ring $\mathbb{R}[t]/(t^2+1)$ is isomorphic to $\mathbb{C}$.

Chit-chat 27.14. How cool is that?

Chit-chat 27.15. In general, when you have a ring R and you quotient out its polynomial ring by some equation, you "add on" an element to R that satisfies that polynomial equation. This is the beginnings of Galois Theory, and you can learn more about it if you take Barry Mazur's class next semester.

4. Fields

Definition 27.16. A commutative ring is called a *field* if $R - \{0\}$ is a group under multiplication.

Example 27.17. $\mathbb{R}, \mathbb{Q}, \mathbb{C}$, since every non-zero element has a multiplicative inverse.

Non-example 27.18. $\mathbb{Z}$, since any integer that's not ± 1 does not admit a multiplicative inverse.

Chit-chat 27.19. More on these in coming weeks, for sure!