Lecture 26: Rings

We're going to move on from groups, though your homework will still develop new ideas about groups.

1. Definition of rings

Definition 26.1. Recall that a *monoid* is a group without inverses. That is, a monoid is a set M together with a function

$$\cdot : M \times M \to M$$

which has a unit, and which is associative. We say a monoid is *commutative* if $ab = ba$ for all $a, b \in M$.

Definition 26.2. An *associative ring* is a triple $(R, +, \cdot)$ where R is a set, and

1. $+ : R \times R \to R$ is a function making $(R, +)$ into an abelian group. We call this operation *addition*, and we call its identity element 0.
2. $\cdot : R \times R \to R$ is a function making R into a monoid. We call the $\cdot$ operation *multiplication*, and we denote the unit by 1.
3. Finally, we demand that multiplication distributes over addition: This means that for all $a, b, c \in R$, we have
$$a(b+c) = ab + ac \qquad \text{and} \qquad (b+c)a = ba + ca.$$
where we have written $a \cdot b$ as ab.

We will often simply write R for a ring, leaving the operations $+$ and $\cdot$ implicit.

Definition 26.3. If $(R, \cdot)$ is an abelian monoid, we call R a *commutative* ring.

When we dealt with groups, I proved the cancellation law right away because it was a useful thing to know. Here's another useful thing to know:

Proposition 26.4. Let R be an associative ring, and let 0 be the additive identity for R. Then

$$0 \cdot a = a \cdot 0 = 0$$

for all $a \in R$.

Proof.

$$\begin{aligned} 0 \cdot a &= (0+0) \cdot a && \text{(Since } 0+0=0\text{)} \\ &= 0 \cdot a + 0 \cdot a && \text{(Distributivity)} \end{aligned}$$

By the cancellation law for abelian groups, we can subtract $0 \cdot a$ from both sides of this equation. We are left with $0 = 0 \cdot a$. I leave it to you to prove, analogously, that $a \cdot 0 = 0$. □

Remark 26.5. We won't get to see why in depth, but rings have incredibly different behaviors based on whether they are commutative or not.

2. First examples of commutative rings

Example 26.6. Consider the triple $(\mathbb{Z}, +, \cdot)$. This makes $(\mathbb{Z}, +)$ into an abelian group, and $(\mathbb{Z}, \cdot)$ is certainly a monoid—multiplication has a unit called 1, and it's associative. Distributivity is the usual notion of distributivity you're used to.

Example 26.7. The triple $(\mathbb{Q}, +, \cdot)$ with the usual addition and multiplication is a ring. Likewise for $\mathbb{R}$ and $\mathbb{C}$ with their usual notions of multiplication. These are special kinds of rings, because any element of $R - \{0\}$ has an inverse under multiplication. We'll talk more about the consequences of this later.

Example 26.8 (Polynomial rings)**.** Let $\mathbb{Z}[x]$ denote the set of polynomials in x with integer coefficients. So an element is an expression

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n = \sum_{i=0}^{\infty} a_i x^i$$

where $a_i = 0$ for all i bigger than some finite n. For example, the following are elements in $\mathbb{Z}[x]$:

$$0, \qquad 5, \qquad 3 + x - 5x^4, \qquad x.$$

In the third example, we have $a_0 = 3, a_1 = 1, a_2 = 0, a_3 = 0, a_4 = -5$.

Let $q(x)$ be a polynomial with coefficients b_i. Addition of polynomials is defined as follows:

$$p(x) + q(x) := \sum_{i=0}^{\infty} (a_i + b_i) x^i.$$

Note that since $a_i = 0$ for i bigger than n, and $b_i = 0$ for all i bigger than some m, the sum is indeed a polynomial, as $(a_i + b_i) = 0$ for all i bigger than $\max(m, n)$.

And the product of two polynomials is defined in the usual way:

$$\begin{aligned} p(x) \cdot q(x) &= (a_0 + a_1 x + \dots a_n x^n)(b_0 + b_1 x + \dots b_m x^m) \\ &= a_0 b_0 + (a_1 b_0 + a_0 b_1)x + \dots + a_n b_m x^{n+m} \\ &= \sum_{k \geq 0} (\sum_{i+j=k} a_i b_j) x^k. \end{aligned}$$

Proposition 26.9. $\mathbb{Z}[x]$ is a commutative ring. More generally, if R is a commutative ring, the set of polynomials with coefficients in R, $R[x]$, is a commutative ring.

Proof. You will prove this for homework. □

Example 26.10 (Smooth functions)**.** Here's an example where it's much harder to write down all the elements of the set. Let $C^\infty(\mathbb{R}^n)$ denote the set of all infinitely differentiable functions $f : \mathbb{R}^n \to \mathbb{R}$. Given two functions f and g, we define their sum $f+g$ to be a function that sends $x \in \mathbb{R}^n$ to $f(x)+g(x)$, where this addition takes place in $\mathbb{R}$. Their product fg is the function that sends $x \in \mathbb{R}^n$ to $f(x) \cdot g(x) \in \mathbb{R}$. This is again a ring.

3. The rings $\mathbb{Z}/n\mathbb{Z}$

Chit-chat 26.11. So far, we've seen three examples of rings that we're used to. They've all been infinite. Let's see some finite examples.

Lemma 26.12. Let $\mathbb{Z}/n\mathbb{Z}$ be the set of integers modulo n. The function

$$\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \qquad \overline{a} \cdot \overline{b} := \overline{a \cdot b}$$

is well-defined.

Remark 26.13. We are denoting the equivalence class associated to $a \in \mathbb{Z}$ by $\overline{a}$. Here, $a \cdot b$ is the usual multiplication of integers, and $\overline{a \cdot b}$ denotes its equivalence class mod n.

Proof. We need to show that if $\overline{a} = \overline{a}'$ and $\overline{b} = \overline{b}'$, then

$$\overline{a \cdot b} = \overline{a' \cdot b'}.$$

Well, $a = a'$ modulo n if and only if $a = a' + An$ for some integer A. Likewise, we have that $b = b' + Bn$ for some B. Then

$$ab = (a' + An)(b' + Bn) = a'b' + (a'B + Ab' + AB)n$$

so ab equals $a'b'$ modulo n. □

Corollary 26.14. Let $+$ be the usual addition on $\mathbb{Z}/n\mathbb{Z}$, and let $\cdot$ be the operation above. Then:

1. $(\mathbb{Z}/n\mathbb{Z}, +)$ is an abelian group with unit $\overline{0}$.
2. $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is an abelian monoid with unit $\overline{1}$.
3. The operation $\cdot$ distributes over $+$.

Proof. (1) is something we proved a long time ago.

(2) To prove associativity, note that

$$\begin{aligned}(\overline{a}\cdot\overline{b})\cdot\overline{c} &= \overline{a\cdot b}\cdot\overline{c}\\ &= \overline{(a\cdot b)\cdot c}\\ &= \overline{a\cdot(b\cdot c)} \qquad (1)\\ &= \overline{a}\cdot\overline{b\cdot c}\\ &= \overline{a}\cdot(\overline{b}\cdot\overline{c}).\end{aligned}$$

Every line is by the definition of $\cdot$, except for (1) which uses associativity of multiplication for the integers. Commutativity holds because

$$\overline{a}\cdot\overline{b} = \overline{a\cdot b} = \overline{b\cdot a} = \overline{b}\cdot\overline{a}.$$

Note the middle equality is just commutativity for multiplication for the integers. The unit is 1 because $\overline{a}\cdot\overline{1} = \overline{a\cdot 1} = \overline{a}$.

(3) Distributivity holds because

$$\begin{aligned}\overline{a}\cdot(\overline{b}+\overline{c}) &= \overline{a}\cdot\overline{b+c}\\ &= \overline{a\cdot(b+c)}\\ &= \overline{ab+ac} \qquad (2)\\ &= \overline{ab}+\overline{ac}\\ &= \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}.\end{aligned}$$

Again, every line is by definition, except (2) uses distributivity for the usual integers.

□

4. Motivation for commutative rings

There is now a philosophy in modern math that properties of spaces can be discerned from properties of their set of functions. For instance, by studying the set of polynomial functions on a space X, one can discern properties about the space X itself. And in fact, every set of functions is always a commutative ring. It is the properties of these *rings* that determine certain properties of the *space* X. This is by no means obvious, and some of the most meaningful developments in this direction have only come since the late 1880's—that is, nearly two hundred years after Descartes first noticed that algebraic equations can describe concrete geometry. So if you consider that algebra (from the so-called Golden Age of Islam in the 800's-plus) and geometry (from the Greeks) took nearly a thousand years for Descartes to synthesize, and it took us an even two hundred more years to develop a systematic way to understand that rings are a powerful way to study geometry, you might realize you're setting foot on some pretty rad ideas. We won't be able to even begin to penetrate this narrative—of using rings to study geometry—but if you're interested, you can do some reading on commutative algebra and algebraic geometry.

5. First examples of non-commutative rings

Example 26.15 (Matrix rings)**.** Fix an integer $n \geq 0$ and consider the set $M_{n\times n}(\mathbb{R})$ of all $n \times n$ matrices with entries in $\mathbb{R}$. You can add and multiply matrices, and multiplication of matrices distributes over addition. Hence $M_{n\times n}(\mathbb{R})$ is a ring. To see distributivity explicitly, consider three matrices A, B, C with entries a_{ij}, b_{ij}, c_{ij}. Then the ijth entry of $A(B + C)$ is given by

$$\sum_{k=1}^{n} a_{ik}(b_{kj} + c_{kj}) = \sum_{k=1}^{n} a_{ik}b_{kj} + \sum_{k=1}^{n} a_{ik}c_{kj}$$

but this righthand side is the ijth entry of $AB + AC$. You can likewise show $(B + C)A = BA + CA$.

Example 26.16 (Group rings)**.** Let G be a finite group, and let R be a commutative ring. Then $R[G]$ as a set is the set of all functions from G to R. (So every element $g \in G$ is associated an element $r_g \in R$.) We write such a function as the summation

$$\sum_{g\in G} r_g g.$$

As an example, here is an example of an element of $\mathbb{Z}[S_3]$:

$$5() + 3(12) - 8(123).$$

Addition is the obvious addition—we just add component-wise, so

$$(\sum r_g g) + \sum(s_g g) = \sum_{g\in G}(r_g + s_g)g.$$

I.e., this is just the addition of functions. Multiplication is *not* just multiplication of functions. The product of $\sum r_g g$ and $\sum s_g g$ has the coefficient of g given by

$$\sum_{(g_1,g_2) s.t. g_1g_2=g} r_{g_1}s_{g_2}.$$

Put another way,

$$(\sum_{g\in G} r_g g)(\sum_{h\in G} s_h h) = \sum_{g\in G}\sum_{h\in H} r_g s_h (gh) = \sum_{k\in G}(\sum_{(g,h) s.t. gh=k} r_g s_h)k.$$

Note that this multiplication is not commutative.