Algebra Notes

Sept. 14: Definition and Examples of Rings

Geoffrey Scott

Rings: Motivation and Definition

Throughout your education, you've encountered many different mathematical objects that can be "added" and "multiplied":

Integers, rationals, real numbers: You learned what it meant to "add" and "multiply" numbers in primary school.

Polynomials: You learned what it meant to "add" and "multiply" polynomials with real coefficients in high school

Square matricies: You learned to "add" square matrices by adding the corresponding terms of the matrices, and to "multiply" square matrices by the matrix multiplication algorithm.

Functions: You "add" functions by constructing a new function whose output values are the sum (as numbers) of the output values of the original functions, and you "multiply" functions by constructing a new function whose output values are the product (as numbers) of the output values of the original functions.

If you were an apt student, you might have complained to your teachers that the terms "add" and "multiply" are really overloaded! Why use the same two words to describe such different operations on such different kinds of mathematical objects?

One reason is that there are properties of these "adding" and "multiplying" operations that are true in all of these examples – properties such as $a+b = b+a$ and $a(bc) = (ab)c$ and $a(b+c) = ab + ac$ and $(b + c)a = ba + ca$. In this way, the process of "adding" and "multiplying" square matrices (or polynomials, or functions) *behaves like* the process of "adding" and "multiplying" numbers. As you learn more mathematics, you will encounter *even more* mathematical objects that have "addition" and "multiplication" operations with these properties, so mathematicians have decided to give a name to these objects: a *ring*.

Definition: A **ring** is a set R with two operations, called *addition* (written $a+b$) and *multiplication* (written $a * b$ or $a \cdot b$ or ab) such that

- $(R, +)$ is an abelian group. In case you forget, this means:
  - Addition is associative: $a + (b + c) = (a + b) + c$
  - There is an identity element 0, with $0 + a = a + 0 = a$ for all a.
  - Every element has an inverse $a + (-a) = 0$.
  - Addition is commutative: $a + b = b + a$.
- Multiplication is associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Multiplication distributes over addition:

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (b + c) \cdot a = b \cdot a + c \cdot a$$

Notation: We often write "0" for the additive identity of a ring. For any ring element r and natural number n, then expression r^n means r multiplied by itself n times.

Examples of Rings

We've seen some examples of rings above.

Example 0: The integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the polynomials with real coefficients $\mathbb{R}[x]$, the $n \times n$ matrices of integers $M_n(\mathbb{Z})$, the continuous functions on the real line $C(\mathbb{R})$. In each case, the addition and multiplication operations are the ones you learned in grade school.

We can also invent new rings by taking abelian groups we know from group theory, and inventing a multiplication rule that satisfies the ring axioms.

Example 1: Recall that the elements of the abelian group $\mathbb{Z}_4 (= \mathbb{Z}/4\mathbb{Z})$ are the cosets

$$[0] = \{4k \mid k \in \mathbb{Z}\} \qquad [1] = \{1 + 4k \mid k \in \mathbb{Z}\}$$
$$[2] = \{2 + 4k \mid k \in \mathbb{Z}\} \qquad [3] = \{3 + 4k \mid k \in \mathbb{Z}\}.$$

We can define a multiplication operation on $\mathbb{Z}_4$ according to the table below.

$*$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

In fact, we can make any of the abelian groups $\mathbb{Z}/n\mathbb{Z}$ into a ring by defining multiplication as $[a][b] = [ab]$.

Example 2: For any real number n, the abelian group $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ is a ring under the standard multiplication of numbers. When n is an integer, $n\mathbb{Z}$ is a subset of $\mathbb{Z}$ which is closed under addition, multiplication, and taking additive inverses. In other words, $n\mathbb{Z}$ is a subset of the ring $\mathbb{Z}$ which is itself a ring.

Definition: A nonempty subset $S \subseteq R$ of a ring which is closed under the addition and multiplication operations, as well as taking additive inverses, is called a **subring** of R.

Constructing New Rings from Old Ones

Construction 1: For *any* ring R, we can consider the polynomials with coefficients in R, written $R[x]$. Examples of the rules for addition and multiplication are below. Each r_i and r_i' is an element of R.

$$(r_2x^2 + r_1x + r_0) + (r_2'x^2 + r_1'x + r_0') = (r_2 + r_2')x^2 + (r_1 + r_1')x + (r_0 + r_0')$$
$$(r_2x^2 + r_1x + r_0) \cdot (r_2'x^2 + r_1'x + r_0') = (r_2r_2')x^4 + (r_2r_1' + r_1r_2')x^3 + (r_2r_0' + r_1r_1' + r_0r_2')x^2 + (r_1r_0' + r_0r_1')x + (r_0r_0')$$

Construction 2: If R and S are two rings, the **product** $R \times S$ is the ring whose elements are pairs (r, s), where $r \in R$ and $s \in S$, and the operations are defined as follows.

$$(r, s) + (r', s') = (r + r', s + s')$$
$$(r, s) \cdot (r', s') = (r \cdot r', s \cdot s')$$

Construction 3: If R is any ring, we can consider the ring of $n \times n$ matrices with entries in R, written $M_n(R)$. The addition and multiplication rules for square matrices is the same as the one you learned in grade school.

Construction 4: For certain rings R, we can construct a new ring whose elements behave like fractions of elements of R, generalizing the way in which elements of $\mathbb{Q}$ are fractions of elements of $\mathbb{Z}$. We'll learn this construction next lecture.

WARNINGS

Although we can think of rings as "mathematical objects that you can add and multiply, sort of like numbers," there are some properties of numbers that are *not* true in all rings.

Warning 0: Not all rings have an element 1 that satisfies the condition $1a = a1 = a$ for all ring elements a, but the most commonly encountered rings in mathematics do. Some (misguided) people include the requirement "1 exists" in the *definition* of a ring.

> **Definition:** An element 1 of a ring R that satisfies $1a = a1 = a$ for all $a \in R$ is called a **multiplicative identity** of R. A ring with a multiplicative identity element 1 is called a **ring with unity** or **ring with identity**.

If a multiplicative identity exists, it must be unique. To see this, suppose 1_a and 1_b are both multiplicative identities. Then $1_a 1_b = 1_b$ and $1_a 1_b = 1_a$, so $1_b = 1_a$.

Warning 1: Sometimes, $ab \neq ba$. For example, try taking two elements a and b in the ring of 2 by 2 matrices of integers and calculating ab and ba. Unless you got very lucky when you chose a and b, you will find that $ab \neq ba$. There is a special name given to a ring for which $ab = ba$ is true for *all* elements a and b.

> **Definition:** A ring R is **commutative** if for all $a, b \in R$, $ab = ba$.

Warning 2: You can't "divide" in rings. In the ring of real numbers, the expression $\frac{a}{b}$ is shorthand for ab^{-1}, and the symbol b^{-1} means the *multiplicative inverse* of b (i.e. the real number such that $b^{-1} \cdot b = b \cdot b^{-1} = 1$). In an arbitrary ring R, not all elements have multiplicative inverses. First, it's possible that a ring doesn't even contain a multiplicative identity (so the concept of a "multiplicative inverse" doesn't even make sense). Even if a ring contains 1, some elements won't have a multiplicative inverse. Elements that do are called *units*.

> **Definition:** For $a \in R$, an element $b \in R$ is called a **multiplicative inverse** of a if $ab = ba = 1$. If a has a multiplicative inverse, it is called **invertible** or **a unit**. If every nonzero element of R is a unit then R is called a **division ring**. A commutative division ring is called a **field**.

Warning 3: For elements a, b in a ring R, sometimes $ab = 0$ even when a and b are both nonzero. For example, $[2] \cdot [3] = 0$ in $\mathbb{Z}/6\mathbb{Z}$.

Definition: If a and b are nonzero elements of R such that $ab = 0$ or $ba = 0$, then a and b are called **zero divisors**. A commutative ring R with identity is called an **integral domain** if it has no zero divisors.

For these reasons, you have to be very careful when you're proving things about rings, because you might get tempted to use properties that *feel true* but aren't. On the other hand, there are some properties of rings that feel true and *are* true. I've proved one of them below.

Proposition: Let R be a ring. For any $a \in R$, $0a = a0 = 0$

Proof: Because 0 is an additive identity, $0 + 0 = 0$. Combining this with the distributive property gives

$$0a = (0 + 0)a = 0a + 0a.$$

Adding (-0a) to both sides of the equation proves $0 = 0a$. The proof that $a0 = 0$ is similar.

Proposition: Let R be a ring with identity. If b_1 and b_2 are both multiplicative inverses of a, then $b_1 = b_2$.

Proof: Observe that $b_1ab_2 = b_11 = b_1$, and also $b_1ab_2 = 1b_2 = b_2$. Therefore, $b_1 = b_2$

Summary of Today's Vocab

Commutative ring: A ring R is *commutative* if $ab = ba$ for all $a, b \in R$.

Division ring: A ring R with identity is a *divison ring* if every nonzero element is a unit.

Field: A commutative ring R with identity is called a *field* if every nonzero element is a unit.

Identity: An element a of a ring is *the identity* or *one* if $ab = ba = b$ for all $b \in R$. Note: if it exists, it is unique.

Integral domain: A commutative ring R with identity is called an *integral domain* if it has no zero divisors.

Unit: An element a of a ring with identity is a *unit* if there is some $b \in R$ for which $ab = ba = 1$.

Zero: The additive inverse of a ring is called *zero*. Note: it is unique.

Zero divisor: An element $a \neq 0$ of a ring R is a *zero divisor* if there is $b \neq 0$ such that $ab = 0$ or $ba = 0$.