7-29-2022

Rings

Definition. A **ring** is an abelian group R with binary operation $+$ ("addition"), together with a second binary operation $\cdot$ ("multiplication"). The operations satisfy the following axioms:

1. Multiplication is **associative**: For all $a, b, c \in R$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

2. The **Distributive Law** holds: For all $a, b, c \in R$,

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

Remark. 1. To say that R is an abelian group under addition means that the following axioms hold:

(a) (Associativity) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.

(b) (Identity) There is an element $0 \in R$ such that $a + 0 = a$ and $0 + a = a$ for all $a \in R$.

(c) (Inverses) For all $a \in R$, there is an element $-a \in R$ such that $a + (-a) = 0$ and $(-a) + a = 0$.

(d) (Commutativity) $a + b = b + a$ for all $a, b \in R$.

Definition. A ring R has a **multiplicative identity** if there is an element $1 \in R$ such that $1 \neq 0$, and such that for all $a \in R$,

$$1 \cdot a = a \quad \text{and} \quad a \cdot 1 = a.$$

A ring satisfying this axiom is called a **ring with** 1, or a **ring with identity**.

Note that in the term "ring with identity", the word "identity" refers to a *multiplicative* identity. Every ring has an additive identity ("0") by definition.

Remark. I'll often suppress the multiplication symbol and simply write "ab" for "$a \cdot b$". As usual, a^2 means $a \cdot a$, a^3 means $a \cdot a \cdot a$, and so on.

However, note that *negative powers* of elements are not always defined: An element in a ring might not have a multiplicative inverse. This means that you don't always have "division"; you do have "subtraction", since that's the same as adding the additive inverse.

Many elementary algebraic operations work the way you'd expect. (There will be some surprises later, however.)

Proposition. Let R be a ring.

(a) If $r \in R$, then $r \cdot 0 = 0 = 0 \cdot r$.

(b) Let $r \in R$, and let $-r$ denote the additive inverse of r. If R is a ring with identity, then $(-1) \cdot r = -r$.

(c) Let $r, s \in R$. Then $(-r) \cdot s = -(rs) = r \cdot (-s)$.

Proof. (a) Let $r \in R$. Note that

$$r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0.$$

Therefore $0 = r \cdot 0$. □

(b) Suppose R is a ring with identity, and let $r \in R$. Then

$$(-1) \cdot r + r = (-1) \cdot r + 1 \cdot r = (-1 + 1) \cdot r = 0 \cdot r = 0.$$

Therefore, $(-1) \cdot r$ is the additive inverse of r, i.e. $(-1) \cdot r = -r$. □

(c) The proof is similar to the proof of (b). □

Notation. If R is a ring and n is a positive integer, nr is short for $r + r + \cdots r$ (n summands). Likewise, if n is a negative integer, nr is $(-n)r$. (This is the usual convention for an abelian group.)

Notice that, for example, $13 \cdot 1 \in \mathbb{Z}_6$ makes sense according to this convention: It is 1 added to itself 13 times. However, you should not write "$13 \in \mathbb{Z}_6$", since 13 is *not* an element of $\mathbb{Z}_6$. □

Definition. If R is a ring and $ab = ba$ for all $a, b \in R$, R is a **commutative ring**.

Note that the adjective "commutative" applies to the multiplication operation; the addition operation is *always* commutative by definition.

Example. Which of the following sets are rings under the usual operations? Are they commutative? Do they have an identity element?

$$\mathbb{Z}, \quad 2\mathbb{Z}, \quad \mathbb{Q}, \quad \mathbb{Q}^+, \quad \mathbb{R}, \quad \mathbb{C}.$$

$\mathbb{Z}$ is a commutative ring with identity.

$2\mathbb{Z}$ is a commutative ring, but it does not have an identity.

$\mathbb{Q}$ is a commutative ring with identity.

$\mathbb{Q}^+$, the set of positive rationals, is not a ring. It does not contain an identity for addition.

$\mathbb{R}$ is a commutative ring with identity.

$\mathbb{C}$ is a commutative ring with identity. □

The ring of quaternions.

The ring of quaternions is the set

$$\mathbb{H} = \{w + xi + yj + zk \mid w, x, y, z \in \mathbb{R}\}.$$

The "H" honors William Rowan Hamilton, who discovered the quaternions in the 1840's.

You add elements in the obvious way, e.g.

$$(2 + 4i - 9j + 11k) + (13 - i + 5j + 17k) = 15 + 3i - 4j + 28k.$$

Multiply elements using the following multiplication table:

$\times$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

(This is the multiplication table for the group of the quaternions Q; in $\mathbb{H}$, 1, i, j, and k can be multiplied by real numbers as if they were vectors. In fact, ignoring the multiplication, $\mathbb{H}$ is just a 4-dimensional vector space over $\mathbb{R}$.)

For example,

$$(3i - 2k) \cdot (3 + 2j) = 15i.$$

$\mathbb{H}$ is a noncommutative ring, since (e.g.) $ij = k$ but $ji = -k$. In fact, Hamilton apparently was stuck on this point for many years. He knew that complex numbers could be used to represent rotations in two dimensions, and he was trying to construct an algebraic system for representing rotations in three dimensions. The problem is that rotations in three dimensions don't commute, whereas he expected his algebraic system to have a commutative multiplication — as did all the number systems known up to that time.

Verifying the other ring axioms is routine, but very tedious! We'll add $\mathbb{H}$ to our collection of common number systems, along with the integers, the rationals, the real numbers, and the complex numbers.

Example. (**The integers mod n as rings**) Construct a multiplication table for $\mathbb{Z}_3$. What kind of ring is it?

*	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

For example, $2 \cdot 2 = 1$, since as integers $2 \cdot 2 = 4$, and 4 reduces to 1 mod 3.
With these operations, $\mathbb{Z}_3$ becomes a commutative ring with 1.
In general, $\mathbb{Z}_n$ is a commutative ring with 1. □

Example. (**A ring without an identity**) Prove that the set of even integers $2\mathbb{Z}$ with the usual operations is a ring without an identity.

Suppose that $e \in 2\mathbb{Z}$ is an identity. Then $e = 2n$ for some $n \in \mathbb{Z}$. Since e is an identity, I must have (for instance)

$$\begin{aligned} e \cdot 6 &= 6 \\ 2n \cdot 6 &= 6 \\ 2n &= 1 \end{aligned}$$

Since there is no integer n for which this is true, $2\mathbb{Z}$ cannot have an identity. □

Example. (**A ring of matrices**) $M(2, \mathbb{R})$ is the set of 2×2 matrices with real entries. The operations are the usual matrix addition and multiplication. The additive identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$; the multiplicative identity is $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Show by example that $M(2, \mathbb{R})$ is a noncommutative ring.

$$\begin{bmatrix} 1 & 2 \\ 3 & -1 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 4 & 1 \end{bmatrix} = \begin{bmatrix} 10 & 3 \\ 2 & 2 \end{bmatrix}, \quad \text{but} \quad \begin{bmatrix} 2 & 1 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} 1 & 2 \\ 3 & -1 \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 7 & 7 \end{bmatrix}. \quad \square$$

Example. (**A ring of functions**) $C[0, 1]$ is the set of continuous functions $f : [0, 1] \to \mathbb{R}$. Operations are pointwise addition and multiplication:

$$(f + g)(x) = f(x) + g(x) \quad \text{and} \quad (fg)(x) = f(x)g(x).$$

Is $C[0,1]$ a commututative ring? What are the additive and multiplicative identities?

$C[0,1]$ is a commutative ring, since by commutativity of real number multiplication,

$$(fg)(x) = f(x)g(x) = g(x)f(x) = (gf)(x).$$

The constant functions 0 and 1 are the additive and multiplicative identities, respectively. □

Polynomial rings.

Let R be a commutative ring. $R[x]$ denotes the **ring of polynomials** in one variable with coefficients in R. Add and multiply polynomials as usual.

For example, $\mathbb{R}[x]$ consists of all polynomials with real coefficients: things like

$$x + 2, \quad 3 - 7x^2 + 54x^{17}, \quad 42, \ldots.$$

The formal, precise way to define $R[x]$ is to define it to be the collection of finite ordered n-tuples

$$\{(r_0, r_1, \ldots, r_n) \mid n \geq 0, r_i \in R\}.$$

(That is, a polynomial is the "vector" of its coefficients.) Now you can define addition and multiplication by writing down some ugly, unenlightening formulas. The point of mentioning this is to show that we're not doing something invalid by thinking of polynomials as "formal sums in powers of x" — you could do things in a perfectly rigorous way if you chose.

Note that polynomials are not *functions* in this context. For example, let $R = \mathbb{Z}_2$ and look at $f(x) = x^2 + x$. This is *not* zero *as a polynomial*, even though $f(0) = 0$ and $f(1) = 0$; i.e., even though *it vanishes on every element of the ring.* □
