

Rings

Definition 1 (Ring). A ring is a set R equipped with two operations $+$ and \cdot , which satisfy the following properties.

- A1. $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.
- A2. There is an element $0_R \in R$ (called a zero) such that $a + 0_R = 0_R + a = a$ for all $a \in R$.
- A3. For every $a \in R$ there is an element $-a \in R$ (called a negative of a) such that $a + (-a) = (-a) + a = 0_R$.
- A4. $a + b = b + a$ for all $a, b \in R$.
- M. $(ab)c = a(bc)$ for all $a, b, c \in R$.
- D. $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$ for all $a, b, c \in R$.

Proposition 1. Let R be a ring.

- 1. The zero element of R is unique in the following sense: if $a, b \in R$ such that $a + b = a$, then $b = 0_R$.
- 2. Negative elements in R are unique in the following sense: If $a, b \in R$ such that $a + b = 0_R$, then $b = -a$.
- 3. $-(-a) = a$ for all $a \in R$.
- 4. $0_R \cdot a = a \cdot 0_R = 0_R$ for all $a \in R$.
- 5. $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$.
- 6. $(-a)(-b) = ab$ for all $a, b \in R$.

Proof.

- 1. Suppose $a + b = a$. Now $-a + (a + b) = -a + a$, and by A1 $(-a + a) + b = -a + a$. By A3 we have $0_R + b = 0_R$, and by A2 we have $b = 0_R$.
- 2. Suppose $a + b = 0_R$. Now $-a + (a + b) = -a + 0_R$, and by A1 we have $(-a + a) + b = -a + 0_R$. By A3 we have $0_R + b = -a + 0_R$, and using A2 (twice) we have $b = -a$.
- 3. By definition, $(-a) + a = 0_R$, so by the uniqueness of negatives we have $a = -(-a)$.
- 4. Let $a \in R$. Now $a \cdot a + 0_R \cdot a = (a + 0_R) \cdot a = a \cdot a$, and so $0_R \cdot a = 0_R$. The other equality is similar.
- 5. Let $a, b \in R$. Now $(-a)b + ab = (-a + a)b = 0_R \cdot b = 0_R$, so that $(-a)b = -(ab)$. The other equality is similar.
- 6. Using the previous statement, we have $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$.

□

Examples

$\mathbb{Z}, \mathbb{Z}/(n)$ The integers are a ring by definition, and we showed that the integers mod n are a ring for any $n > 0$.

\mathbb{Q} The rational numbers are a ring under the usual addition and multiplication; we will prove this later. (Actually we will define the rational numbers.)

\mathbb{R}, \mathbb{C} The real and complex numbers are also rings, although even defining these sets of “numbers” is beyond the scope of this text.

0 The smallest possible ring must have at least one element, the zero. Suppose this is *all* we have. Now the arithmetic is pretty boring: $0 + 0 = 0$ and $0 \cdot 0 = 0$. It is straightforward to check that these operations make the set $\{0\}$ into a ring. This example isn’t very interesting, so we call this the *trivial ring* or the *zero ring*.

R^A Let R be a ring, and let A be any nonempty set. Then the set

$$R^A = \{\varphi \mid \varphi : A \rightarrow R\}$$

is a ring under the “pointwise” operations

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x) \quad \text{and} \quad (\alpha\beta)(x) = \alpha(x)\beta(x).$$

$\text{Mat}_2(R)$ Let R be a ring, and consider the set

$$\text{Mat}_2(R) = \left\{ \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \mid a_{11}, a_{12}, a_{21}, a_{22} \in R \right\}.$$

These are just the 2×2 matrices with entries in R . The usual matrix addition and multiplication make $\text{Mat}_2(R)$ into a ring. Specifically, we define

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} + \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{bmatrix}$$

and

$$\begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix} \cdot \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix} = \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix}.$$

$2\mathbb{Z}$ Consider the set

$$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}.$$

It is not too difficult to show that this set is a ring under the usual addition and multiplication of integers.

2^X Let X be any nonempty set. The powerset 2^X is a ring under the operations $A + B = (A \setminus B) \cup (B \setminus A)$ and $A \cdot B = A \cap B$. This is called a *ring of sets*.

Commutative and Unital Rings

Our list of examples is starting to get complicated, so we make two additional definitions to start drawing distinctions among them.

Definition 2. *Let R be a ring.*

- *We say that R is commutative if it satisfies the following additional property.*

C. $ab = ba$ for all $a, b \in R$.

- *We say that R is unital if it satisfies the following additional property.*

U. There is an element $1 \in R$ (called a one) such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

Proposition 2. *Let R be a unital ring.*

1. *The one element of R is unique in the following sense: if $u \in R$ such that $u \cdot a = a$ for all $a \in R$, then $u = 1$.*
2. *$-a = (-1) \cdot a$ for all $a \in R$.*

Proof. 1. Suppose u is such an element. In particular, $1 = u \cdot 1 = u$.

2. Let $a \in R$. Then $a + (-1)a = 1a + (-1)a = (1 + (-1))a = 0a = 0$, so that $(-1)a = -a$.

□