Definition of a ring

A *ring* R is a set, with elements $0, 1 \in R$, together with two binary operations $+$ (addition) and $\times$ (multiplication, often written $\cdot$ or omitted) such that the following properties hold:

(Associativity for $+$)	$a + (b + c) = (a + b) + c$
(Associativity for $\times$)	$a(bc) = (ab)c$
(Identity for $+$)	$a + 0 = 0 + a = a$
(Identity for $\times$)	$1 \cdot a = a \cdot 1 = a$
(Inverses for $+$)	$a + (-a) = (-a) + a = 0$
(Distributivity)	$a(b + c) = ab + ac, \quad (a + b)c = ac + bc$
(Commutativity for $+$)	$a + b = b + a$

These properties are for all $a, b, c \in R$. The "Inverses for $+$" property should be understood as: for each $a \in R$, there is an element called $-a \in R$ such that $a + (-a) = (-a) + a = 0$. A ring is *commutative* if $ab = ba$ for all $a, b \in R$.

Examples of rings include $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{Z}_n$, all with the usual operations of addition and multiplication. Note these are all *commutative* rings.

A "shorter" definition of a ring is as follows: a ring R is a set with binary operations $+$ and $\times$ such that $(R, +)$ is an abelian group with identity $0 \in R$; and $\times$ is associative and has an identity $1 \in R$; and the distributivity properties hold.

We remark that the axiom that "+" is commutative is implied by the other axioms. To see this we compute $(1 + 1)(a + b)$ in two different ways:

$$(1 + 1)(a + b) = 1(a + b) + 1(a + b) = a + b + a + b$$

$$(1 + 1)(a + b) = (1 + 1)a + (1 + 1)b = a + a + b + b$$

We have used distributivity and also that 1 is a multiplicative identity. Then we can add $-a$ to the left sides and $-b$ to the right sides of these equations to get $b + a = a + b$.

▶ **Let R be a ring and $a, b \in R$. Then:**

(i) $a0 = 0a = 0$

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

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

Proof. To prove (i), we compute $a0 = a(0 - 0) = a0 - a0 = 0$, and similarly $0a = 0$. For (ii), use distributivity: $ab + a(-b) = a(b + (-b)) = a0 = 0$; this implies $a(-b) = -ab$. Similarly $(-a)b = -ab$. Finally, for (iii): from (ii), $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$. □

▶ **Suppose $0 = 1$ in a ring R. Then $R = \{0\}$.**

To see this, we compute for any $a \in R$: $a = a1 = a0 = 0$. Thus every element in R is equal to 0, and this proves the claim. We call $R = \{0\}$, with the operations $+$ and $\times$ defined in the only possible way, the *zero ring*.

For a ring $R \neq \{0\}$, $(R, \times)$ is *not* a group. To see this, note that $R \neq \{0\}$ implies $0 \neq 1$. Then $a0 = 0$ for all $a \in R$. Thus there is no $a \in R$ such that $a0 = 1$. This means 0 does not have a multiplicative inverse. So $(R, \times)$ is not a group.

▶ **Let R be a ring. We make the following definitions:**

(i) $a \in R$ **is a *unit* if there is a** $b \in R$ **such that** $ab = 1$**. We write** $b = a^{-1}$**.**

(ii) $a \in R$ **is a *zero divisor* if there is a non-zero** $b \in R$ **such that** $ab = 0$**.**

The following is a straightforward verification from the definitions.

▶ **Let R be a ring and define $R^\times = \{a \in R : a \text{ is a unit}\}$. Then $(R^\times, \times)$ is a group.**

Note this notation agrees with our earlier notations for $\mathbb{C}^\times$, $\mathbb{Q}^\times$, $\mathbb{R}^\times$ and $\mathbb{Z}_n^\times$.

Here is an example of a non-commutative ring. Consider the set of 2×2 real matrices:

$$\mathrm{M}_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : \ a, b, c, d \in \mathbb{R} \right\}$$

Then we define $+$ to be addition of matrices and $\times$ to be multiplication of matrices. Then, not surprisingly, $\mathrm{M}_2(\mathbb{R})$ is a ring with additive and multiplicative identities given by:

$$\text{“}0\text{”} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{“}1\text{”} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

An example of a zero divisor in $\mathrm{M}_2(\mathbb{R})$ (which is not 0) is the following matrix:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

In fact $AA = A^2 = 0$. Finally, we note that $A \in \mathrm{M}_2(\mathbb{R})$ is a unit if and only if $A \in \mathrm{GL}_2(\mathbb{R})$. We conclude $\mathrm{M}_2(\mathbb{R})^\times = \mathrm{GL}_2(\mathbb{R})$.

▶ **Let R be a ring. We make the following definitions:**

(i) R **is an *integral domain* if it is commutative and** $ab = 0$ **implies** $a = 0$ **or** $b = 0$**.**

(ii) R **is a *division ring* if every non-zero** $a \in R$ **is a unit.**

(iii) R **is a *field* if it is a commutative division ring.**

Note a commutative ring R is an integral domain if and only if the only zero divisor in R is 0. Also, every field is an integral domain. Note also that R is a division ring if and only if the group of units $R^\times$ is exactly $R\backslash\{0\}$.

Examples of fields are $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$. The ring $\mathbb{Z}$ is an integral domain but not a division ring or a field. The ring $\mathrm{M}_2(\mathbb{R})$ is not commutative (hence not an integral domain or a field) and also not a division ring, because it has non-zero zero divisors.

Let's look at some other examples. Consider $\mathbb{Z}_3 = \{0, 1, 2\}$. Note $1 \cdot 1 = 1$ and $2 \cdot 2 = 1$. Thus $\mathbb{Z}_3$ is an integral domain, and even a field. For another example, consider $\mathbb{Z}_4$. Note that $2 \cdot 2 = 0$, so this ring has a non-zero zero divisor, and is not an integral domain.

Now consider $\mathbb{Z}_n$ for n a general positive integer $n > 1$. We know that

$$\mathbb{Z}_n^\times = \{\text{units in } \mathbb{Z}_n\} = \{a (\text{mod } n) : \gcd(a, n) = 1\}$$

The only case in which $\mathbb{Z}_n^\times = \mathbb{Z}_n\backslash\{0\}$ is when n is a prime. Thus the commutative ring $\mathbb{Z}_n$ is a field if and only if n is prime.

Furthermore, suppose n is not prime, and write $n = ab$ for some positive integers a, b less than n. Then $a, b \pmod n$ are non-zero, but $ab \equiv n \equiv 0 \pmod n$. Thus $a, b \pmod n$ are zero divisors in $\mathbb{Z}_n$. Thus $\mathbb{Z}_n$ is not even an integral domain when n is not prime. Thus:

▸ **If $n > 1$ is prime, the ring $\mathbb{Z}_n$ is a field. If n is not prime, $\mathbb{Z}_n$ has (non-zero) zero divisors and so is not an integral domain.**