# Rings

Groups have only one binary operation, but most of the algebraic structures we are familiar with have 2. e.g $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$, $n \times n$ matrices, etc. These are all rings.

**Def:** A ring $R$ is a set together w/ two binary operations $+$ (addition) and $\cdot$ (multiplication) satisfying the following:

1.) $(R, +)$ is an abelian group

2.) $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

3.) It satisfies distributivity:

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

$R$ is commutative if $\cdot$ is commutative. $R$ has an identity (or contain 1) if $\exists\ 1 \in R$ s.t. $1 \cdot a = a \cdot 1$ for all $a \in R$.

We'll usually write $ab$ rather than $a \cdot b$. The additive identity will be 0 and the additive inverse of $a$ is denoted $-a$.

If $a, b \in R$ and $ab = 1 = ba$, $b$ is a multiplicative inverse for $a$. Note that not all rings have multiplicative inverses for each elt.

**Ex:** $\mathbb{Z}$ is a ring w/ identity, but only 1 and $-1$ have

multiplicative inverses.

**Def:** If $R$ is a ring with identity $1$ where $1 \neq 0$, s.t. every nonzero $a \in R$ has a multiplicative inverse, $R$ is called a division ring. A commutative division ring is a field.

**Ex:** $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{R}$ are all fields.

**Ex:** $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring w/ identity (the element $\overline{1}$).

**Ex:** Let $\mathbb{H}$ be the ring of elements of the form $a+bi+cj+dk$, where $a, b, c, d \in \mathbb{R}$. Define $+$ componentwise:

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k) = (a+a')+(b+b')i+(c+c')j+(d+d')k.$$

and multiplication by expanding and then using our rules from $Q_8$ to multiply: $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, etc.

We allow the real coefficients to commute with $i, j, k$, so e.g.

$$(1+i-3k)(j-k) = j-k+ij-ik-3kj+3k^2 = j-k+k+j+3i-3$$
$$= -3+3i+2j$$

This is a division ring!
Note that if we look at the subset where $c=d=0$, we get $\mathbb{C}$.

**Ex:** If $R$ is an (additive) abelian group, we can define $a \cdot b = 0 \ \forall\, a, b \in R$. (called a trivial ring)

From the definition, we can deduce a few basic properties of rings:

**Prop:** Let $R$ be a ring.

1.) $0a = a0 = 0 \quad \forall\, a \in R$

2.) $(-a)b = a(-b) = -(ab) \quad \forall\, a, b \in R$

3.) $(-a)(-b) = ab \quad \forall\, ab \in R$

4.) If $R$ has an identity $1$, then it's unique.

**Pf:** 1.) $0a = (0+0)a = 0a + 0a \Rightarrow 0 = 0a \; (= a0$ by an analogous argument).

2.) $(-a)b + ab = (-a+a)b = 0b = 0$, so $(-a)b = -(ab) \; (= a(-b))$

3.) $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab.$

4.) If $x \in R$ is a multiplicative identity, then

$1 - x = (1-x)1 = \underbrace{1 \cdot 1}_{1} - \underbrace{x \cdot 1}_{1} = 1 - 1 = 0$, so $1 = x$. $\square$

Unlike rings that we're used to, arbitrary rings may have two nonzero elements that multiply to $0$.

**Ex:** In $\mathbb{Z}/4\mathbb{Z}$, $\bar{2} \neq 0$, but $(\bar{2})^2 = \bar{4} = 0$.

**Def:** Let $R$ be a ring.

1.) Let $a \in R$ s.t. $a \neq 0$. If $\exists$ $b \in R$ s.t. $ab = 0$ or $ba = 0$, ($b \neq 0$)

$a$ is called a zero divisor.

2.) If $R$ has an identity $1 \neq 0$, then $u \in R$ is a unit if there is some $v \in R$ s.t. $uv = vu = 1$. (i.e. if $u$ has a multiplicative inverse). The set of units of $R$ is denoted $R^\times$.

Note: $R^\times$ forms a group under multiplication! In a field, every nonzero element is a unit.

Zerodivisors can never be units! If $ca = 1$ and $ab = 0$, for some $b \neq 0$, $c \neq 0$, then $b = cab = c0 = 0$, a contradiction.
$\Rightarrow$ Fields can never have zero divisors.

Ex: $\mathbb{Z}$ has no zero divisors, and its units are $-1, 1$.

Ex: In $\mathbb{Z}/n\mathbb{Z}$, if $m \mid n$, then $\overline{m}$ is a zero divisor.
Otherwise, if $m \nmid n$, we showed $m \in (\mathbb{Z}/n\mathbb{Z})^\times$ and is thus a unit. i.e. all the nonzero elements are units or zerodivisors, and $\mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow$ $n$ is prime.

Ex: Let $D \in \mathbb{Z}$ s.t. $D$ is not a perfect square.

Define $\mathbb{Q}(\sqrt{D}) := \{ a + b\sqrt{D} \mid a, b \in \mathbb{Q} \} \subseteq \mathbb{C}$

Multiplication and addition are defined as in $\mathbb{C}$. i.e.

$$(a+b\sqrt{D})(a'+b'\sqrt{D}) = \underbrace{(aa'+bb'D)}_{\in \mathbb{Q}} + (ab'+ba')\sqrt{D}$$

Note that if $a$ and $b$ aren't both 0, we have

$$(a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - b^2 D \neq 0,$$ since $D$ isn't

a perfect square.

Thus $\frac{(a-b\sqrt{D})}{a^2-b^2D}$ is the inverse of $a+b\sqrt{D}$, so all nonzero

elements have inverses, and $\mathbb{Q}(\sqrt{D})$ is commutative, so it's a field, called a quadratic field.

Rings that have no zero divisors behave a lot more nicely, sharing many properties with $\mathbb{Z}$. (Hence their name...)

**Def:** A commutative ring w/ identity $1 \neq 0$ is called an integral domain if it has no zero divisors.

Non zero divisors have a nice cancellation property:

**Proposition:** Let $R$ be a ring and $a, b, c \in R$ s.t. $a$ is not a zero divisor. If $ab = ac$, then $a=0$ or $b=c$. In particular, this holds for any three elements in an integral domain.

**Pf:** $ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b-c) = 0$. So either

$a = 0$ or $b - c = 0 \longrightarrow b = c$. □

While not all integral domains are fields, this prop implies the following:

**Cor:** Any finite integral domain is a field.

**Pf:** Let $R$ be a finite integral domain. Let $a \in R$ be nonzero. WTS that $a$ has a multiplicative inverse.

Consider the function $R \to R$ defined $x \longmapsto ax$.
If $ax = ay$, then by the prop, $x = y$, so this map is injective. Since $R$ is finite, it's also surjective, so $\exists\ b \in R$ s.t. $ab = 1$. Thus, $R$ is a field. □

**Def:** A subring of a ring $R$ is a subgroup (under addition) that is closed under multiplication.

Note that since $R$ is a ring, any subring defined in this way will automatically satisfy the ring axioms, so it will itself be a ring.

**Remark:** To check that a subset $S$ of a group is a subgroup, we just need that it's nonempty and $a - b \in S$.
This gives us the following:

**Subring criterion:** $S \subseteq R$ is a subring if and only if $S$ is nonempty and closed under subtraction and multiplication.

**Ex:** $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, and all containments are subrings.

**Ex:** $n\mathbb{Z}$ is a subring of $\mathbb{Z}$ $\forall$ $n \in \mathbb{Z}$.

**Ex:** Let $R = \{f : \mathbb{R} \to \mathbb{R}\}$ = set of functions from $\mathbb{R} \to \mathbb{R}$. This is a ring w/ $(f+g)(a) = f(a) + g(a)$ and $(fg)(a) = f(a)g(a)$.

The set of continuous functions $\mathbb{R} \to \mathbb{R}$ is a subring of $R$.

**Ex:** Let $D \in \mathbb{Z}$ be squarefree. Define $\mathbb{Z}[D] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$. This is a subset of $\mathbb{Q}(\sqrt{D})$, and it's clearly a subring, since it's closed under subtraction, and if $a, b, c, d \in \mathbb{Z}$,

$$(a + b\sqrt{D})(c + d\sqrt{D}) = \underbrace{ac + bdD}_{\uparrow \mathbb{Z}} + \underbrace{(ad + bc)}_{\uparrow \mathbb{Z}}\sqrt{D} \in \mathbb{Z}[\sqrt{D}].$$

Recall that in $\mathbb{Q}(\sqrt{D})$, $a + b\sqrt{D}$ has inverse

$$\frac{(a - b\sqrt{D})}{a^2 - b^2 D} = \frac{a}{a^2 - b^2 D} - \frac{b}{a^2 - b^2 D}\sqrt{D}$$ which is not necessarily in $\mathbb{Z}[\sqrt{D}]$.

i.e. $\mathbb{Z}[\sqrt{D}]$ is not a field. In particular any $a \in \mathbb{Z} \subseteq \mathbb{Z}[\sqrt{D}]$ s.t. $a \neq 1, -1$, has no inverse.

**Ex:** (Matrix rings) Let $R$ be a ring. Define $M_n(R)$ to be the set of all $n \times n$ matrices with entries from $R$. Denote

$$(a_{ij}) \in M_n(R)$$

to be the matrix where $a_{ij} \in R$ is the entry in the $i^{th}$ row and $j^{th}$ column.

This is a ring where addition and multiplication are the standard matrix operations. Note that

$$0 = (a_{ij}) \text{ where } a_{ij} = 0 = \begin{pmatrix} 0 & 0 & \cdots \\ 0 & 0 & \cdots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

and if $R$ has $1$, then the multiplicative identity of $M_n(R)$ is $(a_{ij})$ where

$$a_{ij} = \begin{cases} 1 \text{ if } i=j \\ 0 \text{ if } i \neq j \end{cases} = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}.$$

Note that if $n \geq 2$ and $R$ is nontrivial, $M_n(R)$ is not commutative — even if $R$ is commutative!

Let $a, b \in R$ s.t. $ab \neq 0$. Define

$$A = \begin{pmatrix} a & 0 & \cdots \\ 0 & 0 & \\ \vdots & & \ddots \end{pmatrix} = (a_{ij}) \text{ s.t. } a_{11} = a,\ a_{ij} = 0\ \forall i,j \text{ not both one,}$$

and $B = \begin{pmatrix} 0 & b & 0 & \cdots \\ 0 & 0 & & \\ \vdots & & \ddots & \end{pmatrix} = (b_{ij})$ s.t. $b_{12} = b$ and all other $b_{ij} = 0$.

Then $AB = \begin{pmatrix} 0 & ab & 0 & 0 & \cdots \\ & \ddots & \ddots & & \end{pmatrix} \neq 0$, but $BA = 0$, so $AB \neq BA$.

In this case, A and B are both zero divisors.

If R has a 1, then the units of $M_n(R)$ are invertible matrices. In fact, these form a group under multiplication, called $GL_n(R)$, the general linear group. It's <u>not</u> a ring:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

invertible

invertible

not invertible (zero divisor)