1 Basic Concepts

We study properties and structures of algebraic objects called *rings*.
One example of a *ring* to always keep in mind is $\mathbb{Z}$, the ring of integers.

$$\{..., -10, ..., -2, -1, 0, ..., 10, ..., 10^6\}$$

1.1 Some properties of $\mathbb{Z}$

Can *add* integers to get another integer

$$a + b \in \mathbb{Z} \qquad \forall a, b \in \mathbb{Z}$$

Addition in $\mathbb{Z}$ is *associative*

$$(a + b) + c = a + (b + c) = a + b + c \qquad \forall a, b, c \in \mathbb{Z} \tag{1}$$

Addition in $\mathbb{Z}$ is *commutative*

$$a + b = b + a \qquad \forall a, b \in \mathbb{Z} \tag{2}$$

There is an identity for addition in $\mathbb{Z}$, namely 0

$$a + 0 = 0 + a = a \qquad \forall a \in \mathbb{Z} \tag{3}$$

Each integer can be negated

$$-a \in \mathbb{Z} \qquad \forall a \in \mathbb{Z}$$

And this is an *additive inverse*

$$a + (-a) = (-a) + a = 0 \tag{4}$$

Previous four points summarised as

Definition 1.1. $\mathbb{Z}$ is an abelian group under addition

We can also *multiply* two integers to get another integer $ab \in \mathbb{Z} \forall a, b \in \mathbb{Z}$ and multiplication is *associative*

$$a(bc) = (ab)c = abc \forall a, b, c \in \mathbb{Z} \tag{5}$$

The two *operations*, addition and multiplication, obey *distributive laws*

$$\left.\begin{aligned} a(b + c) = ab + ac \\ (a + b)c = ac + bc \end{aligned}\right\} \forall a, b, c \in \mathbb{Z} \tag{6}$$

The above specific properties of $\mathbb{Z}$ can be generalized to *axioms* that collectively define any (abstract ring)
Before the formal definition,another useful and quite different example $M_2(\mathbb{R})$.

Example 1.1. Let $M_2(\mathbb{R})$ denote the set of all 2x2 matrices with entries in $\mathbb{R}$, the real numbers
We can add elements of $M_2(\mathbb{R})$:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} \sqrt{2} & 3 \\ 5 & -7 \end{pmatrix} = \begin{pmatrix} (1+\sqrt{2}) & 4 \\ 5 & -6 \end{pmatrix} \qquad \in M_2(\mathbb{R}) \tag{7}$$

$$a + b \in M_2(\mathbb{R}) \forall a, b \in M_2(\mathbb{R}) \tag{8}$$

Note. Notice how we are doing addition in $\mathbb{R}$ to do addtion in $M_2(\mathbb{R})$

Note. Also nothing special about $M_2\mathbb{R}$,also possible for $M_3(\mathbb{R})$, $M_4(\mathbb{R})$, ..., $M_n(\mathbb{R})$

Matrix addition is *associative* and *commutative*

Example 1.2.

$$(\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix}) + \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + (\begin{pmatrix} e & f \\ g & h \end{pmatrix}) + \begin{pmatrix} w & x \\ y & z \end{pmatrix}) \quad \in M_2(\mathbb{R}) \tag{9}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{10}$$

Note. Again these properties hold for $M_2\mathbb{R}$ because they hold in $\mathbb{R}$.
$M_2\mathbb{R}$ has a zero namely the zero matrix.
Every element of $M_2\mathbb{R}$ has an additive inverse, see $\mathbb{Z}$ example.

Definition 1.2 (Basic Concepts)**.** $M_2\mathbb{R}$ is an *abelian* group under matrix addition

Just as with addition, $M_2\mathbb{R}$ has multipliction and is associative. And distributes over addition

Remark. Matrix multiplication is **not** commutative

1.2 Axiomatic Definitions

An algebraic structure is a set on which(unary,binary,ternary,..) operations are defined, & usually the operation/s obey laws(*axioms*)

Definition 1.3. A ***Group*** is a set G with a binary operation,denoted $\cdot$, a unary operation
$x \in G \to x^-1 \in G$ such that
i) $a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad \forall a, b, c \in G$
ii) $a \cdot 1 = 1 \cdot a = a \qquad \forall a \in G$
iii) $a \cdot a^-1 = a^-1 \cdot a = 1 \qquad \forall a \in G$

Remark. .
1) i) is the associative law
2) 1 is the identity of G, this 1 is unique
3) x^-1 is the inverse of x
4) The operation $\cdot$ is usually called *multiplication* and is usually omitted i.e, $ab = a \cdot b$
5) If $\cdot$ is commutative then G is called *abelian*
6) If we drop axioms ii),iii) and dont require inverses or identity then the structure is a semigroup
7) Not requiring inverses we have a *monoid*

Definition 1.4. A non-empty set R is a ***Ring*** equipped with two binary operations(addition and multiplication) connected by distributive laws
• R is an abelian group wrt $+$
• R is a semigroup wrt multiplication
• Distributivity:

$$\left.\begin{aligned} a(b+c) = ab + ac \\ (a+b)c = ac + bc \end{aligned}\right\} \forall a, b, c \in R \tag{11}$$

Remark. See text for examples of rings, too lazy to type them

2 Elementary Properties of Rings

Here we study the basic properties of a ring

Lemma 2.1. *if R is a ring, then $\forall r, s \in R$ (i) $r0 = 0r = 0//$ (ii) $(-r)s = r(-s) = -rs$ (iii) $(-r)(-s) = rs$*

Proof. .
i) $0 + 0 = 0$
Hence $r(0 + 0) = r)$
$\Rightarrow r0 + r0$ by distributivity
$\Rightarrow r0 + r0 - r0 = r0 - r0$
$\Rightarrow r0 + 0 = 0$
$\Rightarrow r0 = 0$
Similarly, $0r = 0$
ii) $(-r)s + rs = (-r + r)s$
$= 0s$
$= 0$
Hence $(-r)s$ is the additive inverse of rs
iii)$(-r)(-s) + (-rs)$
$= (-r)(-s) + r(-s)$ by ii)
$= (-r + r)(-s)$ distributivity
$= o(-s) = 0$
Hence, $(-r)(-s) = -(-rs) = rs$

□

2.1 Special Kinds of Rings

• A ring R is commutative if $ab = ba \forall a, b \in R$
• A ring R has *multiplicative identity* if $\exists$ element $1 \in R$ such that $1r = r1 = r \forall r \in R$
• The multiplicative identity is unique: if e is identity too then $1e = 1$ but $1e = e$ since 1 is identity. So $1 = e$

Definition 2.1. An ***Integral Domain*** is a commutative ring with $1(\neq 0)$ and no zero-divisors

Note. $1 = 0$ in a ring $R \leftrightarrow R = \{0\}$

Example 2.1.

$$\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$$

are all integral domains. $M_n(\mathbb{C})$ is not an integral domain

Lemma 2.2. *Let R be an integral domain, $a \in R \setminus \{0\}$, and $x, y \in R$*
Then

$$ax = ay \Rightarrow x = y \tag{12}$$

The cancellation laws for multiplication in integral domains

Proof.

$$ax = ay \tag{13}$$
$$\Rightarrow ax - ay = 0 \tag{14}$$
$$\Rightarrow a(x - y) = 0 \tag{15}$$
$$\Rightarrow x - y = 0 \tag{16}$$
$$\Rightarrow x = y \tag{17}$$
$$\tag{18}$$

(15) because 'a' is not a zer0-divisor □

Definition 2.2. A ***Field*** is a commutative ring in which the set of non-zero elements i a group under multiplication

• So if F is a field then $\exists 1 \in F$ such that $1x = x \forall x \in F \setminus \{0\}$, Since $1 \cdot 0 = 0$ by an earlier Lemma 1 really is the multiplicative identity of F

• Also for each $a \in F \setminus \{0\}$,
$\exists a^-1 \in F \setminus \{0\}$ such that $aa^-1 = 1$

• Every field is an integral domain. For if $a \in F \setminus \{0\}, \exists a^-1 \in F \setminus \{0\}$ such that$ab = 0 then b = 1b = a^-1(ab) = a^1 \cdot 0 = 0$