1.1 Rings and Ideals

A ring $A$ is a set with $+$, $\cdot$ such that

(1) $(A, +)$ is an abelian group;
(2) $(A, \cdot)$ is a semigroup;
(3) $\cdot$ distributes over $+$ on both sides.
In this course all rings $A$ are **commutative**, that is,

$$\forall x, y \in A \quad x \cdot y = y \cdot x$$

and have an **identity element** $1$ (easily seen to be unique)

$$\exists 1 \in A \quad (\forall x \in A) \quad 1 \cdot x = x \cdot 1 = x.$$
If $1 = 0$ then $A = \{0\}$ (easy to see), called the zero ring.

Multiplication will be denoted by juxtaposition, and simple facts used without comment, such as

\[
(\forall x, y \in A)
\begin{align*}
x 0 &= 0, \\
(-x)y &= x(-y) = -(xy), \\
(-x)(-y) &= xy.
\end{align*}
\]
Call a subset $S$ of a ring $A$ a **subring** if

\[
\begin{align*}
(i) & \quad 1 \in S; \\
(ii) & \quad (\forall x, y \in S) \quad x + y, xy, -x \in S.
\end{align*}
\]

Condition (ii) is easily seen to be equivalent to

\[
\begin{align*}
(ii)' & \quad (\forall x, y \in S) \quad x - y, xy \in S.
\end{align*}
\]
Note: In other contexts authors replace the condition $1 \in S$ by $S \neq \emptyset$ (which is not equivalent!).

Examples:

(1) $\mathbb{Z}$ is the only subring of $\mathbb{Z}$.

(2) $\mathbb{Z}$ is a subring of $\mathbb{Q}$, which is a subring of $\mathbb{R}$, which is a subring of $\mathbb{C}$. 
(3) \( \mathbb{Z}[i] = \{ a + bi \mid a, b \in \mathbb{Z} \} \) \((i = \sqrt{-1})\),

the ring of **Gaussian integers** is a subring of \( \mathbb{C} \).

(4) \( \mathbb{Z}_n = \{ 0, 1, \ldots, n - 1 \} \)

with addition and multiplication mod \( n \).

(Alternatively \( \mathbb{Z}_n \) may be defined to be the **quotient ring** \( \mathbb{Z}/n\mathbb{Z} \), defined below).
(5)  \( R \) any ring, \( x \) an indeterminate. Put
\[
R[[x]] = \{ a_0 + a_1 x + a_2 x^2 + \ldots \mid a_0, a_1, \ldots \in R \},
\]
the set of **formal power series over** \( R \), which becomes a ring under addition and multiplication of power series. Important subring:
\[
R[x] = \{ a_0 + a_1 x + \ldots + a_n x^n \mid n \geq 0, a_0, a_1, \ldots, a_n \in R \},
\]
the ring of **polynomials over** \( R \).
Call a mapping \( f : A \rightarrow B \) (where \( A \) and \( B \) are rings) a **ring homomorphism** if

(a) \( f(1) = 1 \);

(b) \((\forall x, y \in A)\)

\[
f(x + y) = f(x) + f(y)
\]

and

\[
f(xy) = f(x)f(y)
\]
in which case the following are easily checked:

(i) \( f(0) = 0 \);

(ii) \( (\forall x \in A) \quad f(-x) = -f(x) \);

(iii) \( f(A) = \{ f(x) \mid x \in A \} \), the image of \( f \) is a subring of \( B \);

(iv) Composites of ring hom’s are ring hom’s.
An **isomorphism** is a bijective homomorphism, say $f : A \to B$, in which case we write

$$A \cong B \quad \text{or} \quad f : A \cong B.$$ 

It is easy to check that

$$\cong \quad \text{is an equivalence relation.}$$
A nonempty subset $I$ of a ring $A$ is called an ideal, written $I \triangleleft A$, if

(i) \((\forall x, y \in I)\) \quad x + y, \ -x \in I

\[
\text{[ clearly equivalent to ]}
\]

(i)' \((\forall x, y \in I)\) \quad x - y \in I

(ii) \((\forall x \in I)(\forall y \in A)\) \quad xy \in I.
In particular $I$ is an additive subgroup of $A$, so we can form the quotient group

$$A/I = \{ I + a \mid a \in A \},$$

the group of cosets of $I$,

with addition defined by, for $a, b \in A$,

$$(I + a) + (I + b) = I + (a + b).$$
Further $A/I$ forms a ring by defining, for $a, b \in A$,

$$(I + a) (I + b) = I + (ab).$$

Verification of the ring axioms is straightforward.

— only tricky bit is first checking multiplication is well-defined:
If \( I + a = I + a' \) and \( I + b = I + b' \) then

\[
a - a', \ b - b' \in I,
\]

so

\[
ab - a'b' = ab - ab' + ab' - a'b'
\]

\[
= a(b - b') + (a - a')b' \in I,
\]

yielding \( I + ab = I + a'b' \).
We call \( A/I \) a **quotient ring**.

The mapping

\[
\phi : A \to A/I , \quad x \mapsto I + x
\]

is clearly a surjective ring homomorphism, called the **natural map**, whose kernel is

\[
\ker \phi = \{ x \in A \mid I + x = I \} = I .
\]

Thus all ideals are kernels of ring homomorphisms. The converse is easy to check, so
kernels of ring homomorphisms with domain $A$ are precisely ideals of $A$.

The following important result is easy to verify:

**Fundamental Homomorphism Theorem:**

If $f : A \rightarrow B$ is a ring homomorphism with kernel $I$ and image $C$ then

$$A/I \cong C.$$
Proposition: Let $I \triangleleft A$ and $\phi : A \to A/I$ be the natural map. Then

(i) ideals $\mathcal{J}$ of $A/I$ have the form

$$\mathcal{J} = J/I = \{ I + j \mid j \in J \}$$

for some $J$ such that $I \subseteq J \triangleleft A$.

(ii) $\phi^{-1}$ is an inclusion-preserving bijection between ideals of $A/I$ and ideals of $A$ containing $I$. 
Example: The ring

\[ \mathbb{Z}_n = \{ 0, 1, \ldots, n - 1 \} \]

with mod \( n \) arithmetic is isomorphic to \( \mathbb{Z}/n\mathbb{Z} \):

follows from the Fundamental Homomorphism Theorem, by observing that the mapping \( f : \mathbb{Z} \to \mathbb{Z}_n \) where

\[ f(z) = \text{remainder after dividing } z \text{ by } n \]

is a ring homomorphism with image \( \mathbb{Z}_n \) and kernel \( n\mathbb{Z} \).
Example: \( \mathbb{z}/9\mathbb{z} \cong \mathbb{z}_9 \) has ideals

\[
\mathbb{z}/9\mathbb{z}, \quad 3\mathbb{z}/9\mathbb{z}, \quad 9\mathbb{z}/9\mathbb{z}
\]

(corresponding under the isomorphism to the ideals \( \mathbb{z}_9, \{0, 3, 6\}, \{0\} \) of \( \mathbb{z}_9 \))

which correspond under \( \phi^{-1} \) to

\[
\mathbb{z}, \quad 3\mathbb{z}, \quad 9\mathbb{z}
\]

respectively, a complete list of ideals of \( \mathbb{z} \) which contain \( 9\mathbb{z} \).
Zero-divisors, nilpotent elements and units:

Let \( A \) be a ring.

Call \( x \in A \) a **zero divisor** if

\[
(\exists y \in A) \quad y \neq 0 \quad \text{and} \quad xy = 0 .
\]

**Examples:**

2 is a zero divisor in \( \mathbb{Z}_{14} \).

5, 7 are zero divisors in \( \mathbb{Z}_{35} \).
A nonzero ring in which 0 is the only zero divisor is called an **integral domain**.

**Examples:** \( \mathbb{Z}, \mathbb{Z}[i], \mathbb{Q}, \mathbb{R}, \mathbb{C} \).

We can construct many more because of the following easily verified result:

**Proposition:** If \( R \) is an integral domain then the polynomial ring \( R[x] \) is also.
Corollary: If $R$ is an integral domain then the polynomial ring $R[x_1, \ldots, x_n]$ in $n$ commuting indeterminates is also.

Call $x \in A$ \textbf{nilpotent} if

$$x^n = 0 \quad \text{for some } n > 0.$$
All nilpotent elements in a nonzero ring are zero divisors, but not necessarily conversely.

**Example:** \( 2 \cdot 3 = 0 \) in \( \mathbb{Z}_6 \), so 2 is a zero divisor, but

\[
2^n = \begin{cases} 
2 & \text{if } n \text{ is odd} \\
4 & \text{if } n \text{ is even}
\end{cases}
\]

so 2 is not nilpotent in \( \mathbb{Z}_6 \).
Call $x \in A$ a **unit** if

$$xy = 1$$

for some $y \in A$, in which case it is easy to see that $y$ is unique, and we write $y = x^{-1}$.

It is routine to check that

the units of $A$ form an abelian group under multiplication.
**Examples:**

(1) The units of $\mathbb{Z}$ are $\pm 1$.

(2) The units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$.

(3) If $x \in \mathbb{Z}_n$ then $x$ is a unit iff $x$ and $n$ are coprime as integers. Thus all nonzero elements of $\mathbb{Z}_n$ are units iff $n$ is a prime.
A **field** is a nonzero ring in which all nonzero elements are units.

**Examples:** \( \mathbb{Q} \), \( \mathbb{R} \), \( \mathbb{C} \) and \( \mathbb{Z}_p \), where \( p \) is a prime, are fields.

It is easy to check that all fields are integral domains.
Not all integral domains are fields (e.g. \( \mathbb{Z} \)).

However integral domains are closely related to fields by the construction of **fields of fractions** described in **Part 3**.

A **principal** ideal \( P \) of \( A \) is an ideal generated by a single element, that is, for some \( x \in A \),

\[
P = Ax = xA = \{ ax \mid a \in A \}.
\]
Note that

\[ A1 = A, \quad \text{and} \quad A0 = \{0\}. \]

Clearly, for \( x \in A \),

\[ x \text{ is a unit iff } Ax = A. \]
Proposition: Let $A$ be nonzero. TFAE

1. $A$ is a field.

2. The only ideals of $A$ are $\{0\}$ and $A$.

3. Every homomorphism of $A$ onto a nonzero ring is injective.