Definition of a ring

A ring is a non-empty subset $R$ with two binary operations, written $a \cdot b$ or $ab$ and $a + b$, such that for all $a, b, c \in R$ we have

- $a + b = b + a$,
- $(a + b) + c = a + (b + c)$,
- $\exists 0 \in R$ so $a + 0 = a$,
- $\exists - a \in R$ so $a + (-a) = 0$,
- $(ab)c = a(bc)$,
- $a(b + c) = ab + ac$,
- $(b + c)a = ba + ca$. 
We say a ring $R$ has an **identity or unity** if $\exists 1 \in R$ so $1a = a1 = a$.

If for all $a, b \in R$, $ab = ba$ we say $R$ is **commutative**.

If $u \in R$ satisfies $uw = wu = 1$ for some $w \in R$ we say $u$ is a **unit** of $R$.

If $a, b \in R$ and for some element $c \in R$, $ac = b$ we say $a$ **divides** $b$ and write $a \mid b$.

**Consequences:**

$(R, +, 0)$ is an **abelian group**.

$U = \{u \in R : u$ is a unit$\}$ is a multiplicative group $(U, ., 1)$, the group of units of $R$. 
(1) \( \mathbb{Z} \), the ring of rational integers, \( U = \{-1, 1\} \).

(2) \( \mathbb{Q} \), the ring of rational numbers, \( U = \mathbb{Q} \setminus \{0\} \).

(3) \( M(n, \mathbb{R}) \), \( n \geq 1 \), the non-commutative ring of real matrices, with \( U = \{A \in M(n, \mathbb{R}) : \det A \neq 0\} \).

(4) The ring of continuous real functions on \([0, 1]\).

(5) for \( \mathbb{Z}/n\mathbb{Z} \), \( n \geq 2 \), the ring of integers modulo \( n \).
Theorem 1

(1) \( a0 = 0a = 0, \)
(2) \( a(-b) = (-a)b = -(ab), \)
(3) \( (-a)(-b) = ab, \)
(4) \( a(b - c) = ab - ac, \)
(5) \( (-1)a = -a, \)
(6) \( (-1)(-1) = 1. \)

Proof of (5)

\[
\begin{align*}
a + (-1)a & = 1.a + (-1).a \\
& = (1 + (-1)).a \\
& = 0.a = 0
\end{align*}
\]

Hence, because inverses are unique, \((-1)a = -a.\)
Proof of (6)

By (3), with \(a = b = 1\): \((-1)(-1) = 1.1 = 1\).

By Theorem 1, simple properties can be used confidently, but in general \(ab \neq ba\) and \(ab = ac \iff b = c\).

In \(R = \mathbb{Z}/6\mathbb{Z}\), \([2][3] = [6] = [0] = [2][0]\) but \([3] \neq [0]\).
### Definition

If $R$ is a ring and $S \subset R$ a subset which is a ring using the operations of $R$ we say $S$ is a **subring** of $R$.

### Examples

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$
2. The differentiable functions on $\mathbb{R}$ are a subring of the continuous functions on $\mathbb{R}$
3. $5\mathbb{Z} = \{0, \pm 5, \pm 10, \ldots\} \subset \mathbb{Z}$ is a subring with no 1, an **ideal**.
Definition

A zero-divisor $a$ of a ring $R$ is such that there is a nonzero element $b$ in $R$ with $ab = 0$. An integral domain is a commutative ring with a unity and with no zero-divisors.

Examples

(1) $\mathbb{Z}$ the ring of rational integers is an integral domain,
(2) $\mathbb{Z}/6\mathbb{Z}$ the ring of integers modulo 6 is not an integral domain,
(3) $\mathbb{Z}/p\mathbb{Z} = GF(p)$, $p$ a prime, is an integral domain,
(4) $C[0, 1]$ the continuous functions on $[0, 1]$ is not an integral domain,
(5) $M(2, \mathbb{Z})$ $2\times 2$ matrices with integral coefficients is not an integral domain,
(6) $\mathbb{Z}[x]$ the ring of polynomials in $x$ with integer coefficients is an integral domain.
Cancellation property

If $R$ is an integral domain then if $a \neq 0$ and $ab = ac$ we have $b = c$.

Definition of a field

A field is a commutative ring with a unity in which every non-zero element has a multiplicative inverse, i.e. is a unit.

Examples

(1) If $p$ is a prime then $GF(p)$ is a field with $p$ elements.
(2) $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{C}$ are fields.
(3) $\mathbb{Q}(x)$ the set of rational functions in $x$ with rational coefficients is a field.
Theorem 2  Every finite integral domain is a field.

Proof: Let $R$ be a finite integral domain with unity 1.

Let $a \in R$ be a fixed but arbitrary non-zero element.

Let $\{r_1, r_2, \cdots, r_n\}$ be a list of all the non-zero elements of $R$.

Then if for some indices $i, j$ with $1 \leq i \leq j \leq n$ we have $a.r_i = a.r_j$, we must have, by the cancellation property, $r_i = r_j$ so $i = j$.

Thus the elements $\{a.r_1, \cdots, a.r_n\} \subset R$ are distinct.

There are $n$ of them so they are exactly all of the $n$ non-zero elements.

Therefore, for some index $i$, $a.r_i = 1 \implies a$ has an inverse, and hence $R$ is a field.
Let \( R \) be a ring with a unity \( 1 \). If for all \( n \in \mathbb{N} \),
\[ n \cdot 1 = 1 + \cdots + 1 \neq 0 \]
we say the characteristic of \( R \), denoted \( \text{char } R \), is 0. Otherwise \( \text{char } R \) is the minimum value of \( n \) such that \( n \cdot 1 = 0 \).

Note that if \( n \in \mathbb{N} \) and \( a \in R \), \( n \cdot a := a + a + \cdots + a \), the sum of \( n \) copies of \( a \).
**Characteristic of an integral domain**

**Theorem 3:** If $R$ is an integral domain then $\text{char } R = 0$ or is a rational prime.

Assume there exists an $n \in \mathbb{N}$ such that $n \cdot 1 = 0$ and let $n = s \cdot t$ in $\mathbb{N}$.

Then, since the product of $s$ copies of $1$ and $t$ copies of $1$ is $st$ copies of $1$, we have $0 = n \cdot 1 = (st) \cdot 1 = (s \cdot 1)(t \cdot 1)$.

Since $R$ is an integral domain we must have $s \cdot 1 = 0$ or $t \cdot 1 = 0$, so $s = n$ or $t = n$.

Therefore $n$ is prime.
Let $I \subset R$ be a subring. We say $I$ is an **ideal** if for all $x \in R$ and $a \in I$, $x.a$ and $a.x$ are in $I$.

**Examples**

(1) $\{0\}$ and $R$ are ideals of $R$, called the **trivial** ideals.

(2) $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for all $n \in \mathbb{Z}$.

(3) If $R$ is **commutative with 1** and $r \in R$ then

$$\langle r \rangle := \{x.r : x \in R\}$$

is the **principal ideal** generated by $r$.

(4) More generally

$$\langle r_1, \cdots, r_n \rangle := \{x_1.r_1 + \cdots + x_n.r_n : x_i \in R\}$$

is the **ideal** generated by $\{r_1, \cdots, r_n\}$.
Definition: we say the subset \([r] := r + A := \{r + a : a \in A\}\) is the \textbf{coset} with representative \(r\) with respect to the subring \(A\) in the ring \(R\).

For a fixed subring \(A\), the set of cosets forms an \textbf{additive group} with operation

\[(r + A) + (s + A) := (r + s) + A.\]
Factor Ring Theorem 4

The set of cosets forms a ring with operation
\((x + A)(y + A) := xy + A\) if and only if \(A\) is an ideal. If so we call the ring \(R/A\) or \(R\) modulo \(A\).

Let \(A\) be an ideal of \(R\) and let \(x + A = x' + A\) and \(y + A = y' + A\).

Then \(x = x' + a, \ y = y' + b, \ a, b \in A\).

Thus

\[ xy = (x' + a)(y' + b) = x'y' + (x' b + ay' + ab) \]

so \(xy - x'y' \in A\) and therefore we can define unambiguously
\((x + A)(y + A) := (xy + A)\).

It is easy to check the details that this multiplication gives a ring structure to the set of cosets.
$\mathbb{Z}/3\mathbb{Z} = \{\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$

A ring with 3 elements.

$(2 + 3\mathbb{Z})(2 + 3\mathbb{Z}) = 4 + 3\mathbb{Z} = 1 + 3\mathbb{Z}$

or $[2][2] = [4] = [1], \ [r] = r + 3\mathbb{Z}$. 
Maximal Ideals

Definition

An ideal $M \subset R$, where $R$ is commutative, is called maximal if $M \neq \{0\}$, $M \neq R$ (so we say $M$ is proper), and if $B$ is any ideal with $M \subset B \subset R$ then $B = M$ or $B = R$.

Examples

(1) $\langle 2 \rangle \subset \mathbb{Z}$ is maximal,
(2) $\langle 13 \rangle \subset \mathbb{Z}$ is maximal,
(3) $\langle 2, 3 \rangle \subset \mathbb{Z}$ is not maximal since $\langle 2, 3 \rangle \subset \langle 2 \rangle \subset \mathbb{Z}$,
(4) In $\mathbb{Z}[x]$, $\langle x \rangle$ is not maximal since $\langle x \rangle \subset \langle x, 3 \rangle \subset \mathbb{Z}[x]$. 
**Theorem 5**: If $A \subset R$ is an ideal in a commutative ring with unity, then $A$ is maximal if and only if $R/A$ is a field.

**Proof**

Let $R/A$ be a field, and $B$ an ideal with $A \subset B \subset$ and $A \neq B$.

Let $b \in B \setminus A$ so $[b] \neq [0]$.

Thus there exists a $c$ in $R$ so $[b][c] = [1]$ or $bc - 1 \in A \subset B$.

But $B$ is an ideal so $bc \in B$ and thus $1 = (1 - bc) + bc \in B$ so $B = R$.

Therefore $A$ is a maximal ideal.
Now let $A$ be maximal and $x \in R \setminus A$ be non-zero.

Let $B = \{rx + a : r \in R, \ a \in A\}$. Then $B$ is an ideal, $A \subset B$ and $A \neq B$.

Thus $B = R$. But then $1 \in B$ so there exists $r \in R, \ a \in A$ with $1 = rx + a$ so

$[1] = [r][x]$ or $1 + A = (r + A)(x + A)$ so $x$ has a multiplicative inverse. Thus $R/A$ is a field.
Prime Ideals

Definition

An ideal $P \subset R$, where $R$ is commutative, is called prime if $P$ is proper and $ab \in P$ implies $a \in P$ or $b \in P$ or both.

Examples

(1) $\langle 2 \rangle \subset \mathbb{Z}$ is a prime ideal. More generally, let $p$ be a rational prime. Then $\langle p \rangle \subset \mathbb{Z}$ is a prime ideal.

(2) $\langle 6 \rangle \subset \mathbb{Z}$ is not a prime ideal, nor is $\langle n \rangle$ whenever $n$ is composite.

(3) $4\mathbb{Z}$ as a ring has no prime ideals. We need to assume each ideal $A$ of $\mathbb{Z}$ is generated by one element, i.e. $A = \langle g \rangle$. Then if $A \subset 4\mathbb{Z}$ is an ideal, $A = \langle 4g \rangle$ and $2.2g \in A$, but $2 \notin A$. 
**Theorem 6:** If $A \subset R$ is an ideal in a commutative ring with unity, then $A$ is prime if and only if $R/A$ is an integral domain.

Let $R/A$ be an integral domain and let $ab \in A$.

Then $(a + A)(b + A) = ab + A = A = 0 + A$ so $[a][b] = [0]$.

Therefore $[a] = [0]$ or $[b] = [0]$. So $a \in A$ or $b \in A$ and $A$ is prime.

Let $A \subset R$ be a prime ideal and let in $R/A$, $[a][b] = [0]$.

Then $ab \in A$ so $a \in A$ or $b \in A$. Thus $[a] = [0]$ or $[b] = [0]$ and $R/A$ is an integral domain.