Definition (Rings)

A ring $A$ is a set with an addition and a multiplication so that:

1. $A$ is an Abelian group w.r.t. its addition, and so
   - $A$ has a zero element, denoted 0.
   - Every $x \in A$ has an additive inverse $-x$.

2. Multiplication is associative and distributive over addition, i.e.,
   \[
   (xy)z = x(yz),
   x(y + z) = xy + xz, \quad (x + y)z = xz + yz.
   \]

Remarks

1. 0 is absorbant, i.e., $0x = x0 = 0$ for all $x \in A$.
2. $x(y - z) = xy - xz$ and $(x - y)z = xz - yz$. 
A ring $A$ is commutative when

$$xy = yx \quad \text{for all } x, y \in A.$$  

An identity element $1 \in A$ is such that

$$1x = x1 = x \quad \text{for all } x \in A.$$  

Such an element is unique.

By a ring we shall always mean a commutative ring with an identity element.

If $1 = 0$, then $x = 1x = 0x = 0$, and so 0 is the unique element. We called this ring the zero ring and denote it by 0.
Definition (Ring Homomorphisms)

Given rings $A$ and $B$, a ring homomorphism $f : A \to B$ is a map such that

1. $f(x + y) = f(x) + f(y)$.
2. $f(xy) = f(x)f(y)$.
3. $f(1) = 1$.

Remark

The property (i) implies that

$$f(x - y) = f(x) - f(y), \quad f(-x) = -f(x), \quad f(0) = 0.$$  

Remark

If $f : A \to B$ and $g : B \to C$ are ring homomorphisms, then the composition $g \circ f : A \to C$ is a ring homomorphism as well.
Definition (Subrings)

A subring of a ring $A$ is a subset $S$ that is closed under addition and multiplication and contains the unit. That is,

$$x, y \in S \implies x + y \in S \text{ and } xy \in S,$$
$$1 \in S.$$ 

Remarks

1. Any subring is a ring.
2. If $S$ is a subring of a ring $A$, then the inclusion map of $S$ into $A$ is a ring homomorphism.
Definition (Ideals)

An ideal $\mathfrak{a}$ of a ring $A$ is an additive subgroup such that $A\mathfrak{a} \subset \mathfrak{a}$. That is,

$$x, y \in \mathfrak{a} \implies x + y \in \mathfrak{a},$$

$$x \in A \text{ and } y \in \mathfrak{a} \implies xy \in \mathfrak{a}.$$ 

Observation

The multiplication of $A$ uniquely descends to a multiplication on the quotient $A/\mathfrak{a}$, with respect to which $A/\mathfrak{a}$ is a ring.

Remarks

1. $A/\mathfrak{a}$ is called a quotient ring. Its elements $x + \mathfrak{a}$ are called cosets (of $\mathfrak{a}$ in $A$).
2. The canonical map $\phi : A \to A/\mathfrak{a}$ is a surjective ring homomorphism.
Proposition

There is a one-to-one order-preserving correspondence between ideals \( \mathfrak{b} \) of \( A \) that contains \( \mathfrak{a} \) and the ideals \( \overline{\mathfrak{b}} \) of \( A/\mathfrak{a} \) given by
\[
b = \phi^{-1}(\overline{\mathfrak{b}}).
\]

Fact

Let \( f : A \to B \) is a ring homomorphism. Then
1. The kernel \( f^{-1}(0) \) is an ideal of \( \mathfrak{a} \).
2. The image \( f(A) \) is a subring of \( B \).
3. \( f \) induces a ring isomorphism \( A/f^{-1}(0) \cong f(A) \).

Remark

The notation \( x \equiv y \pmod{\mathfrak{a}} \) means that \( x - y \in \mathfrak{a} \).
Definition (Zero-Divisors, Integral Domains)

- A zero-divisor of a ring $A$ is any element $x$ that divides 0, i.e., there is $y \neq 0$ such that $xy = 0$.
- A (non-zero) ring with no non-zero divisors $\neq 0$ is called an integral domain. That is, we have

$$x \neq 0 \text{ and } xy = 0 \implies y = 0.$$ 

Examples

The following rings are integral domains:

- The ring of integers $\mathbb{Z}$.
- Any polynomial rings $k[x_1, \ldots, x_n]$, where $k$ is a field.
### Definition (Nilpotent Elements)
An element $x \in A$ is nilpotent when $x^n = 0$ for some $n \geq 1$.

### Remark
Any nilpotent element is a zero-divisor (unless $A = 0$). The converse is not true in general.
Definition (Units)

- A unit of $A$ is any element $x$ that divides 1, i.e., there is $y \in A$ such that $xy = 1$.
- In this case $y$ is unique and is denoted $x^{-1}$.

Fact

The set of units of $A$ is a (multiplicative) Abelian group.
**Definition (Principal Ideals)**

A principal ideal is any ideal generated by a single element, i.e., it is of the form $Ax$ for some $x \in A$.

**Remarks**

1. We shall also denote $Ax$ by $(x)$. It consists of all multiples $ax$, $a \in A$.
2. $x$ is a unit if and only if $(x) = A = (1)$.
3. The zero ideal $(0)$ is denoted $0$. 

Definition (Fields)
A field is a ring $A$ in which $1 \neq 0$ and every $x \neq 0$ is a unit.

Remark
Every field is an integral domain. The converse is not true (e.g., $\mathbb{Z}$).

Proposition (Proposition 1.2)
Let $A$ be a non-zero ring. TFAE:
(i) $A$ is a field.
(ii) The only ideals in $A$ are 0 and $A$.
(iii) Every ring homomorphism of $A$ into a non-zero ring is one-to-one.
Prime Ideals and Maximal Ideals

<table>
<thead>
<tr>
<th>Definition (Prime Ideals)</th>
<th>An ideal $p \subsetneq A$ is prime when $xy \in p \Rightarrow x \in p$ or $y \in p$.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fact</td>
<td>$p$ is prime $\iff A/p$ is an integral domain.</td>
</tr>
<tr>
<td>Definition (Maximal Ideals)</td>
<td>An ideal $m \subsetneq A$ is maximal when there is no ideal $\alpha$ such that $m \subsetneq \alpha \subsetneq A$.</td>
</tr>
<tr>
<td>Fact (Proposition 1.1 + Proposition 1.2)</td>
<td>$m$ is maximal $\iff A/p$ is a field. In particular, any maximal ideal is prime.</td>
</tr>
<tr>
<td>Remark</td>
<td>The zero ideal is prime if and only if $A$ is an integral domain.</td>
</tr>
</tbody>
</table>
**Fact**

Let $f : A \rightarrow B$ be a ring homomorphism and $q$ a prime ideal. Then $f^{-1}(q)$ is a prime ideal in $A$.

**Remark**

If $\mathfrak{n}$ is a maximal ideal in $A$, then $f^{-1}(\mathfrak{n})$ is prime, but it need not be maximal (e.g., $A = \mathbb{Z}$, $B = \mathbb{Q}$, $\mathfrak{n} = 0$).
Theorem (Theorem 1.3; see Atiyah-MacDonald + Carlson)

Every ring \( A \neq 0 \) admits a maximal ideal.

Corollary (Corollary 1.4)

For any ideal \( \alpha \subset A \), there is a maximal ideal that contains \( \alpha \).

Corollary (Corollary 1.5)

Every non-unit of \( A \) is contained in a maximal ideal.
Remark

There are rings with exactly one maximal ideal, e.g., fields (in which 0 is the unique maximal ideal).

Definition

1. A ring with exactly one maximal ideal \( \mathfrak{m} \) is called a local ring.
2. The field \( k = A/\mathfrak{m} \) is called the residual field of \( A \).

Proposition (Proposition 1.6)

(i) Let \( \mathfrak{m} \varsubsetneq A \) be an ideal such that any \( x \in A \setminus \mathfrak{m} \) is a unit. Then \( A \) is local ring and has \( \mathfrak{m} \) as unique maximal ideal.

(ii) Let \( \mathfrak{m} \) be a maximal ideal such that every element of \( 1 + \mathfrak{m} \) is a unit. Then \( A \) is a local ring.
Prime Ideals and Maximal Ideals

Example

Let $A = k[x_1, \ldots, x_n]$, $k$ field. If $f \in A$ is irreducible, then the ideal $(f)$ is prime.

Example

Let $A = \mathbb{Z}$. Then

1. Every ideal of $\mathbb{Z}$ is a principal ideal $(m)$ for some $m \geq 0$.
2. $(m)$ is a prime ideal if and only if $m = 0$ or is a prime number.
3. All the ideals $(p)$ with $p$ prime are maximal, since $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$ is a field.
4. The same holds for $A = k[x_1]$, but not for $A = k[x_1, \ldots, x_n]$ with $n \geq 2$. 
Example (Principal Ideal Domain)

A principal ideal domain is an integral domain in which every ideal is principal (e.g., \( \mathbb{Z} \), \( k[x_1] \)). In such an ideal every non-zero prime ideal is maximal.
Proposition (Proposition 1.7)

Let $A$ be a ring. Denote by $\mathfrak{N}$ the set of all nilpotent elements of $A$. Then the following holds:

1. $\mathfrak{N}$ is an ideal
2. The quotient ring $A/\mathfrak{N}$ has no non-zero nilpotent elements.

Definition

The ideal $\mathfrak{N}$ is called the nilradical of $A$.

Proposition (Proposition 1.8; see Atiyah-MacDonald)

The nilradical $\mathfrak{N}$ is the intersection of all the prime ideals of $A$. 
Definition

The Jacobson radical $\mathcal{R}$ of $A$ is the intersection of all its maximal ideals.

Proposition (Proposition 1.9)

$$\mathcal{R} = \{ x \in A; \ 1 - xy \text{ is a unit for all } y \in A \}.$$
Operations on Ideals

**Definition (Sum of Ideals)**

If $a$ and $b$ are ideals in a ring $A$, their sum $a + b$ is the set all sums $x + y$ with $x \in a$ and $y \in b$.

**Fact**

$a + b$ is the smallest ideal that contains $a$ and $b$.

**Definition (Sum of Ideals)**

Given a (possibly infinite) family $\{a_i\}_{i \in I}$ of ideals of $A$, the sum $\sum_{i \in I} a_i$ consists of all finite sums $\sum x_i$ with $x_i \in a_i$.

**Fact**

$\sum_{i \in I} a_i$ is the smallest ideal that contains the $a_i$'s.
Fact
The intersection of any family of ideals \((\mathfrak{a}_i)_{i \in I}\) is an ideal.

Consequence
The ideals of \(A\) form a complete lattice with respect to inclusion, i.e., every subset has a supremum and an infimum.
Definition (Product of Ideals)

The product of two ideals \( \mathfrak{a} \) and \( \mathfrak{b} \) in \( A \) is the ideal \( \mathfrak{a} \mathfrak{b} \) generated by \( \mathfrak{a} \) and \( \mathfrak{b} \). It consists of all finite sums \( \sum x_i y_i \) with \( x_i \in \mathfrak{a} \) and \( y_i \in \mathfrak{b} \).

Remark

1. We similarly define the product of any finite family of ideals.
2. In particular, the power \( \mathfrak{a}^n \), \( n \geq 1 \), of an ideal \( \mathfrak{a} \) is generated by products \( x_1 \cdots x_n \) with \( x_j \in \mathfrak{a} \).
3. By convention \( \mathfrak{a}^0 = (1) = A \).
### Example

Suppose that \( A = \mathbb{Z} \), \( a = (m) \) and \( b = (n) \). Then:

1. \( a + b \) is the ideal generated by \( \gcd(m, n) \) (greatest common divisor, a.k.a. highest common factor).
2. \( a \cap b \) is the ideal generated by \( \text{lcm}(m, n) \) (lowest common multiple).
3. \( ab = (mn) \).

### Example

\( A = k[x_1, \ldots, x_n] \), \( a = (x_1, \ldots, x_n) \) ideal generated by \( x_1, \ldots, x_n \). Then \( a^m, m \geq 1 \), consists of all polynomials with no terms of degree \( \leq m \).
Remarks

1. The three operations (sum, intersection, product) are all associative and commutative.

2. We also have the distributive law,

\[ a(b + c) = ab + ac. \]

3. In \( \mathbb{Z} \) the laws \( \cap \) and \( + \) are distributive over each other. This is not true for a general ring. At best we have the modular law,

\[ a \cap (b + c) = a \cap b + a \cap c \quad \text{if } a \supseteq b \text{ or } a \supseteq c. \]

4. In \( \mathbb{Z} \) we have \((a + b)(a \cap b) = ab\). In general, we only have

\[ (a + b)(a \cap b) \subseteq ab. \]
Definition

Two ideals \( a \) and \( b \) are said to be coprime when \( a + b = (1) \). That is, there are \( x \in a \) and \( y \in b \) such that \( x + y = 1 \).

Fact

We always have the inclusions,

\[(a + b)(a \cap b) \subseteq ab \quad \text{and} \quad ab \subseteq a \cap b.\]

Thus, if \( a \) and \( b \) are coprime, then we have

\[a \cap b = ab.\]
Definition (Direct Product of Rings)
Let $A_1, \ldots, A_n$ be rings ($n \geq 2$).

1. The direct product $A := \prod_{i=1}^{n} A_i$ consists of sequences $(x_1, \ldots, x_n)$ with $x_i \in A_i$.
2. We equip it with the component-wise addition and multiplication.

Facts

1. $\prod_{i=1}^{n} A_i$ is a commutative ring with identity $(1, \ldots, 1)$.
2. The projections $p_i : A \to A_i$ defined by $p_i(x) = x_i$ are ring homomorphisms.
Let $A$ be a ring $a_1, \ldots, a_n$ ideals of $A$. Define $\phi : A \rightarrow \prod_{i=1}^{n}(A/a_i)$ by

$$\phi(x) = (x + a_1, \ldots, x + a_n), \quad x \in A.$$ 

**Fact**

$\phi$ is a ring homomorphism.

**Proposition (Proposition 1.10)**

The following holds.

1. If $a_i$ and $a_j$ are coprime whenever $i \neq j$, then $\prod a_i = \cap a_i$.
2. $\phi$ is onto if and only if $a_i$ and $a_j$ are coprime whenever $i \neq j$.
3. $\phi$ is one-to-one if and only if $\cap a_i = 0$. 

Remark
The union $\mathfrak{a} \cup \mathfrak{b}$ need not be an ideal in general.

Proposition (Proposition 1.11)

1. Assume that $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are prime ideals and $\mathfrak{a}$ is an ideal contained in $\bigcup \mathfrak{p}_i$. Then $\mathfrak{a} \subseteq \mathfrak{p}_i$ for some $i$.

2. Assume that $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are ideals and $\mathfrak{p}$ is a prime ideal containing $\bigcap \mathfrak{a}_i$. Then $\mathfrak{p} \supseteq \mathfrak{a}_i$ for some $i$. If $\mathfrak{p} = \bigcap \mathfrak{a}_i$, then $\mathfrak{p} = \mathfrak{a}_i$ for some $i$. 
Operations on Ideals

**Definition (Ideal Quotient)**

If \( a \) and \( b \) are ideals in a ring \( A \), their ideal quotient is

\[
(a : b) := \{ x; \, xb \subseteq a \}.
\]

**Fact**

\( (a : b) \) is an ideal.

**Definition**

\( (0; b) \) is called the annihilator of \( b \) and is also denoted by \( \text{Ann}(b) \). It consists of all \( x \in A \) such that \( xb = 0 \).

**Remarks**

1. When \( b \) is a principal ideal \((x)\) we shall denote \((a : (x))\) and \(\text{Ann}((x))\) by \((a : x)\) and \(\text{Ann}(x)\), respectively.
2. \(\text{Ann}(x) = \{ y \in A; xy = 0 \}\).
3. The set of all non-zero divisors in \( A \) is \( D = \bigcup_{x \neq 0} \text{Ann}(x) \).
Example

$A = \mathbb{Z}$, $a = (m)$, $b = (n)$. Then

$$(a : b) = (q), \quad q = \frac{m}{\gcd(m, n)}.$$

Exercise (Exercise 1.12; see Carlson)

(i) $a \subset (a : b)$.

(ii) $(a : b)b \subset a$.

(iii) $((a : b) : c) = (a : bc) = ((a : c) : b)$.

(iv) $\bigcap a_i : b) = \bigcap (a_i : b)$.

(v) $a : \bigcap b_i) = \bigcap (a : b_i)$. 
Definition (Radical of an Ideal)

Let \( \mathfrak{a} \) be an ideal of \( A \). Its radical is

\[
\tau(\mathfrak{a}) := \{ x \in A; \ x^n \in \mathfrak{a} \text{ for some } n \geq 1 \}.
\]

Fact

If \( \phi : A \to A/\mathfrak{a} \) is the canonical homomorphism, then \( \tau(\mathfrak{a}) = \phi^{-1}(\mathfrak{N}_{A/\mathfrak{a}}) \), and hence \( \tau(\mathfrak{a}) \) is an ideal (since the nilradical \( \mathfrak{N}_{A/\mathfrak{a}} \) is an ideal by Proposition 1.7).
Exercise (Exercise 1.13; see Carlson)

(i) \( r(a) \supseteq a \).

(ii) \( r(r(a)) = r(a) \).

(iii) \( r(ab) = r(a \cap b) = r(a) \cap r(b) \).

(iv) \( r(a) = (1) \iff a = (1) \).

(v) \( r(a + b) = r(r(a) + r(b)) \).

(vi) If \( p \) is prime, then \( r(p^n) = p \) for all \( n \geq 1 \).

Proposition (Proposition 1.14)

The radical \( r(a) \) is the intersection of the prime ideals that contains \( a \).
Remark

Given any subset $E \subseteq A$ we may define its radical $r(E)$ as above. This is not an ideal in general (unless $E$ is an ideal).

Fact

Given any family $E_\alpha$ of subsets of $A$, we have $r(\bigcup E_\alpha) = \bigcup r(E_\alpha)$.

Proposition (Proposition 1.15)

The set $D$ of zero-divisors of $A$ is equal to $\bigcup_{x \neq 0} r(\text{Ann}(x))$. 
Example

Let $A = \mathbb{Z}$, $\alpha = (m)$. Let $p_1, \ldots, p_r$ be the prime divisors of $m$. Then

$$r(\alpha) = (p_1 \cdots p_r) = \bigcap_{i=1}^{r} (p_i).$$

Proposition (Proposition 1.16)

If $\alpha$ and $\beta$ are ideals of $A$ such that $r(\alpha)$ and $r(\beta)$ are coprime, then $\alpha$ and $\beta$ are coprime.
Let \( f : A \rightarrow B \) be a ring homomorphism.

**Fact**

If \( \mathfrak{a} \) is an ideal, then \( f(\mathfrak{a}) \) need not be an ideal.

**Definition (Extension)**

The extension \( \mathfrak{a}^e \) of \( \mathfrak{a} \) is the ideal \( Bf(\mathfrak{a}) \) generated by \( \mathfrak{a} \). That is, \( \mathfrak{a}^e \) consists of all finite sums \( \sum y_if(x_i) \) with \( y_i \in B \) and \( x_i \in \mathfrak{a} \).

**Fact**

If \( \mathfrak{b} \) is an ideal of \( B \), then \( f^{-1}(\mathfrak{b}) \) is in ideal of \( A \).

**Definition (Contraction)**

\( f^{-1}(\mathfrak{b}) \) is called the contraction of \( \mathfrak{b} \) and is denoted by \( \mathfrak{b}^c \).
### Facts

1. If \( b \) is prime, then its contraction \( b^c \) is prime as well.
2. If \( a \) is a prime ideal of \( A \), then its extension \( b^e \) need not be prime (cf. example below).

### Example (see Atiyah-MacDonald)

Consider the inclusion \( \mathbb{Z} \to \mathbb{Z}[i] \), where \( i = \sqrt{-1} \). The extension of a prime ideal \( (p) \) in \( \mathbb{Z} \) may or may not be prime. Namely:

- \((2)^e = ((1 + i)^2)\), the square of a prime ideal in \( \mathbb{Z}[i] \).
- If \( p \equiv 1 \pmod{4} \), then \((p)^e\) is the product of two distinct prime ideals.
- If \( p \equiv 2 \pmod{4} \), then \((p)^e\) is prime in \( \mathbb{Z}[i] \).
Definition

- \( C \) is the set of contracted ideals in \( A \).
- \( E \) is the set of extended ideals in \( B \).

Proposition (Proposition 1.17; see also Carlson)

(i) \( a \subseteq a^{ec} \) and \( b \supseteq b^{ce} \).
(ii) \( a = a^{ece} \) and \( b = b^{cec} \).
(iii) \( C = \{a; \ a^{ec} = a\} \), \( E = \{b; \ b^{ce} = b\} \), and \( a \rightarrow a^e \) is a bijection from \( C \) onto \( E \) with inverse \( b \rightarrow b^c \).
## Exercise (Exercise 1.18; see Carlson)

Let $a_1$ and $a_2$ be ideals of $A$ and let $b_1$ and $b_2$ be ideals of $B$.

\[
\begin{align*}
(a_1 + a_2)^e &= a_1^e + a_2^e, \\
(a_1 \cap a_2)^e &\subseteq a_1^e \cap a_2^e, \\
(a_1 a_2)^e &= a_1^e a_2^e, \\
(a_1 : a_2)^e &\subseteq (a_1^e : a_2^e), \\
\text{and } r(a)^e &\subseteq r(a^e),
\end{align*}
\]

\[
\begin{align*}
(b_1 + b_2)^c &\supseteq b_1^c + b_2^c, \\
(b_1 \cap b_2)^c &= b_1^c \cap b_2^c, \\
(b_1 b_2)^c &\supseteq b_1^c b_2^c, \\
(b_1 : b_2)^c &\subseteq (b_1^c : b_2^c), \\
\text{and } r(b)^c &= r(b^c).
\end{align*}
\]

The set of ideals $E$ is closed under sum and product, and $C$ is closed under the other three operations (intersection, ideal quotient and radical).