This document contains lecture notes for the course Math 557, Ring Theory, taught at the University of Idaho by me, Brooks Roberts, in the fall of 2022. The text for the course was *Steps in Commutative Algebra*, by R. Y. Sharp. The coverage of the notes begin near the end of the first chapter of Sharp. These notes are essentially a copy of the material as presented in my lectures.

Contents

1 Commutative rings and subrings 1

2 Ideals 4

3 Prime ideals and maximal ideals 12

4 Primary Decomposition 26

1 Commutative rings and subrings

We recall that a **Euclidean domain** is an integral domain $R$ with a function $\partial : R - 0 \rightarrow \mathbb{N}_0$ (called the **degree function**) such that:

(i) If $a, b \in R - 0$, and $a \mid b$, i.e., there exists $c \in R$ such that $ac = b$, then $\partial(a) \leq \partial(b)$.

(ii) If $a, b \in R$ with $b \neq 0$, then there exist $q, r \in R$ such that

$$a = qb + r$$

and $r = 0$ or $r \neq 0$ and $\partial(r) < \partial(b)$.

Here are some examples of integral domains that are Euclidean:

**Example.** If $K$ is a field, then $K$ is a Euclidean domain with $\partial(r) = 1$ for all $r \in R - 0$.

**Example.** $\mathbb{Z}$ is a Euclidean domain with $\partial(n) = |n|$.

**Example.** Let $K$ be a field, and let $X$ be an indeterminate. Then $K[X]$ is a Euclidean domain with $\partial(p) = \deg(p)$.

**Example.** $R = \mathbb{Z}[i]$, the **Gaussian integers**, with

$$\partial(a) = |a|^2 = x^2 + y^2, \quad a = x + iy, \quad x, y \in \mathbb{Z}.$$

Here, $i = \sqrt{-1}$.

**Proof.** We need to prove that $(R, \partial)$ has the two properties of a Euclidean domain. Let $a, b \in R - 0$ with $a \mid b$. Let $c \in R$ be such that $ac = b$. We have

$$\partial(b) = |b|^2 = |ac|^2 = |a|^2|c|^2 = \partial(a)\partial(c).$$

Since $\partial(b), \partial(a),$ and $\partial(c)$ are positive integers we must have $\partial(a) \leq \partial(b)$. 

For the second property, let $a, b \in \mathbb{R}$ with $b \neq 0$. We consider $ab^{-1} \in \mathbb{C}$. We have

$$ab^{-1} = x + iy, \quad x, y \in \mathbb{Q}.$$ 

There exist $m, n \in \mathbb{Z}$ and $g, h \in \mathbb{Q}$ such that

$$x = m + g, \quad y = n + h, \quad |g| \leq 1/2, \quad |h| \leq 1/2.$$

Hence,

$$ab^{-1} = (m + g) + i(n + h),$$

$$ab^{-1} = (m + in) + (g + ih),$$

$$a = (m + ih)b + (g + ih)b$$

where

$$q = m + in, \quad r = (g + ih)b.$$ 

Since $a, b, \text{ and } q$ are in $R$, so is $r$. Now

$$\partial(r) = |r|^2 = |g + ih|^2 \cdot |b|^2 = (g^2 + h^2) \partial(b) \leq (1/4 + 1/4) \partial(b) < \partial(b).$$

This completes the proof.

Let $(R, \partial)$ be a Euclidean domain. In general, the $q$ and $r$ in the definition of a Euclidean domain are not uniquely determined. The Gaussian integers provide an example. We have

$$11 + 7i = \underbrace{(2 - i)}_{a} \underbrace{(2 + 5i)}_{q} + \underbrace{(2 - i)}_{b} \underbrace{(2 + 5i)}_{r}, \quad \partial(r) = 5 < \partial(b) = 29.$$

But we also have

$$11 + 7i = \underbrace{(2 - 2i)}_{a} \underbrace{(2 + 5i)}_{q} + \underbrace{(-3 + i)}_{b} \underbrace{(2 + 5i)}_{r}, \quad \partial(r) = 10 < \partial(b) = 29.$$

However, if $R = \mathbb{Z}$ or $R = K[X]$, then $q$ and $r$ are uniquely determined.

The Gaussian integers are an example of the ring of integers of a quadratic extension of $\mathbb{Q}$. Such rings of integers are studied in algebraic number theory. Many of the concepts of commutative...
algebra, especially early in its history, were developed for algebraic number theory. If $D$ is a square-free integer, then the ring of integers in $\mathbb{Q}(\sqrt{D})$ is:

$$R = \mathbb{Z}[\omega]$$

where

$$\omega = \begin{cases} 
\sqrt{D} & \text{if } D \equiv 2, 3 \pmod{4}, \\
\frac{1 + \sqrt{D}}{2} & \text{if } D \equiv 1 \pmod{4}.
\end{cases}$$

It is natural to consider whether or not $R$ is Euclidean with

$$\partial(a + b\omega) = |a^2 - b^2D|$$

for $a, b \in \mathbb{Z}$ in analogy to the Gaussian integers. It is known that there are twenty-one values of $D$ for which $R$ with this $\partial$ is Euclidean. These values are $D = -1, -2, -3, -7, -11$ and $D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$

**Unique factorization domains.** We now consider another class of examples of integral domains that turns out to be more general than Euclidean domains.

Let $R$ be an integral domain. Let $r \in R$. We say that $r$ is an **irreducible element** of $R$ if:

(i) $r \neq 0$ and $r$ is not a unit.

(ii) If $a, b \in R$ and $r = ab$, then $a$ is a unit or $b$ is a unit.

We say that $R$ is a **unique factorization domain** if:

(i) For all $r \in R$ such that $r \neq 0$ and $r$ is not a unit, there exist irreducible elements $p_1, \ldots, p_s$ such that

$$r = p_1 \cdots p_s.$$ 

(ii) If $p_1, \ldots, p_s$ and $q_1, \ldots, q_t$ are irreducible elements in $R$ and

$$p_1 \cdots p_s = q_1 \cdots q_t$$

then $s = t$, and after a renumbering, there exist units $u_1, \ldots, u_s \in R$ such that $p_i = u_i q_i$ for $i = 1, \ldots, s$.

We will often abbreviate “unique factorization domain” as “UFD”.

We will prove the following theorem later on.

**Theorem 1.** If $R$ is a Euclidean domain, then $R$ is a unique factorization domain.

By the theorem, the following are all UFDs: any field, $\mathbb{Z}$, $K[X]$ for $K$ a field, and $\mathbb{Z}[i]$.

We also have the following theorem:

**Theorem 2.** If $R$ is a unique factorization domain, then $R[X]$ is a unique factorization domain.

By repeated use of this theorem, if $R$ is a UFD, then so is $R[X_1, \ldots, X_n]$.  

3
One way to prove Theorem 2 is as follows. Let \( K \) be field of fractions of \( R \). We know that \( K[X] \) is a Euclidean domain. By Theorem 1 we have that \( K[X] \) is a UFD. We now use this to prove that \( R[X] \) is a UFD; this uses the Gauss Lemma.

We note that if \( R \) is a UFD, then it can happen that \( R[[X]] \) is not a UFD.

It is fairly common that the existence condition (i) for a UFD holds for a ring \( R \). For example, if \( R \) is a Noetherian domain, then (i) holds. The uniqueness condition (ii) is the key point. If \( R \) is the ring of integers in an algebraic number field, then (i) does hold, but (ii) usually does not. Let \( R = \mathbb{Z}[\omega] \) as above. If \( D < 0 \), then it is known that \( R \) is a UFD for exactly \( D = 1, 2, -3, -7, -11, -19, -43, -67, -163 \). If \( D > 0 \), then it is still an open problem to determine when \( R \) is a UFD. It is conjectured that there are infinitely many \( D > 0 \) such that \( R \) is a UFD, but this is not known. Historically, the problem that not all rings are UFDs led to the introduction of the concept of “ideal numbers” or what are nowadays called ideals.

2 Ideals

Let \( R \) be a commutative ring (as usual, with identity 1). Let \( I \) be a subset of \( R \). We say that \( I \) is an **ideal** of \( R \) if:

(i) \( I \neq \emptyset \).

(ii) If \( a, b \in I \), then \( a + b \in I \).

(iii) If \( r \in R \) and \( a \in I \), then \( ra \in I \).

Assume that \( I \) is an ideal of \( R \). Then \( I \) is an additive subgroup of \( R \). To see this it suffices to prove that if \( a, b \in I \), then \( a - b \in I \). Let \( a, b \in I \). Then \( -b = (-1)b \in I \) by (iii); we now have \( a - b \in I \) by (ii).

Besides being an additive subgroup of \( R \), the set \( I \) also the property that \( ra \in I \) for \( r \in R \) and \( a \in A \).

**Example.** Let \( R \) be a commutative ring. Then 0 and \( R \) are ideals of \( R \).

**Example.** Let \( R \) and \( S \) be commutative rings, and let \( f : R \to S \) be a ring homomorphism. Define the **kernel** of \( f \) to be

\[
\ker(f) = \{ r \in R : f(r) = 0 \}.
\]

Then \( \ker(f) \) is an ideal of \( R \).

**Proof.** The set \( \ker(f) \) is non-empty because \( 0 \in \ker(f) \). Let \( a, b \in \ker(f) \). Then \( f(a + b) = f(a) + f(b) = 0 + 0 = 0 \), so that \( a + b \in \ker(f) \). Finally, let \( r \in R \) and \( a \in \ker(f) \). Then

\[
f(ra) = f(r)f(a) = f(r) \cdot 0 = 0,
\]

so that \( ra \in \ker(f) \). \( \square \)

This example shows that ideals are the analogues of normal subgroups.

**Example.** Let \( R \) be a commutative ring. Let \( a \in R \). Define

\[
(a) = Ra = aR = \{ ra : r \in R \}.
\]
Then \((a)\) is an ideal of \(R\). The ideal \((a)\) is called the \textbf{principal ideal} generated by \(a\) and \(a\) is said to be a \textbf{generator} of \((a)\).

**Proof.** Clearly, \((a)\) is non-empty. Let \(x, y \in (a)\). Then there exist \(r, s \in R\) such that \(x = ra\) and \(y = sa\). We have \(x + y = ra + sa = (r + s)a\). It follows that \(x + y \in I\) so that property (ii) holds. It is clear that property (iii) holds; hence, \(I\) is an ideal. 

**Example.** If \(R = \mathbb{Z}\) and \(n \in \mathbb{Z} - 0\), then we can consider the principal ideal \((n) = \mathbb{Z}n = n\mathbb{Z}\). This is the set of all the integers divisible by \(n\).

Let \(R\) be an integral domain. We say that \(R\) is a \textbf{principal ideal domain} if every ideal of \(R\) is principal. We will abbreviate “principal ideal domain” to “PID”.

**Theorem 3.** Let \(R\) be a Euclidean domain. Then \(R\) is a principal ideal domain.

**Proof.** Let \(I\) be an ideal of \(R\). If \(I = 0\) then \(I\) is principal. Assume that \(I \neq 0\). Consider the set

\[\{ \partial(b) : b \in I, b \neq 0 \}.\]

This is a non-empty set of non-negative integers. It follows that this set contains a smallest element \(\partial(b)\) for some \(b \in I\). We claim that \(I = (b)\). It is clear that \((b) \subseteq I\). Let \(a \in I\). There exist \(q, r \in R\) such that

\[a = qb + r \text{ and } r = 0 \text{ or } r \neq 0 \text{ and } \partial(r) < \partial(b).\]

If \(r = 0\), then \(a = qb\) so that \(a \in (b)\). Assume that \(r \neq 0\); we will obtain a contradiction. Since \(r \neq 0\) we have \(\partial(r) < \partial(b)\). Also, \(r = a - qb \in I\). This contradicts the minimality of \(\partial(b)\). We have proven that \(a \in (b)\) so that \(I \subseteq (b)\). 

By this theorem we see immediately that \(\mathbb{Z}\) and \(K[X]\) for \(K\) a field are PIDs. But very many important rings are not PIDs. For example, in the exercises you will prove that if \(K\) is field then \(K[X_1, X_2]\) is not a PID.

Later on we will prove that every PID is a UFD.

**Creating ideals.** We now consider some important ways to make ideals. The first is via intersections of ideals.

**Proposition 4.** Let \(R\) be a commutative ring, and let \((I_\lambda)_{\lambda \in \Lambda}\) be a collection of ideals of \(R\). Then the intersection

\[I = \bigcap_{\lambda \in \Lambda} I_\lambda\]

is an ideal of \(R\). The ideal \(I\) is called the \textbf{intersection} of the family \((I_\lambda)_{\lambda \in \Lambda}\).

**Proof.** Since 0 is contained in every ideal, the intersection \(I\) is non-empty. Let \(a, b \in I\). Let \(\lambda \in \Lambda\). Then \(a, b \in I_\lambda\). This implies that \(a + b \in I_\lambda\). It follows that \(a + b \in I\), proving that \(I\) has property (ii). The argument that \(I\) has property (iii) is similar. 

5
Example. If \(m, n \in \mathbb{Z} - 0\), then
\[
(m) \cap (n) = \mathbb{Z}m \cap \mathbb{Z}n = (\text{lcm}(m, n)) = \mathbb{Z}\text{lcm}(m, n) = \text{lcm}(m, n)\mathbb{Z}.
\]

To define more ways of creating ideals we first need some notation. Let \(R\) be a commutative ring. Let \(A, B, A_1, \ldots, A_n\) be non-empty subsets of \(R\). We define
\[
A_1 + \cdots + A_n = \{a_1 + \cdots + a_n : a_1 \in A_1, \ldots, a_n \in A_n\}.
\]

We also define
\[
AB = \{\sum_{i=1}^{n} a_i b_i : n \in \mathbb{N}, a_1, \ldots, a_n \in A, b_1, \ldots, b_n \in B\}.
\]

More generally, we define
\[
A_1 \cdots A_n = \text{the set of all finite sums of elements of the form } a_1 \cdots a_n, a_1 \in A_1, \ldots, a_n \in A_n.
\]

We also define
\[
A^n = A \cdots A.
\]

**Proposition 5.** Let \(R\) be a commutative ring. Let \(H\) be a non-empty subset of \(R\). Then the set \(RH = HR\) is an ideal of \(R\) called the **ideal generated by** \(H\).

**Proof.** This is a straightforward verification. \(\square\)

Let the notation be as in Proposition 5. Then we will also write \((H)\) for \(RH = HR\). Assume that \(H = \{h_1, \ldots, h_t\}\). We then write \((h_1, \ldots, h_t)\) for \(RH = HR = (H)\). We call \((h_1, \ldots, h_t)\) the **ideal generated** by \(h_1, \ldots, h_t\) and say that \((H)\) is **finitely generated**. It is easy to see that
\[
(h_1, \ldots, h_t) = \{r_1 h_1 + \cdots + r_t h_t : r_1, \ldots, r_t \in R\}.
\]

This extends the concept of an ideal generated by a single ideal, i.e., a principal ideal. We can form new ideals by taking sums.

**Proposition 6.** Let \(R\) be a commutative ring, and let \(I_1, \ldots, I_n\) be ideals of \(R\). Then the sum \(I_1 + \cdots + I_n\) is an ideal of \(R\).

**Proof.** This is a straightforward verification. \(\square\)

**Example.** Let \(R\) be a commutative ring and let \(h_1, \ldots, h_t \in R\). Then
\[
(h_1, \ldots, h_t) = (h_1) + \cdots + (h_t).
\]

**Example.** If \(m, n \in \mathbb{Z} - 0\), then
\[
(m) + (n) = \mathbb{Z}m + \mathbb{Z}n = \mathbb{Z} = \mathbb{Z}\gcd(m, n) = (\gcd(m, n)).
\]
Finally, we can form products of ideals.

**Proposition 7.** Let $R$ be a commutative ring and let $I_1, \ldots, I_n$ be ideals of $R$. Then the **product** $I_1 \cdots I_n$ is an ideal of $R$.

**Proof.** This is again a straightforward verification. □

Suppose that $I$, $J$, and $K$ are ideals of a commutative ring $R$. Then it is easy to verify the following statements:

\[
IJ \subseteq I \cap J,
\]
\[
(IJ)K = I(JK),
\]
\[
IJ =JI,
\]
\[
RI = I,
\]
\[
0I = 0,
\]
\[
I(J + K) = IJ + IK.
\]

**Example.** If $a, b \in R$, then $(a)(b) = (ab)$.

**Example.** It can happen that $IJ \nsubseteq I \cap J$. For example, take $R = \mathbb{Z}$, $I = (2)$, $J = (4)$. Then $IJ = (8)$, but $(2) \cap (4) = (lcm(2, 4)) = (4)$. However, if $I + J = R$ (in this case we say that $I$ and $J$ are coprime or comaximal) then $IJ = I + J$.

We consider one more way to create ideals. As usual, let $R$ be a commutative ring. Let $I$ and $J$ be ideals of $R$. Then the **ideal quotient** $(I : J)$ is by definition

\[
(I : J) = \{ r \in R : rJ \subseteq I \}.
\]

It is easy to verify that $(I : J)$ is an ideal of $R$. An important special case is when $I = 0$. In this case we have

\[
(0 : J) = \{ r \in R : rJ = 0 \}.
\]

This is called the **annihilator** of $J$, and is also written as

\[
\text{Ann}(J) = (0 : J).
\]

You will have a chance to work with this concept in the exercises.

**Residue class rings.** Assume that $R$ is a commutative ring, and that $I$ is an ideal of $R$. Regard $R$ and $I$ just as abelian groups under addition. Then $I$ is a subgroup of $R$, and since $R$ is abelian, $I$ is trivially a normal subgroup of $R$. We can therefore consider the quotient group

\[
R/I = \{ a + I : a \in R \}.
\]
Here,  

\[ a + I = \{ a + c : c \in I \}. \]

We recall that \( a + I \) is called a coset of \( I \) in \( R \), and the elements of \( a + I \) are called representatives for \( a + I \). If \( a' \in a + I \), then we have \( a' + I = a + I \) (if \( a' \in a + I \), then \( a' = a + c \) for some \( c \in I \), so that \( a' + I = a + c + I = a + I \) because \( c + I = I \) as \( c \in I \)). The addition on \( R/I \) is defined by  

\[ (a + I) + (b + I) = (a + b) + I \]

for \( a, b \in R \). It turns out that we can also define a multiplication on \( R/I \) so that \( R/I \) becomes a ring. We define  

\[ (a + I)(b + I) = ab + I \]

for \( a, b \in R \).

**Lemma 8.** The multiplication on \( R/I \) is well-defined, and \( R/I \) is a commutative ring with identity \( 1 + R \).

**Proof.** We need to prove that the multiplication does not depend on the choice of coset representatives. Let \( a_1, a_2, b_1, b_2 \in R \) be such that  

\[ a_1 + I = a_2 + I, \quad b_1 + I = b_2 + I. \]

We may write \( a_2 = a_1 + c \) and \( b_2 = b_1 + d \) for some \( c, d \in I \). Now  

\[
\begin{align*}
  a_2b_2 + I & = (a_1 + c)(b_1 + d) + I \\
  & = a_1b_1 + a_1d + cb_1 + cd + I \\
  & = a_1b_1 + I.
\end{align*}
\]

Here we have used \( a_1d + cb_1 + cd \in I \) because \( c, d \in I \) and \( I \) is an ideal. It follows that the multiplication is well-defined. It is now easy to check that \( R/I \) is a commutative ring with identity \( 1 + R \).

A coset \( r + I \in R/I \) is often denoted by \( \bar{r} \), i.e., one writes \( \bar{r} = r + I \). We refer to \( R/I \) as the **residue class ring** of \( R \) modulo \( I \) (or \( R \mod I \)). We have \( 1_{R/I} = \bar{1} = 1 + R \) and \( 0_{R/I} = \bar{0} = 0 + I = I \).

**Example.** Let \( n \) be a positive integer. Then \( n\mathbb{Z} = (n) \) is an ideal of \( \mathbb{Z} \). We can consider the residue class ring \( \mathbb{Z}/n\mathbb{Z} \). If \( n \) is a prime, then \( \mathbb{Z}/n\mathbb{Z} \) is a field. If \( n \) is not a prime, then \( \mathbb{Z}/n\mathbb{Z} \) has zero divisors, and thus not an integral domain. For example, suppose that \( n = 6 = 2 \cdot 3 \). Then  

\[
(2 + 6\mathbb{Z})(3 + 6\mathbb{Z}) = 6 + 6\mathbb{Z} = 6\mathbb{Z} = 0_{\mathbb{Z}/6\mathbb{Z}},
\]

which can also be written as  

\[
\bar{2} \cdot \bar{3} = \bar{6} = \bar{0}.
\]
Assume again that $R$ is a commutative ring and that $I$ is an ideal in $R$. Define

$$p : R \rightarrow R/I$$

by

$$p(r) = r + I = \bar{r}, \quad r \in I.$$ 

We verify that $f$ is a ring homomorphism as follows. First of all, we have $p(1) = 1 + R = 1_{R/I}$.

Next, let $r, s \in R$. Then

$$p(r + s) = r + s + I = (r + I) + (s + I) = p(r) + p(s).$$

And

$$p(r)p(s) = (r + I)(s + I) = rs + I = p(rs).$$

Thus, $p$ is a ring homomorphism. We refer to $p$ as the \textit{natural} or \textit{canonical} ring homomorphism from $R$ to $R/I$. Let $r \in R$. Then

$$r \in \ker(f) \iff p(r) = 0_{R/I} \iff r + I = I \iff r \in I.$$ 

That is,

$$\ker(p) = I.$$ 

**Proposition 9.** Let $R$ be a commutative ring, and let $I$ be a subset of $R$. Then $I$ is an ideal of $R$ if and only if $I$ is the kernel of a ring homomorphism from $R$ to another commutative ring.

**Proof.** Assume that $I$ is an ideal of $R$. Then $I = \ker(p)$, where $p : R \rightarrow R/I$ is the canonical homomorphism. Conversely, assume that $I$ is the kernel of a ring homomorphism $f : R \rightarrow S$, i.e., $I = \ker(f)$. Earlier, we proved that $\ker(f)$ is an ideal. Hence, $I = \ker(f)$ is an ideal. \hfill $\Box$

**Theorem 10** (Ring isomorphism theorem). Let $R$ and $S$ be commutative rings, and let $f : R \rightarrow S$ be a ring homomorphism. Then the function

$$\bar{f} : R/\ker(f) \xrightarrow{\sim} \text{im}(f)$$

defined by

$$\bar{f}(r + \ker(f)) = f(r), \quad r \in R$$

is a well-defined ring isomorphism.
Proof. To prove that \( f \) is well-defined we need to prove that the definition of \( \tilde{f} \) does not depend on the choice of coset representative. Let \( r_1, r_2 \in R \) and assume that \( r_1 + \ker(f) = r_2 + \ker(f) \). Then there exists \( k \in \ker(f) \) such that \( r_1 = r_2 + k \). We have

\[
\tilde{f}(r_1) = \tilde{f}(r_2 + k) = \tilde{f}(r_2) + \tilde{f}(k) = f(r_2) + f(k) = f(r_2) + 0 = f(r_2).
\]

It follows that \( \tilde{f} \) is well-defined. It is easy to verify that \( \tilde{f} \) is a ring homomorphism using that \( f \) is a ring homomorphism. To see that \( \tilde{f} \) is injective, assume that \( r \in R \) is such that \( f(r + \ker(f)) = 0 \). Then \( f(r) = 0 \), so that \( r \in \ker(f) \). This implies that \( r + \ker(f) = \ker(f) = 0_{R/\ker(f)} \). Hence, \( f \) is injective. To see that \( \tilde{f} \) is surjective, let \( s \in \text{im}(f) \). Then there exists \( r \in R \) such that \( f(r) = s \). We have \( \tilde{f}(r + \ker(f)) = f(r) = s \), which proves that \( \tilde{f} \) is surjective. Since \( f \) is injective and surjective, \( \tilde{f} \) is bijective and is thus a ring isomorphism.

You will have a chance to use this theorem in the exercises.

**Theorem 11 (Ideals in residue class rings).** Let \( R \) be a commutative ring, let \( I \) be an ideal of \( R \), and let \( p : R \to R/I \) be the canonical homomorphism. The function

\[
i : \{\text{ideals of } R \text{ containing } I\} \to \{\text{ideals of } R/I\}
\]

defined by

\[
i(J) = p(J) = J/I = \{r + I : r \in J\}
\]

for \( J \) an ideal of \( R \) containing \( I \) is a well-defined bijection. If \( Q \) is an ideal of \( R/I \), then

\[
J = p^{-1}(Q) = \{r \in R : p(r) \in Q\}
\]

is the ideal of \( R \) containing \( I \) such that \( i(J) = Q \).

Proof. It is easy to see that \( i \) is well-defined, i.e., if \( J \) is an ideal of \( R \) containing \( I \), then \( i(J) = J/I \) is an ideal of \( R/I \). To see that \( i \) is injective, let \( J_1 \) and \( J_2 \) be ideals of \( R \) containing \( I \) such that \( i(J_1) = i(J_2) \). We need to prove that \( J_1 = J_2 \). Let \( x \in J_1 \). Then since \( i(J_1) = i(J_2) \) we have \( x + I \in \{r + I : r \in J_1\} = \{r + I : r \in J_2\} \); therefore, there exists \( r \in J_2 \) such that \( x + I = r + I \). We have

\[
x \in x + I = r + I \subseteq r + J_2 = J_2.
\]

This proves \( J_1 \subseteq J_2 \); similarly, \( J_2 \subseteq J_1 \), so that \( J_1 = J_2 \) and \( i \) is injective. To prove that \( i \) is surjective, let \( Q \) be an ideal of \( R/I \) and define \( J = p^{-1}(Q) \). We leave it to the reader to verify that \( J \) is an ideal of \( R \). To verify that \( i(J) = Q \), first let \( r \in J \). By the definition of \( J \), \( p(r) \in Q \), i.e., \( r + J \in Q \). It follows that \( i(J) \subseteq Q \). Conversely, let \( s \in R \) be such that \( s + I \in Q \), i.e., \( p(s) \in Q \). Then by the definition of \( J \) we have \( s \in J \). Hence, \( s + I \in i(J) \), so that \( Q \subseteq i(J) \). We now have \( i(J) = Q \), proving that \( i \) is surjective.

**Example.** Let \( R = \mathbb{Z} \) and \( I = 6\mathbb{Z} = (6) \). By the theorem, the ideals of \( R/I = \mathbb{Z}/6\mathbb{Z} \) are in bijection
with the ideals of \( R = \mathbb{Z} \) that contain \( I = 6\mathbb{Z} \). An ideal \( (n) = n\mathbb{Z} \) contains \( (6) = 6\mathbb{Z} \) if and only if \( n \mid 6 \). The ideals that contain \( (6) = 6\mathbb{Z} \) are \((1) = \mathbb{Z}, (2) = 2\mathbb{Z}, (3) = 3\mathbb{Z}, \) and \((6) = 6\mathbb{Z} \). Thus, \( \mathbb{Z}/6\mathbb{Z} \) has 4 ideals which are:

\[
\begin{align*}
(\bar{1}) &= \{0, 1, 2, 3, 4, 5\}, \\
(\bar{2}) &= \{0, 2, 4\}, \\
(\bar{3}) &= \{0, 3\}, \\
(\bar{6}) &= \{0\}.
\end{align*}
\]

We can try to generalize the situation of the previous theorem. Suppose that \( R \) and \( S \) are commutative rings, and \( f : R \to S \) is a ring homomorphism. How can we relate the ideals of \( R \) and \( S \) via \( f \)? Assume first that \( J \) is an ideal of \( S \). We can then consider

\[ f^{-1}(J) = \{ r \in R : f(r) \in J \}. \]

We claim this is an ideal of \( R \). It is clear that \( f^{-1}(J) \) is non-empty and that \( f^{-1}(J) \) is closed under addition. Let \( r \in R \) and \( a \in f^{-1}(J) \). Then

\[ f(ra) = f(r)f(a) \in J \]

because \( f(a) \in J \) and \( J \) is an ideal. It follows that \( ra \in f^{-1}(J) \), completing the proof that \( f^{-1}(J) \) is an ideal of \( R \). The ideal \( f^{-1}(J) \) of \( R \) is called the \textit{contraction} of \( J \), and is denoted by

\[ J^c = f^{-1}(J). \]

Next, suppose that \( I \) is an ideal of \( R \). Can we naturally obtain an ideal of \( S \)? It turns out that there are examples when \( f(I) = \{ f(r) : r \in I \} \) is \textit{not} an ideal of \( S \). Instead, we consider the ideal generated by \( f(I) \), which is \( (f(I)) \). The ideal \( (f(I)) \) is called the \textit{extension} of \( I \) and is denoted by

\[ I^e = (f(I)). \]

The following facts hold.

\textbf{Lemma 12.} Let \( R \) and \( S \) be commutative rings, let \( f : R \to S \) be a ring homomorphism, let \( I \) be an ideal of \( R \), and let \( J \) be an ideal of \( S \). Then

\begin{itemize}
  \item[(i)] \( I \subseteq I^{ec} \).
  \item[(ii)] \( J^{ce} \subseteq J \).
  \item[(iii)] \( I^e = I^{ece} \).
  \item[(iv)] \( J^{ece} = J^c \).
\end{itemize}

\textit{Proof.} (i). Let \( r \in I \). Then \( f(r) \in I^e \) by the definition of \( I^e \). This implies that \( r \in f^{-1}(I^e) = I^{ec} \). Thus, \( I \subseteq I^{ec} \).
(ii). We have
\[ J^{ee} = (f(f^{-1}(J))) \subseteq J \]
(Note that since \( f(f^{-1}(J)) \subset J \) and \( J \) is an ideal, we have \( (f(f^{-1}(J))) \subset J \)).

(iii). By (i), \( I \subseteq I^{ec} \). This implies that \( I^e \subseteq I^{ece} \). By (ii) we have \( I^{ece} \subseteq I^e \). It follows that \( I^e = I^{ece} \). eq (iv). By (ii), \( J^{ec} \subset J \); hence, \( J^{ece} \subseteq J^e \). By (i) we have \( J^e \subseteq J^{ece} \). We now have \( J^{ece} = J^e \).

As a corollary of this lemma we see that there is bijection
\[ C_R = \{ \text{all contractions of ideals of } S \} \leftrightarrow E_S = \{ \text{all extensions of ideals of } R \} \]
defined by
\[ I \mapsto I^e, \quad \text{for } I \in C_R, \]
\[ J^e \leftrightarrow J, \quad \text{for } J \in E_S. \]

3 Prime ideals and maximal ideals

Let \( R \) be a commutative ring and let \( M \) be an ideal of \( R \). We say that \( M \) is a maximal ideal of \( R \) if

(i) \( M \) is a proper ideal of \( R \), i.e., \( M \subsetneq R \).

(ii) If \( I \) is an ideal of \( R \) such that \( M \subseteq I \subseteq R \), then \( I = M \) or \( I = R \).

Lemma 13. Let \( R \) be a commutative ring. Then \( R \) is a field if and only if \( R \) has exactly two distinct ideals, namely \( 0 \) and \( R \).

Proof. Assume that \( R \) is a field. Of course, \( 0 \) and \( R \) are ideals of \( R \). Since \( F \) is a field we have \( 0 \neq 1 \) (this is part of the definition of a field). This implies that \( 0 \neq R \) so that \( R \) has at least two distinct ideals. Let \( I \) be another ideal of \( R \); we claim that \( I = 0 \) or \( I = R \). Assume that \( I \neq 0 \). Then there exists \( x \in I \) such that \( x \neq 0 \). Since \( R \) is a field there exists \( r \in R \) such that \( rx = 1 \). Now \( rx = 1 \in I \) because \( I \) is an ideal. Since \( 1 \in I \) every element of \( R \) is in \( I \), i.e., \( I = R \).

Now assume that \( R \) has exactly two distinct ideals. Let \( x \in R, x \neq 0 \). Consider the ideal \( (x) \). Since \( x \) is non-zero, \( (x) \) must be \( R \). Therefore, \( 1 \in (x) \). Hence, there exists \( r \in R \) such that \( rx = 1 \). This implies that \( R \) is a field.

Lemma 14. Let \( R \) be a commutative ring and let \( M \) be an ideal of \( R \). Then \( M \) is a maximal ideal of \( R \) if and only if \( R/M \) is a field.

Proof. By Theorem 11 applied to \( R \) and \( M \), there is a bijection
\[ \{ \text{ideals } J \text{ of } R \text{ such that } M \subseteq J \subseteq R \} \leftrightarrow \{ \text{ideals of } R/M \}. \]
Therefore,

\[ M \text{ is a maximal ideal } \iff \text{ the first set has two elements} \]
\[ \iff \text{ the second set has two elements} \]
\[ \iff R/M \text{ is a field (by Lemma 13).} \]

This completes the proof. \( \Box \)

**Example.** The maximal ideals of \( \mathbb{Z} \) are the ideals \((m) = m\mathbb{Z}\) where \( m \) is a prime.

**Proof.** Let \( M \) be an ideal of \( \mathbb{Z} \). Since \( \mathbb{Z} \) is a PID, we have \( M = (m) = m\mathbb{Z} \) for some \( m \in \mathbb{Z} \). Now \( M \) is a maximal ideal of \( \mathbb{Z} \) \( \iff \mathbb{Z}/M = \mathbb{Z}/m\mathbb{Z} \) is a field (Lemma 13) \( \iff m \) is a prime (elementary number theory).

This completes the proof. \( \Box \)

**Example.** Let \( K \) be a field and let \( f \in K[X] \) be non-zero and not a unit, i.e., not in \( K^* = K - 0 \). Let \( R = K[X] \) and \( M = (f) \). Then \( M \) is a maximal ideal of \( R \) if and only if \( f \) is irreducible.

**Proof.** Assume that \( M \) is maximal; we need to show that \( f \) is irreducible. Assume that \( f = pq \) with \( p, q \in R \). We need to prove that \( p \) is a unit or \( q \) is a unit. Assume that \( p \) is not a unit. We have \( M = (f) \subseteq (p) \subseteq R \). Since \( p \) is not a unit we have \( (p) \not\subseteq R \). Since \( M \) is maximal this implies that \( (p) = M = (f) \). Let \( g \in R \) be such that \( p = fg \). We now have

\[ f = pq = fgq. \]

As \( R \) is an integral domain this yields \( 1 = gq \) so that \( q \) is a unit. Hence, \( f \) is irreducible. Assume that \( f \) is irreducible; we need to prove that \( M \) is maximal. Assume that \( I \) is an ideal of \( R \) such that \( M \subseteq I \subseteq R \). Since \( R \) is a PID there exists \( g \in R \) such that \( I = (g) \). Now \( (f) \subseteq (g) \); hence, there exists \( h \in R \) such that \( f = gh \). Since \( f \) is irreducible either \( g \) is a unit or \( h \) is a unit. If \( g \) is a unit, then \( I = R \); if \( h \) is a unit, then \( I = M \). It follows that \( M \) is maximal. \( \Box \)

**Example.** Let \( K \) be a field and let \( X_1, \ldots, X_n \) be indeterminates. Let \( a_1, \ldots, a_n \in K \). Then \( M = (X_1 - a_1, \ldots, X_n - a_n) \) is a maximal ideal of \( R = K[X_1, \ldots, X_n] \).

**Proof.** Let \( p : R \to R/M \) be the canonical map. Let \( t \) be the restriction of \( p \) to \( K \), so that \( t \) is map \( t : K \to R/M \). We claim that \( t \) is a ring isomorphism. Since \( t \) is the restriction of \( p \), \( t \) is a ring homomorphism. To prove that \( t \) is injective we prove that \( \ker(t) = 0 \). Let \( a \in \ker(t) \). Then \( t(a) = 0 \), i.e., \( a + M = M \). This implies that \( a \in M \). Hence, there exist \( p_1, \ldots, p_n \in R \) such that

\[ a = p_1(X_1 - a_1) + \cdots + p_n(X_n - a_n). \]
Evaluating both sides at \((a_1, \ldots, a_n)\), we obtain \(a = 0\). Thus, \(\ker(t) = 0\) and \(t\) is injective. To prove that \(t\) is surjective we note first that since \(X_i - a_i \in M\) we have for \(i = 1, \ldots, n\)

\[
X_i + M = a_i + M \\
\bar{X}_i = \bar{a}_i.
\]

Now let \(g \in R\). Write

\[
g = \sum_{(i_1, \ldots, i_n) \in \Lambda} c_{i_1, \ldots, i_n} X_1^{i_1} \cdots X_n^{i_n}.
\]

Using that \(\bar{X}_i = \bar{a}_i\) for \(i = 1, \ldots, n\), we have

\[
\bar{g} = \sum_{(i_1, \ldots, i_n) \in \Lambda} \bar{c}_{i_1, \ldots, i_n} \bar{X}_1^{i_1} \cdots \bar{X}_n^{i_n}
\]

\[
= \sum_{(i_1, \ldots, i_n) \in \Lambda} \bar{c}_{i_1, \ldots, i_n} \bar{a}_1^{i_1} \cdots \bar{a}_n^{i_n}
\]

\[
= g(a_1, \ldots, a_n)
\]

\[
= t(g(a_1, \ldots, a_n)).
\]

Since every element of \(R/M\) is of the form \(\bar{g}\) for some \(g \in R\), we see that \(t\) is surjective. Since \(t\) is an isomorphism of rings, and since \(K\) is a field, \(R/M\) is also a field. By Lemma 14 the ideal \(M\) is maximal.

If the notation is as in the last example, and if \(K\) is algebraically closed, then it turns out that every maximal ideal of \(R = K[X_1, \ldots, X_n]\) is an \(M\) as in the example, i.e., \(M = (X_1 - a_1, \ldots, X_n - a_n)\) for some \(a_1, \ldots, a_n \in K\). This is a famous theorem called the **Hilbert Nullstellensatz** (zeros theorem).

**Lemma 15.** Let \(R\) be a commutative ring and let \(M\) be an ideal of \(R\) such that \(I \subseteq M \subseteq R\). Then \(M\) is a maximal ideal of \(R\) if and only if \(M/I\) is a maximal ideal of \(R/I\).

**Proof.** Using Lemma 13 we have:

\[
M\text{ maximal ideal of } R \iff R/M\text{ is as field} \quad \text{(Lemma 13)}
\]

\[
\iff (R/I)/(M/I) \cong R/M \text{ is a field}
\]

\[
\iff M/I \text{ is a maximal ideal of } R/I \quad \text{(Lemma 13)}.
\]

This completes the proof.

One can also prove the existence of maximal ideals using Zorn’s Lemma. Let \(X\) be a non-empty set, let \(\leq\) be a relation on \(X\). We say that \(\leq\) is a **partial order** if

(i) \(\leq\) is **reflexive**: if \(x \in X\), then \(x \leq x\).

(ii) \(\leq\) is **antisymmetric**: if \(x, y \in X\) and \(x \leq y\) and \(y \leq x\), then \(x = y\).

14
(iii) \( \leq \) is **transitive**: if \( x, y, z \in X \) and \( x \leq y \) and \( y \leq z \), then \( x \leq z \).

Assume that \( X \) is partially ordered with respect to \( \leq \). Let \( Y \subseteq X \) be a subset of \( X \). We say that \( Y \) is **totally ordered** if for all \( x, y \in Y \) we have \( x \leq y \) or \( y \leq x \). We say that \( Y \) has an **upper bound** in \( X \) if there exists \( x \in X \) such that \( y \leq x \) for \( y \in Y \). Finally, let \( m \in X \). We say that \( m \) is a **maximal element** of \( X \) if there does not exist \( x \in X \) such that \( m \leq x \) and \( x \neq m \); this is equivalent to for all \( x \in X \), if \( m \leq x \), then \( x = m \).

**Theorem 16** (Zorn’s Lemma). Let \( X \) be a non-empty set that is partial ordered with respect to the relation \( \leq \). If every totally ordered non-empty subset \( Y \) of \( X \) has an upper bound in \( X \), then \( X \) contains a maximal element.

**Proof.** This is equivalent to the axiom of choice of set theory. \( \square \)

**Proposition 17.** Let \( R \) be a commutative ring, and let \( I \) be a proper ideal of \( R \), i.e., \( I \subseteq R \). Then there exists a maximal ideal \( M \) of \( R \) such that \( I \subseteq M \subseteq R \).

**Proof.** Let \( X \) be the set of all proper ideals \( J \) of \( R \) such that \( I \subseteq J \subseteq R \). The set \( X \) contains \( I \) and is thus non-empty. We will use the partial order \( \subseteq \) on \( X \). Let \( Y \) be a totally ordered subset of \( X \). Let \( B \) be the union of all the elements of \( Y \). We claim that \( B \in X \). Since every element of \( Y \) contains \( I \), the set \( B \) certainly contains \( I \) and is thus non-empty. Let \( b_1, b_2 \in B \). There exist \( J_1, J_2 \in Y \) such that \( b_1 \in J_1 \) and \( b_2 \in J_2 \). Since \( Y \) is totally ordered we have \( J_1 \subseteq J_2 \) or \( J_2 \subseteq J_1 \). Assume that \( J_1 \subseteq J_2 \). Then \( b_1, b_2 \in J_2 \), and hence \( b_1 + b_2 \in J_2 \subseteq B \) since \( J_2 \) is an ideal. Similarly, if \( J_2 \subseteq J_1 \), then \( b_1 + b_2 \in B \). Next, let \( r \in R \) and \( b \in B \). There exists \( J \in Y \) such that \( b \in J \). Since \( J \) is an ideal we have \( rb \in J \subseteq B \). It follows that \( B \) is an ideal. Since \( I \subseteq B \), \( B \in X \). Also, by construction we have \( J \subseteq B \) for all \( J \in Y \); hence, \( B \) is an upper bound for \( Y \). By Zorn’s Lemma, \( X \) contains a maximal element \( M \). The element \( M \) is a maximal ideal that contains \( I \). \( \square \)

Let \( R \) be a commutative ring, and let \( P \) be an ideal of \( R \). We say that \( P \) is a **prime ideal** of \( R \) if

(i) \( P \) is a proper ideal of \( R \), i.e., \( P \nsubseteq R \).

(ii) If \( a, b \in R \) and \( ab \in P \), then \( a \in P \) or \( b \in P \).

**Example.** Let \( R \) be an integral domain. Then \( 0 \) is a prime ideal of \( R \).

We will consider non-trivial examples of prime ideals after a number of lemmas.

**Lemma 18.** Let \( R \) be a commutative ring and let \( P \) be an ideal of \( R \). Then \( P \) is a prime ideal of \( R \) if and only if \( R/P \) is an integral domain.

**Proof.** Assume that \( P \) is a prime ideal. Since \( P \) is proper, \( R/P \neq 0 \). Assume that \( a, b \in R \) are such that \( ab = (a + P)(b + P) = P \). Then \( ab + P = P \) so that \( ab \in P \). Since \( P \) is a prime ideal we have \( a \in P \) or \( b \in P \); this is equivalent to \( a = 0 \) or \( b = 0 \). Hence, \( R/P \) is an integral domain. Next, assume that \( R/P \) is an integral domain. Then \( R/P \neq 0 \); hence, \( P \) is proper. Assume that \( a, b \in R \) are such that \( ab \in P \). Then \( ab = 0 \) in \( R/P \). Since \( R/P \) is an integral domain we have \( a = 0 \) or \( b = 0 \). This means that \( a \in P \) or \( b \in P \). Hence, \( P \) is a prime ideal. \( \square \)
Lemma 19. Let $R$ be a commutative ring and let $I$ be an ideal of $R$. Let $P$ be an ideal of $R$ such that $I \subseteq P \subseteq R$. Then $P$ is a prime ideal of $R$ if and only if $P/I$ is a prime ideal of $R/I$.

Proof. Using Lemma 18) we have:

\[
P \text{ is a prime ideal of } R \iff R/P \text{ is an integral domain } \iff (R/I)/(P/I) \cong R/P \text{ is an integral domain } \iff P/I \text{ is a prime ideal of } R/I.
\]

This completes the proof.

Lemma 20. Let $R$ be a commutative ring, and let $M$ be a maximal ideal of $R$. Then $M$ is a prime ideal of $R$.

Proof. We have

\[
M \text{ is a maximal ideal of } R \implies R/M \text{ is a field } \implies R/M \text{ is an integral domain } \implies M \text{ is a prime ideal}.
\]

This completes the proof.

We will now study maximal and prime ideals in the context of PIDs. Let $R$ be an integral domain. Let $p \in R$ be non-zero and not a unit. We say that $p$ is a prime element of $R$ if the following holds: if $a, b \in R$ and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Lemma 21. Let $R$ be an integral domain. Let $p \in R$ and assume that $p$ is non-zero and not a unit. Then

(i) If $p$ is prime, then $p$ is irreducible.
(ii) $p$ is prime if and only if $(p)$ is a prime ideal.

Proof. (i). Let $p$ be prime. Suppose that $p = ab$; to prove that $p$ is irreducible we need to prove that $a$ is a unit or $b$ is a unit. Since $p = ab$ we have $p \mid ab$. Since $p$ is prime we obtain $p \mid a$ or $p \mid b$. Assume that $p \mid a$. Then $pc = a$ for some $c \in R$. We now have:

\[
pc = a \implies abc = a \implies bc = 1.
\]

Here, the last step follows because $R$ is an integral domain. It follows that $b$ is a unit. Similarly, if $p \mid b$, then $a$ is a unit. It follows that $p$ is irreducible.

(ii). Assume that $p$ is prime. Let $a, b \in R$ be such that $ab \in (p)$. Then $p \mid ab$. Since $p$ is prime we have $p \mid a$ or $p \mid b$, i.e., $a \in (p)$ or $b \in (p)$. Assume that $(p)$ is prime. Let $a, b \in R$ and assume that $p \mid ab$. Then $ab \in (p)$. Since $(p)$ is prime we have $a \in (p)$ or $b \in (p)$. This means that $p \mid a$ or $p \mid b$. 

\]
Lemma 22. Let $R$ be a PID. Let $p \in R$ be non-zero and not a unit. Then the following are equivalent:

(i) $(p)$ is a maximal ideal of $R$.

(ii) $(p)$ is a non-zero prime ideal of $R$.

(iii) $p$ is a prime element of $R$.

(iv) $p$ is an irreducible element of $R$.

Proof. (i) $\implies$ (ii). This follows from Lemma 20.

(ii) $\implies$ (iii). This follows from Lemma 21.

(iii) $\implies$ (iv). This follows from Lemma 21.

(iv) $\implies$ (i). Assume that $p$ is an irreducible element of $R$. Assume that $I$ is an ideal of $R$ such that $(p) \subseteq I \subseteq R$. Since $R$ is a PID, there exists $a \in R$ such that $I = (a)$. Now $(p) \subseteq (a)$; hence, there exists $b \in R$ such that $p = ab$. Since $p$ is irreducible either $a$ is a unit or $b$ is a unit. If $a$ is a unit, then $(a) = R$; if $b$ is a unit, then $(a) = (p)$. It follows that $R$ is maximal. \qed

Let $R$ be a commutative ring. We will write

$$\text{spec}(R) = \text{the set of all prime ideals of } R,$$

$$\text{m-spec}(R) = \text{the set of all maximal ideals of } R.$$

The set $\text{spec}(R)$ is called the **spectrum** of $R$. We have

$$\text{m-spec}(R) \subseteq \text{spec}(R).$$

From the lemmas, we see that:

$$R \text{ is a PID } \implies \text{m-spec}(R) = \text{spec}(R) - 0.$$

There are other important rings for which this equality holds, e.g., the ring of integers in an algebraic number field (examples of this are $\mathbb{Z}$ and $\mathbb{Z}[\omega]$). But there are also many important rings for which this equality does not hold.

**Example.** Let $K$ be a field and let $X_1, \ldots, X_n$ be indeterminates, and let $R = K[X_1, \ldots, X_n]$. Consider the ideals

$$(X_1) \subseteq (X_1, X_2) \subseteq (X_1, X_2, X_3) \subseteq \cdots \subseteq (X_1, \ldots, X_n)$$

of $R$. These ideals are mutually distinct, $(X_1), (X_1, X_2), \ldots, (X_1, \ldots, X_{n-1})$ are prime, and $(X_1, \ldots, X_n)$ is maximal.

**Proof.** Let $k \in \{1, \ldots, n\}$. Then

$$R/(X_1, \ldots, X_k) = K[X_1, \ldots, X_n]/(X_1, \ldots, X_k) \cong K[X_{k+1}, \ldots, X_n].$$
It follows that $R/(X_1, \ldots, X_k)$ is an integral domain; also, if $k = n$, then $R/(X_1, \ldots, X_k)$ is a field. This proves that $(X_1), (X_1, X_2), \ldots, (X_1, \ldots, X_{n-1})$ are prime, and $(X_1, \ldots, X_n)$ is maximal. The proof that these ideals are mutually distinct is left to the reader.

It turns out that all these examples of $R$, (PIRs, rings of algebraic integers, and polynomial rings) are examples of what are called Noetherian rings. As the course progresses we will mainly study Noetherian rings. To define this concept we need some definitions. Let $R$ be a commutative ring. We say that $R$ satisfies the ascending chain condition on ideals

\[
I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots
\]

there exists $n \in \mathbb{N}$ such that

\[
I_n = I_{n+1} = I_{n+2} = \cdots,
\]

i.e., the sequence becomes stationary. We say that $R$ satisfies the maximal condition on ideals if any non-empty set $X$ of ideals of $R$ contains a maximal element $I$, i.e., for all $J \in X$, if $I \subseteq J$, then $I = J$.

**Lemma 23.** Let $R$ be a commutative ring. Then the following are equivalent.

(i) $R$ satisfies the ascending chain condition on ideals.

(ii) $R$ satisfies the maximal condition on ideals.

(iii) Every ideal of $R$ is finitely generated, i.e., if $I$ is an ideal of $R$, then there exist $r_1, \ldots, r_n \in R$ such that $I = (r_1, \ldots, r_n)$.

**Proof.** (i) $\implies$ (ii) Assume that $R$ satisfies the ascending chain condition on ideals, but does not satisfy the maximal condition on ideals; we will obtain a contradiction. Since $R$ does not satisfy the maximal condition there exists be a non-empty set $X$ of ideals of $R$ which does not have a maximal element. Let $I_1 \in X$. Since $I_1$ is not maximal, there exists an ideal $I_2 \in X$ such that $I_1 \subsetneq I_2$. Similarly, there exists $I_3 \in X$ such that $I_2 \subsetneq I_3$. Continuing, we obtain a chain of ideals

\[
I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots.
\]

This contradicts the ascending chain condition.

(ii) $\implies$ (i) Assume that $R$ satisfies the maximal condition on ideals. Let

\[
I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots
\]

be a sequence of ideals in $R$. Let $X = \{I_i : i \in \mathbb{N}\}$. This set has a maximal element $I_n$. Since $I_n$ is a maximal element of $X$ and since $I_n \subseteq I_m$ for $m \geq n$, we must have $I_m = I_n$ for $m \geq n$. It follows that $R$ satisfies the ascending chain condition on ideals.

(i) $\implies$ (iii) Assume that $R$ satisfies the ascending chain condition on ideals, but there exists a ideal $I$ of $R$ that is not finitely generated; we will obtain a contradiction. Let $x_1 \in I$. Since $I$ is not finitely generated we have $(x_1) \not\subseteq I$. Hence, there exists $x_2 \in I - (x_1)$. We have $(x_1) \not\subseteq (x_1, x_2)$. 

18
Since $I$ is not finitely generated, $(x_1, x_2) \subseteq I$; hence there exists $x_3 \in I - (x_1, x_2)$. We have $(x_1, x_2) \subsetneq (x_1, x_2, x_3)$. Continuing, we obtain a sequence of ideals of the following form:

$$(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$$

This contradicts the ascending chain condition.

(iii) $\implies$ (i) Assume that every ideal of $R$ is finitely generated. Let

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

be a sequence of ideals in $R$. Let $I = \bigcup_{i=1}^{\infty} I_i$. Using that the above sequence is ascending it is straightforward to verify that $I$ is an ideal of $R$. The ideal $I$ is finitely generated; let $r_1, \ldots, r_n$ be such that $I = (r_1, \ldots, r_n)$. Now each $r_i$ is contained in some $I_m$; it follows that if $m \geq \max(m_1, \ldots, m_n)$, then $r_1, \ldots, r_n \in I_m$. This implies that $I = (r_1, \ldots, r_n) \subseteq I_m$ for $m \geq \max(m_1, \ldots, m_n)$. Since $I_m \subseteq I$ for all $m \in \mathbb{N}$ we obtain $I_m = I$ for all $m \geq \max(m_1, \ldots, m_n)$ so that our ascending chain of ideals becomes stationary.

We will say that a commutative ring $R$ is **Noetherian** if it satisfies the three equivalent conditions from Lemma 23. It is evident that a PID is Noetherian because every ideal in a PID is generated by a single element. Also, it is another famous theorem of Hilbert, call the **Hilbert basis theorem**, that $R[X_1, \ldots, X_n]$ is Noetherian if $R$ is Noetherian. In particular, if $K$ is a field and $X_1, \ldots, X_n$ are indeterminates, then $K[X_1, \ldots, X_n]$ is Noetherian.

**Lemma 24.** Let $R$ be an integral domain and let $I$ be a principal ideal of $R$. Assume that $I \neq 0$. Let $a, b \in R$. Then $a$ and $b$ are both generators of $I$ if and only if there exists a unit $r \in R$ such that $a = rb$.

**Proof.** Assume first that $a$ and $b$ are both generators of $I$. Since $(a) = (b)$ there exist $r, s \in R$ such that $a = rb$ and $b = sa$. Now $a = rb = rsa$, so that $a(1 - rs) = 0$. Since $R$ is an integral domain we have $a = 0$ or $1 - rs = 0$. We cannot have $a = 0$ because $I \neq 0$. Hence, $1 - rs = 0$, i.e., $1 = rs$. Therefore, $r$ is a unit.

Next, assume that there exists a unit $r \in R$ such that $a = rb$. We then have $(a) \subseteq (b)$. Since $r^{-1}a = b$, we also have $(b) \subseteq (a)$. Hence, $(a) = (b)$, and $a$ and $b$ are both generators of $I$. 

**Theorem 25.** If $R$ is a PID then $R$ is a UFD.

**Proof.** We first prove that every non-zero, non-unit is the product of irreducibles. Assume this does not hold; we will obtain a contradiction. Let $X$ be the set of all ideals $(a)$ of $R$ such that $a$ is not the product of irreducibles. The set $X$ is non-empty by our assumption. Since $R$ is a PID, $R$ is Noetherian; by Lemma 23 the set $X$ has a maximal element $(b)$. Consider $b$. Obviously, $b$ is not irreducible. Hence, there exist $c, d \in R$ such that $b = cd$ and $c$ and $d$ are not units. This implies that

$$(b) \subsetneq (c) \subseteq R, \quad (b) \subsetneq (d) \subseteq R.$$
By the maximality of \((b)\) we must have \((c) \notin X\) and \((d) \notin X\). By the definition of \(X\) this implies that \(c\) and \(d\) be written as the product of irreducibles. Hence, \(b\) is a product of irreducibles, a contradiction. Next, we need to prove that every non-zero, non-unit is the product of irreducible in a unique way (see the definition of a UFD). We will leave this to the reader. (Use that since \(R\) is a PID every irreducible element of \(R\) is prime (see Lemma 23)).

Let \(R\) be a commutative ring, and let \(S\) be a subset of \(R\). We say that \(S\) is \textit{multiplicatively closed} or is a \textit{multiplicative subset} if:

(i) \(1 \in S\);
(ii) If \(s_1, s_2 \in S\), then \(s_1, s_2 \in S\).

**Example.** Let \(R\) be a commutative ring and let \(s \in R\) be non-zero. Then \(S = \{s^n : n \in \mathbb{N}_0\}\) is multiplicatively closed.

**Example.** Let \(R\) be a commutative ring and let \(P\) be a prime ideal of \(R\). Define \(S = R - P\). Then \(S\) is a multiplicatively closed subset of \(R\).

**Proof.** Since \(P \subseteq R\) we have \(1 \notin P\) so that \(1 \in S\). Let \(s_1, s_2 \in S\). Then \(s_1s_2 \in S\) because otherwise \(s_1s_2 \in P\) which implies \(s_1 \in P\) or \(s_2 \in P\), a contradiction.

**Theorem 26.** Let \(R\) be a commutative ring, let \(I\) be an ideal of \(R\), and let \(S\) be a multiplicatively closed subset of \(R\). Assume that \(I \cap S = \emptyset\). Let

\[
\Psi = \{J : J \text{ is an ideal of } R \text{ such that } I \subseteq J \text{ and } J \cap S = \emptyset\}.
\]

Order \(\Psi\) be inclusion. Then \(\Psi\) has a maximal element \(P\), and \(P\) is a prime ideal.

**Proof.** We will use Zorn’s Lemma applied to \(\Psi\). The set \(\Psi\) is non-empty because \(I \in \Psi\). Let \(Y\) be a totally ordered subset of \(\Psi\); we must show that \(Y\) has an upper bound in \(\Psi\). Let \(B\) be the union of all the elements in \(Y\). Since \(Y\) is totally ordered, \(B\) is an ideal of \(R\) (see the proof of Proposition 17). Also, it is clear that \(I \subseteq B\) and \(B \cap S = \emptyset\). Hence, \(B\) is contained in \(\Psi\). Thus \(B\) is an upper bound for \(Y\) in \(\Psi\). By Zorn’s Lemma, \(\Psi\) contains a maximal element \(P\). Next, we prove that \(P\) is a prime ideal. Let \(a, b \in R\), and assume that \(ab \in P\). Assume further that \(a \notin P\) and \(b \notin P\); we will obtain a contradiction. Consider the ideal \(P + (a)\). We have

\[
I \subseteq P \subseteq P + (a).
\]

By the maximality of \(P\) in \(\Psi\) we cannot have \(P + (a) \in \Psi\); therefore, \((P + (a)) \cap S = \emptyset\). This implies that there exist \(x \in P\), \(r \in R\), and \(s \in S\) such that

\[
s = x + ra.
\]

Similarly, there exist \(x' \in P\), \(r' \in R\), and \(s' \in S\) such that

\[
s' = x' + r'b.
\]
Now
\[ ss' = (x + ra)(x' + r'b) = xx' + xr'b + rax' + rr'ab. \]
Since \(x, x' \in P\) and \(ab \in P\) we have \(xx' + xr'b + rax' + rr'ab \in P\). Hence, \(ss' \in S \cap P\). This contradicts \(S \cap P = \emptyset\), and completes the proof. \(\square\)

**Proposition 27.** Let \(R\) be a commutative ring and let \(I\) be an ideal of \(R\). let
\[
\text{Var}(I) = \{P : \in \text{Spec}(R) : I \subseteq P\} \quad (\text{the variety of } I).
\]
Then
\[
\sqrt{I} = \bigcap_{P \in \text{Var}(I)} P.
\]

**Proof.** Let \(a \in \sqrt{I}\). There exists \(n \in \mathbb{N}\) such that \(a^n \in I\). Let \(P \in \text{Var}(I)\). Since \(I \subseteq P\), we have \(a^n \in P\). Since \(a\) is prime, \(a \in P\). It follows that \(\sqrt{I} \subseteq \bigcap_{P \in \text{Var}(I)} P\). Conversely, let \(a \in \bigcap_{P \in \text{Var}(I)} P\). Assume that \(a \notin \sqrt{I}\); we will obtain a contradiction. Let \(S = \{a^n : n \in \mathbb{N}_0\}\). Since \(a \notin \sqrt{I}\) we have \(S \cap I = \emptyset\). By Theorem 26, there exists a prime ideal \(Q\) such that \(I \subseteq Q\) and \(Q \cap S = \emptyset\). We have \(Q \in \text{Var}(I)\). By assumption, \(a \in \bigcap_{P \in \text{Var}(I)} P\); hence, \(a \in Q\). This contradicts \(Q \cap S = \emptyset\). \(\square\)

With the notation of Proposition 27, we recall that \(\sqrt{I}\) is called the **radical** of \(I\). It is also sometimes written as \(\text{Rad}(I)\).

**Corollary 28.** Let \(R\) be a commutative ring. We have
\[
\sqrt{0} = \bigcap_{P \in \text{Spec}(R)} P.
\]

**Proof.** This follows immediately from Proposition 27. \(\square\)

With the notation of Corollary 28, \(\sqrt{0}\) is the ideal of all **nilpotent** elements of \(R\), i.e., \(\sqrt{0}\) is the ideal of all \(x \in R\) for which there exists \(n \in \mathbb{N}\) such that \(x^n = 0\).

**Theorem 29.** Let \(R\) be a commutative ring, and let \(I\) be a proper ideal of \(R\), i.e., \(I \subsetneq R\). Then \(\text{Var}(I)\) contains a minimal element with respect to inclusion, i.e., there exists \(P \in \text{Var}(I)\) such that if \(P' \in \text{Var}(I)\) is such that \(I \subseteq P' \subseteq P\), then \(P' = P\).

**Proof.** By Proposition 17 there exists a maximal ideal \(M\) such that \(I \subset M\). It follows that \(\text{Var}(I)\) is non-empty (because any maximal ideal is a prime ideal by Lemma 20). We define a partial order \(\leq\) on \(\text{Var}(I)\) by \(P_1 \leq P_2\) if and only if \(P_2 \subseteq P_1\). Let \(Y\) be a totally ordered subset of \(\text{Var}(I)\). Let \(Q\) be the intersection of all the elements of \(Y\). We claim that \(Q \in \text{Var}(I)\). Since \(Q\) is the intersection of ideals \(Q\) is an ideal of \(R\). It is clear that \(I \subseteq Q\). Also, \(Q\) is a proper ideal of \(R\) because \(Q\) is the intersection of proper ideals. To complete the argument that \(Q \in \text{Var}(I)\) we need to prove that \(R\) is prime. Let \(a, b \in R\) be such that \(ab \in Q\). Assume that \(a \notin Q\); we will prove that \(b \in Q\). Let \(P \in Y\); to prove that \(b \in Q\) we need to prove that \(b \in P\). Since \(a \notin Q\), there exists \(P_1 \in Y\) such
that $a \notin P_1$. Now $ab \in Q \subseteq P_1$. Since $P_1$ is prime, we have $a \in P_1$ or $b \in P_1$; as $a \notin P_1$, we obtain $b \in P_1$. Recalling that $Y$ is totally ordered, we have either $P_1 \subseteq P$ or $P \subseteq P_1$. If $P_1 \subseteq P$, then $b \in P_1 \subseteq P$, i.e., $b \in P$. Assume $P \subseteq P_1$. Then $ab \in Q \subseteq P \subseteq P_1$, so that $a \in P$ or $b \in P$. If $a \in P$, then $a \in P_1$, a contradiction. Hence, $b \in P$. We have proven that $b \in P$ for all $P \in Y$. This implies that $b \in Q$. Hence, $Q$ is a prime ideal. Thus, $Q \in \text{Var}(I)$. Clearly, $Q$ is an upper bound for $Y$. We may now apply Zorn’s Lemma to conclude that \( \text{Var}(I) \) has a maximal element $P$. By the maximality of $P$, if $P_1 \subseteq P$, then $b \in P_1 \subseteq P$, i.e., $b \in P$. Assume $P \subseteq P_1$. Then $ab \in Q \subseteq P \subseteq P_1$, so that $a \in P$ or $b \in P$. If $a \in P$, then $a \in P_1$, a contradiction. Hence, $b \in P$. We have proven that $b \in P$ for all $P \in Y$. This implies that $b \in Q$. Hence, $Q$ is a prime ideal. Thus, $Q \in \text{Var}(I)$. Clearly, $Q$ is an upper bound for $Y$. We may now apply Zorn’s Lemma to conclude that \( \text{Var}(I) \) has a maximal element $P$. By the maximality of $P$, if $P_1 \subseteq P$, then $b \in P_1 \subseteq P$, i.e., $b \in P$. Assume $P \subseteq P_1$. Then $ab \in Q \subseteq P \subseteq P_1$, so that $a \in P$ or $b \in P$. If $a \in P$, then $a \in P_1$, a contradiction. Hence, $b \in P$. We have proven that $b \in P$ for all $P \in Y$. This completes the proof.

Let $R$ be a commutative ring, and let $I$ be a proper ideal of $R$. If $P$ is as in the statement of Theorem 29 then we say that $P$ is a **minimal prime ideal of** $I$, or a **minimal prime ideal containing** $I$. If $R \neq 0$, so that $0$ is a prime ideal of $R$, then we refer to a minimal prime ideal of $0$ as a minimal prime ideal.

**Corollary 30.** Let $R$ be a commutative ring, and let $I$ be a proper ideal of $R$. Then

$$\sqrt{I} = \bigcap_{P \in \text{min}(I)} P$$

where \( \text{min}(I) \) is the set of all minimal prime ideals of $P$.

**Proof.** By Proposition 27 we have

$$\sqrt{I} = \bigcap_{P \in \text{Var}(I)} P.$$  

Since $\text{min}(I) \subseteq \text{Var}(I)$, we have

$$\bigcap_{P \in \text{Var}(I)} P \subseteq \bigcap_{P \in \text{min}(I)} P.$$  

Let $x \in \bigcap_{P \in \text{min}(I)} P$. We claim that $x \in \bigcap_{P \in \text{Var}(I)} P$. Let $P \in \text{Var}(I)$. By an exercise there exists a minimal prime ideal $P'$ of $I$ such that $I \subseteq P' \subseteq P$. Since $x \in \bigcap_{P \in \text{min}(I)} P$ we have $x \in P'$. As $P' \subseteq P$ we get $x \in P$. It follows that $x \in \bigcap_{P \in \text{Var}(I)} P$ so that

$$\bigcap_{P \in \text{min}(I)} P \subseteq \bigcap_{P \in \text{Var}(I)} P.$$  

This completes the proof.

**Lemma 31.** Let $R$ be a commutative ring, and let $P$ be a prime ideal of $R$. Let $I_1, \ldots, I_n$ be ideals of $R$. Then the following are equivalent:

1. For some $j \in \{1, \ldots, n\}$ we have $I_j \subseteq P$.
2. $\bigcap_{i=1}^n I_i \subseteq P$.
3. $\prod_{i=1}^n I_i \subseteq P$.

Moreover, if $P = \bigcap_{i=1}^n I_i$, then $P = I_j$ for some $j \in \{1, \ldots, n\}$. 

22
Proof. (i) \(\Rightarrow\) (ii) This follows from \(\bigcap_{i=1}^{n} I_i \subseteq I_j\) for \(j \in \{1, \ldots, n\}\).

(ii) \(\Rightarrow\) (iii) This follows from \(\prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i\).

(iii) \(\Rightarrow\) (i) Assume that \(\prod_{i=1}^{n} I_i \subseteq P\). Suppose that \(I_j \not\subseteq P\) for all \(j \in \{1, \ldots, n\}\); we will obtain a contradiction. For each \(j \in \{1, \ldots, n\}\) there exists \(a_j \in I_j\) such that \(a_j \notin P\). Now

\[
a_1 \cdots a_n \in \prod_{i=1}^{n} I_i \subseteq P.
\]

Since \(P\) is prime we have \(a_j\) for some \(j \in \{1, \ldots, n\}\). This is a contradiction.

To prove the final statement, assume that \(P = \bigcap_{i=1}^{n} I_i\). Since (ii) \(\Rightarrow\) (i), we have \(I_j \subseteq P\) for some \(j \in \{1, \ldots, n\}\). Also, since \(P = \bigcap_{i=1}^{n} I_i\) we have \(P \subseteq I_j\). Hence, \(P = I_j\). \(\square\)

Let \(R\) be a commutative ring, and let \(I\) and \(J\) be ideals of \(R\). We say that \(I\) and \(J\) are \textit{comaximal} if \(I + J = R\).

**Lemma 32.** Let \(R\) be a commutative ring, and let \(I\) and \(J\) be comaximal ideals of \(R\). Then \(I \cap J = IJ\).

\textit{Proof.} Since \(IJ \subseteq I\) and \(IJ \subseteq J\) we have \(IJ \subseteq I \cap J\). Next, let \(\in I \cap J\). Since \(I + J = R\), there exist \(a \in I\) and \(b \in J\) such that \(a + b = 1\). Hence, \(x = xa + xb = ax + xb\). Now \(a \in I\), and \(x \in I \cap J \subseteq J\) so that \(ax \in IJ\); similarly, \(x \in I \cap J \subseteq I\) and \(b \in J\), so that \(xb \in IJ\). Therefore, \(x = xa + xb \in IJ\).

It follows that \(I \cap J \subseteq IJ\). \(\square\)

**Lemma 33.** Let \(R\) be a commutative ring, and let \(I_1, \ldots, I_n\) be pairwise comaximal ideals of \(R\). Assume that \(n \geq 2\). Then

(i) \(I_1 \cap \cdots \cap I_{n-1}\) and \(I_n\) are comaximal.

(ii) \(I_1 \cap \cdots \cap I_n = I_1 \cdots I_n\).

\textit{Proof.} (i) Let \(J = \bigcap_{i=1}^{n-1} I_i\). Assume that \(J\) and \(I_n\) are not comaximal; we will obtain a contradiction. Since \(J\) and \(I_n\) are not comaximal we have \(J + I_n \not\subseteq R\). By Proposition 17 there exists a maximal ideal \(M\) such that \(J + I_n \subseteq M \not\subseteq R\). By Lemma 20 \(M\) is a prime ideal of \(R\). Now \(J = \bigcap_{i=1}^{n-1} I_i \subseteq M\); by Lemma 31 we have \(I_j \subseteq M\) for some \(j \in \{1, \ldots, n-1\}\). Since \(I_j\) and \(I_n\) are comaximal we have \(R = I_j + I_n\). But \(I_j \subseteq M\) and \(I_n \subseteq M\); hence, \(R = M\). This contradicts that \(M\) is proper.

(ii) We prove this by induction on \(n\). The case \(n = 2\) is Lemma 32. Assume that the \(n \geq 3\) and that the claim holds for \(n - 1\). By the induction hypothesis,

\[
J = \bigcap_{i=1}^{n-1} I_i = \prod_{i=1}^{n-1} I_i.
\]

By (i), the ideals \(J\) and \(I_n\) are comaximal so that \(J \cap I_n = JI_n\) by Lemma 32. Hence,

\[
JI_n = J \cap I_n
\]
\[
\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i.
\]

This completes the proof. \(\square\)

Let \(R\) be a commutative ring, and let \(I\) be an ideal of \(R\). Let \(x, y \in R\). We will write

\[ x \equiv y \pmod{I} \]

to mean that

\[ x + I = y + I \]

or equivalently, \(x - y \in I\).

**Theorem 34** (Chinese Remainder Theorem). Let \(R\) be a commutative ring, and let \(I_1, \ldots, I_n\), with \(n \geq 2\), be pairwise comaximal ideals of \(R\). If \(x_1, \ldots, x_n \in R\), then there exists \(x \in R\) such that

\[ x \equiv x_i \pmod{I_i} \]

for \(i \in \{1, \ldots, n\}\).

**Proof.** We first prove this when \(n = 2\). Since \(I_1\) and \(I_2\) are comaximal we have \(I_1 + I_2 = R\). Hence, there exist \(a_1 \in I_1\) and \(a_2 \in I_2\) such that \(a_1 + a_2 = 1\). Set \(x = x_2a_1 + x_1a_2\). Then

\[ x \equiv x_2a_1 + x_1a_2 \pmod{I_1} \]

\[ \equiv x_1a_2 \pmod{I_1} \quad \text{(because } x_2a_1 \in I_1) \]

\[ \equiv x_1(1 - a_1) \pmod{I_1} \quad \text{(recall that } a_1 + a_2 = 1) \]

\[ \equiv x_1 - x_1a_1 \pmod{I_1} \]

\[ \equiv x_1 \pmod{I_1} \quad \text{(because } x_1a_1 \in I_1). \]

Similarly, \(x \equiv x_2 \pmod{I_2}\). This proves the \(n = 2\) case. Now we prove the general case. Let \(i \in \{1, \ldots, n\}\). Let \(J_i\) be the intersection of all the ideals \(I_1, \ldots, I_n\) except \(I_i\). By Lemma 33 we have that \(I_i\) and \(J_i\) are comaximal. By the \(n = 2\) case there exists \(y_i \in R\) such that

\[ y_i \equiv 1 \pmod{I_i} \quad \text{and} \quad y_i \equiv 0 \pmod{J_i}. \]

Since \(J_i \subseteq I_j\) for \(j \in \{1, \ldots, n\}\) with \(j \neq i\) the fact that \(y_i \equiv 0 \pmod{J_i}\) implies that

\[ y_i \equiv 0 \pmod{I_j} \quad \text{for} \quad j \neq i. \]

Define

\[ x = x_1y_1 + \cdots + x ny_n. \]
Let $i \in \{1, \ldots, n\}$. Then

$$x \equiv x_1y_1 + \cdots + x_ny_n \pmod{I_i}$$

$$\equiv x_iy_i \pmod{I_i} \quad \text{(because } y_j \equiv 0 \pmod{I_i} \text{ for } j \neq i)$$

$$\equiv x_i \pmod{I_i} \quad \text{(because } y_i \equiv 1 \pmod{I_i}).$$

This completes the proof.

Lemma 35. Let $R$ be a commutative ring, and let $I_1, \ldots, I_n$ be ideals of $R$ with $n \geq 2$. Define

$$f : R \rightarrow R/I_1 \times \cdots \times R/I_n$$

by

$$f(r) = (r + I_1, \ldots, r + I_n)$$

for $r \in R$. Then $f$ is a homomorphism of rings and

$$\ker(f) = \bigcap_{i=1}^{n} I_i.$$

Moreover, $f$ is surjective if and only if $I_1, \ldots, I_n$ are pairwise comaximal.

Proof. It is straightforward to verify that $f$ is a ring homomorphism. Let $r \in R$. Then

$$f(r) = 0 \iff r + I_i = I_i \quad \text{for } i \in \{1, \ldots, n\}$$

$$\iff r \in I_i \quad \text{for } i \in \{1, \ldots, n\}$$

$$\iff r \in \bigcap_{i=1}^{n} I_i.$$

Assume that $f$ is surjective. Let $i, j \in \{1, \ldots, n\}$ with $i \neq j$. Since $f$ is surjective, there exists $r \in R$ such that

$$f(r) = (0, \ldots, 0, \underbrace{1 + I_j}_{i\text{-th position}}, 0, \ldots, 0) = (I_i, \ldots, I_{i-1}, \underbrace{1 + I_j}_{i\text{-th position}}, I_{i+1}, \ldots, I_n).$$

this means, in particular, that $r + I_i = 1 + I_i$. Hence, there exists $x \in I_i$ such that $r = 1 + x$. Also, we have $r + I_j = I_j$, so that $r \in I_j$. We now have $1 = r - x \in I_j + I_i$. This implies that $R = I_i + I_j$, so that $I_i$ and $I_j$ are comaximal. Finally, assume that $I_1, \ldots, I_n$ are pairwise comaximal. Then $f$ is surjective by the Chinese Remainder Theorem.

Corollary 36. Let the notation be as in Lemma 35. Assume that $I_1, \ldots, I_n$ are pairwise comaximal. Then there is an isomorphism

$$R/(I_1 \cdots I_n) = R/(I_1 \cap \cdots \cap I_n) \sim R/I_1 \times \cdots \times R/I_n.$$
defined by \( r + (I_1 \cap \cdots \cap I_n) \mapsto (r + I_1, \ldots, r + I_n) \) for \( r \in R \).

**Proof.** This follows from Lemma 35 and Theorem 10.

## 4 Primary Decomposition

Consider the ring \( R = \mathbb{Z} \). If \( I \) is a non-zero proper ideal of \( \mathbb{Z} \) then \( I = (n) \) for some \( n \in \mathbb{Z} \) such that \( n \neq 0 \) and \( n \neq \pm 1 \). We may assume that \( n \) is positive. Factor \( n \) as a product of powers of primes:

\[
n = p_1^{e_1} \cdots p_t^{e_t}.
\]

Then

\[
(n) = (p_1^{e_1}) \cdots (p_t^{e_t}).
\]

Also, since \((p_i^{e_i})\) and \((p_j^{e_j})\) are comaximal for \( i \neq j \), we can write this as

\[
(n) = (p_1^{e_1}) \cap \cdots \cap (p_t^{e_t}).
\]

This is an example of what is called a primary decomposition. We will try to do something similar for every Noetherian ring. That is, we will try to write every ideal as an intersection of certain special ideals (analogous to the \((p_i^{e_i})\)), with each of these special ideals being associated to a prime ideal. We begin by defining what will turn out to be the special ideals.

Let \( R \) be a commutative ring. Let \( Q \) be an ideal of \( R \). We say that \( Q \) is **primary ideal** of \( R \) if

(i) \( Q \) is a proper ideal of \( R \), i.e., \( Q \subsetneq R \).

(ii) If \( a, b \in R \), \( ab \in Q \), and \( a \notin Q \), then there exists \( n \in \mathbb{N} \) such that \( b^n \in Q \).

Condition (ii) of this definition is equivalent to the following: if \( a, b \in R \) and \( ab \in Q \), then \( a \in Q \) or \( b \in \sqrt{Q} \).

**Example.** Clearly, any prime ideal is a primary ideal.

**Lemma 37.** Let \( R \) be a commutative ring, and let \( Q \) be a primary ideal of \( R \). Define \( P = \sqrt{Q} \), the radical of \( Q \). Then \( P \) is a prime ideal of \( R \) that contains \( Q \). Moreover, if \( P' \) is another prime ideal such that \( Q \subseteq P' \), then \( P \subseteq P' \).

**Proof.** First we prove that \( P \) is proper. Since \( Q \) is proper we have \( 1 \notin Q \). It follows that \( 1 \notin \sqrt{Q} = P \); hence, \( P \) is proper. Now suppose that \( a, b \in R \) are such that \( ab \in P = \sqrt{Q} \). We need to prove that \( a \in P \) or \( b \in P \). Assume that \( a \notin P \); we will prove that \( b \in P \). Now since \( ab \in P = \sqrt{Q} \), there exists \( n \in \mathbb{N} \) such that \((ab)^n \in Q \), i.e., \( a^n b^n \in Q \). We must have \( a^n \notin Q \); otherwise, \( a \in \sqrt{Q} = P \). Since \( Q \) is primary, there exists \( m \in \mathbb{N} \) such that \((b^n)^m \in Q \). This means that \( b \in \sqrt{Q} = P \). It follows that \( P \) is prime. Next, assume that \( P' \) is a prime ideal such that \( Q \subseteq P' \). We need to prove that \( P \subseteq P' \). Taking radicals, we have

\[
P = \sqrt{Q} \subseteq \sqrt{P'} = P'.
\]
Let ideals have unique minimal prime ideals.

Proof. Assume that $R/I$ is not trivial and every zero divisor of $R/I$ is nilpotent. Then $R/I$ is non-trivial, $I$ is a proper ideal of $R$. Let $a,b \in R$ with $ab \in I$ and $a \notin I$. Then $(a + I)(b + I) = I$ with $a + I \neq I$. It follows that $b + I$ is a zero divisor in $R/I$. Hence, there exists $n \in \mathbb{N}$ such that $(b + I)^n = I$. This implies that $b^n \in I$. Hence, $I$ is primary.

Now assume that $R/I$ is non-trivial and every zero divisor of $R/I$ is nilpotent. As $R/I$ is non-trivial, $I$ is a proper ideal of $R$. Let $a,b \in R$ such that $ab \in I$ and $a \notin I$. Then $(a + I)(b + I) = I$ with $a + I \neq I$. It follows that $b + I$ is a zero divisor in $R/I$. Hence, there exists $n \in \mathbb{N}$ such that $(b + I)^n = I$. This implies that $b^n \in I$. Hence, $I$ is primary.  

**Lemma 38.** Let $R$ be a commutative ring, and let $I$ be an ideal of $R$. Then $I$ is primary if and only if $R/I$ is a commutative ring and $I$ is a prime ideal.

**Proof.** Assume that $I$ is primary. Then $I$ is a prime ideal of $R$. This implies that $R/I$ is a commutative ring. Now assume that $R/I$ is a commutative ring. Then $I$ is a prime ideal of $R$. Hence, $I$ is primary.

**Proposition 39.** Let $R$ be a commutative ring, and let $Q$ be an ideal of $R$. Let $M = \sqrt{Q}$. If $M$ is maximal, then $Q$ is $M$-primary.

**Proof.** Assume that $M$ is maximal. We have $Q \subseteq \sqrt{Q} = M \subseteq R$. This implies that $Q$ is proper. Since $M$ is maximal, it follows that $Q + (b) = R$. Since $(b) \subset \sqrt{Q}$, this implies that

$$\sqrt{Q} + \sqrt{(b)} = R.$$  

By a previous homework exercise (in general, $\sqrt{I} + \sqrt{J} = (1) \implies I + J = (1)$), we get that $Q + (b) = R$. Hence, there exists $x \in Q$ and $r \in R$ such that $1 = x + rb$. Therefore,

$$a = ax + arb = ax + rb \in Q$$

because $x, ab \in Q$. This contradicts $a \notin Q$. It follows that $Q$ is $M$-primary.  

**Corollary 40.** Let $R$ be a commutative ring, and let $M$ be a maximal ideal of $R$. For every $n \in \mathbb{N}$ the ideal $M^n$ is $M$-primary.

**Proof.** Let $n \in \mathbb{N}$. Then by previous homework exercise we have $\sqrt{M^n} = M$ (this holds for any prime ideal). The proposition implies that $M^n$ is $M$-primary.
End of lecture, Monday, September 26.