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 5

3 Prime ideals and maximal ideals 14

4 Primary Decomposition 28

5 Rings of Fractions 43

1 Commutative rings and subrings

We recall that a **Euclidean domain** is an integral domain \( R \) with a function \( \partial : R - 0 \to \mathbb{N}_0 \) (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 \( b \not= 0 \), then there exist \( q, r \in R \) such that

\[
a = qb + r \quad \text{and} \quad r = 0 \text{ or } r \not= 0 \quad \text{and} \quad \partial(r) < \partial(b).
\]

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 \( a, b \in R \) 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,

\[
ab^{-1} = (m + g) + i(n + h)
\]

\[
ab^{-1} = (m + in) + (g + ih)
\]

\[
a = (m + ih)b + (g + ih)b
\]

\[
a = qb + r,
\]

where

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

Since \( a, b, \) and \( q \) are in \( R \), so is \( r \). Now

\[
\partial(r) = |r|^2
\]

\[
= |g + ih|^2|b|^2
\]

\[
= (g^2 + h^2)\partial(b)
\]

\[
\leq (1/4 + 1/4)\partial(b)
\]

\[
< \partial(b).
\]

This completes the proof. \( \square \)

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

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

But we also have

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

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 $p_i = u_iq_i$ 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 $R[X_1, \ldots, X_n]$.

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 $D = 1, 2, -1, -3, -7, -11, -19, -43, -67, -163$. 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 has 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 $ra \in \ker(f)$.

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 **principal ideal** generated by $a$ and $a$ is said to be a **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 $(n) = n\mathbb{Z} = n\mathbb{Z}$. This is the set of all the integers divisible by $n$.

Let $R$ be an integral domain. We say that $R$ is a **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
\[
a = qb + r \quad \text{and} \quad r = 0 \text{ or } r \neq 0 \quad \text{and} \quad \partial(r) < \partial(b).
\]
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 \( \mathbb{K}[X] \) for \( \mathbb{K} \) a field are PIDs. But very many important rings are not PIDs. For example, in the exercises you will prove that if \( \mathbb{K} \) is field then \( \mathbb{K}[X_1, X_2] \) 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 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. \( \square \)

**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
\[
A_1 \cdots A_n = \text{the set of all finite sums of elements of the form } a_1 \cdots a_n, \quad a_1 \in A_1, \ldots, a_n \in A_n.
\]
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. \( \square \)

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 \( IJ \not\subseteq I \cap J \). For example, take \( R = \mathbb{Z}, I = (2), J = (4) \). Then \( IJ = (8) \), but \( (2) \cap (4) = (\text{lcm}(2, 4)) = (4) \). 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
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
\[
a_2 b_2 + I = (a_1 + c)(b_1 + d) + I
= a_1 b_1 + a_1 d + cb_1 + cd + I
\in I
= a_1 b_1 + I.
\]
Here we have used \( a_1 d + cb_1 + cd \in I \) 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 natural or 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 \( p : R \to R/I \) is the canonical homomorphism. Conversely, assume that \( I \) is the kernel of a ring homomorphism \( f : R \to S \), i.e., \( I = \ker(f) \). Earlier, we proved that \( \ker(f) \) is an ideal. Hence, \( I = \ker(f) \) is an ideal.

**Theorem 10** (Ring isomorphism theorem). Let \( R \) and \( S \) be commutative rings, and let \( f : R \to S \) 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 \( \bar{f} \) 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
\[ f(r_1) = f(r_2 + k) = f(r_2) + f(k) = f(r_2) + 0 = f(r_2). \]
It follows that \( \bar{f} \) is well-defined. It is easy to verify that \( \bar{f} \) is a ring homomorphism using that \( f \) is a ring homomorphism. To see that \( \bar{f} \) is injective, assume that \( r \in R \) is such that \( \bar{f}(r + \ker(f)) = 0 \). 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 \( \bar{f} \) is surjective, let \( s \in \text{im}(f) \). Then there exists \( r \in R \) such that \( f(r) = s \). We have \( \bar{f}(r + \ker(f)) = f(r) = s \), which proves that \( \bar{f} \) is surjective. Since \( f \) is injective and surjective, \( f \) is bijective and is thus a ring isomorphism. \( \square \)
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

$$i : \{\text{ideals of } R \text{ containing } I\} \xrightarrow{\sim} \{\text{ideals of } R/I\}$$

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:

$$(1) = \{0, 1, 2, 3, 4, 5\},$$
$$(2) = \{0, 2, 4\},$$
$$(3) = \{0, 3\},$$
$$(6) = \{0\}.$$

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
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 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 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 extension of $I$ and is denoted by

$$I^e = (f(I)).$$

The following facts hold.

**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

(i) $I \subseteq I^{ee}$.

(ii) $J^{ee} \subseteq J$.

(iii) $I^e = I^{eec}$.

(iv) $J^{ecc} = J^c$.

Proof. (i). Let $r \in I$. Then $f(r) \in I^e$ by the definition of $I^e$. This implies that $r \in f^{-1}(I^e) = I^{ee}$. Thus, $I \subseteq I^{ee}$.

(ii). We have

$$J^{ee} = (f(f^{-1}(J))) \subseteq J$$

(Note that since $f(f^{-1}(J)) \subseteq J$ and $J$ is an ideal, we have $(f(f^{-1}(J))) \subseteq J$).

(iii). By (i), $I \subseteq I^{ee}$. This implies that $I^e \subseteq I^{eec}$. By (ii) we have $I^{eec} \subseteq I^e$. It follows that $I^e = I^{eec}$. eq (iv). By (ii), $J^{ee} \subseteq J$; hence, $J^{ecc} \subseteq J^c$. By (i) we have $J^c \subseteq J^{ecc}$. We now have $J^{ecc} = J^c$. □

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

\[ I \mapsto I^c, \quad \text{for } I \in C_R, \]
\[ J^c \leftrightarrow J, \quad \text{for } J \in E_S. \]
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.

**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

$$
M \text{ is a maximal ideal of } \mathbb{Z} \iff \mathbb{Z}/M = \mathbb{Z}/m\mathbb{Z} \text{ is a field } \iff m \text{ is a prime (elementary number theory)}.
$$

This completes the proof.
Example. Let $K$ be a field and let $f \in K[X]$ be non-zero and not a unit, i.e., not in $K^\times = K - 0$. 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 $(p) \nsubseteq R$. 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. □

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

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

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

$$= \bar{g}(a_1, \ldots, a_n)$$

15
\[ t(g(a_1, \ldots, a_n)). \]

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 \textit{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:

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

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 \textit{partial order} if

(i) \( \leq \) is \textit{reflexive}: if \( x \in X \), then \( x \leq x \).

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

(iii) \( \leq \) is \textit{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 \textit{totally ordered} if for all \( x, y \in Y \) we have \( x \leq y \) or \( y \leq x \). We say that \( Y \) has an \textit{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 \textit{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.

**Proposition 17.** Let \( R \) be a commutative ring, and let \( I \) be a proper ideal of \( R \), i.e., \( I \subsetneq R \). 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 \( I \subseteq J \subsetneq R \). 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 $B \subseteq X$. 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 $I$. \hfill \Box

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., $P \subsetneq R$.

(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 $aP = (a + P)(b + P) = P$. 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 $\bar{a} = 0$ or $\bar{b} = 0$. 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 $\bar{a} \bar{b} = 0$ in $R/P$. Since $R/P$ is an integral domain we have $\bar{a} = 0$ or $\bar{b} = 0$. This means that $a \in P$ or $b \in P$. Hence, $P$ is a prime ideal. \hfill \Box

**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 is a prime ideal of $R$ $\iff$ $R/P$ is an integral domain $\iff$ $(R/I)/(P/I) \cong R/P$ is an integral domain $\iff P/I$ is a prime ideal of $R/I$.

This completes the proof. \hfill \Box

**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

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

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 \textbf{prime element} of $R$ if the following holds: if $a, b \in R$ and $p \mid ab$, then $p \mid a$ or $p \mid b$.

\textbf{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.

\textbf{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 $p \mid b$.

\textbf{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 $R$.

\textbf{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.

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

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

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

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

From the lemmas, we see that:

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

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 $R$, (PIDs, 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** if for all sequences of 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 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 $(x_1) \subsetneq I$. Hence, there exists $x_2 \in I - (x_1)$. We have $(x_1) \subsetneq (x_1, x_2)$. Since $I$ is not finitely generated, $(x_1, x_2) \subsetneq I$; 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

\[ (b) \nsubseteq (c) \nsubseteq R, \quad (b) \nsubseteq (d) \nsubseteq R. \]

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 **multiplicatively closed** or is a **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 \( P \nsubseteq R \) we have \( 1 \neq P \) so that \( 1 \in S \). Let \( s_1, s_2 \in S \). Then \( s_1s_2 \in S \) because otherwise \( s_1s_2 \notin P \) 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
Let $S \cap I = \emptyset$. By Theorem 26, there exists a prime ideal $Q$ such that $I \subset Q$ 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 $Q \cap S = \emptyset$. \hfill $\Box$

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. \hfill $\Box$

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., $I \varsubsetneq R$. 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 $P' \in \text{Var}(I)$ is such that $I \subseteq P' \subseteq P$, then $P = P'$. This completes the proof. \hfill $\Box$

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 $x \in \cap_{P \in \text{min}(I)} P$. We claim that $x \in \cap_{P \in \text{Var}(I)} P$. 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 $x \in \cap_{P \in \text{min}(I)} P$ we have $x \in P'$. As $P' \subseteq P$ we get $x \in P$. It follows that $x \in \cap_{P \in \text{Var}(I)} P$ so that

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

This completes the proof. \qed

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:

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

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

Proof. (i) $\implies$ (ii) This follows from $\bigcap_{i=1}^{n} I_i \subseteq I_j$ for $j \in \{1, \ldots, n\}$.
(ii) $\implies$ (iii) This follows from $\prod_{i=1}^{n} I_i \subseteq \bigcap_{i=1}^{n} I_i$.
(iii) $\implies$ (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 $a_j \not\in P$. 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) $\implies$ (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, $P = I_j$. \qed

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 $I + J = R$. 

24
Lemma 32. Let $R$ be a commutative ring, and let $I$ and $J$ be comaximal ideals of $R$. Then $I \cap J = IJ$.

Proof. Since $IJ \subseteq I$ and $IJ \subseteq J$ we have $IJ \subseteq I \cap J$. Next, let $x \in I \cap J$. 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 $I \cap J \subseteq IJ$.

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) $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.

Proof. (i) Let $J = \cap_{i=1}^{n-1} I_i$. 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 $J = \cap_{i=1}^{n-1} I_i \subseteq M$; 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 $J \cap I_n = JJ_n$ by Lemma 32. Hence,

$$JJ_n = J \cap I_n = \prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i.$$ 

This completes the proof.

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 each $i = 1, \ldots, n$. Therefore, $x \in \prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i$.

25
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

$$x \equiv x_1y_1 + \cdots + x_ny_n \pmod{I_i}$$
$$\equiv x_1y_i \pmod{I_i} \quad \text{(because $y_j \equiv 0 \pmod{I_i}$ for $j \neq i$)}$$
$$\equiv x_i \pmod{I_i} \quad \text{(because $y_i \equiv 1 \pmod{I_i}$)}.$$

This completes the proof. \hfill \Box

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

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

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

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

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 $(b^m)^m \in Q$. 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

$$P = \sqrt{Q} \subseteq \sqrt{P'} = P'.$$

Here, $\sqrt{P'} = P'$ by a homework exercise. This completes the proof. 

With the notation of Lemma 37, it is clear that $P$ is a minimal prime ideal of $Q$, and in fact is the unique minimal prime ideal of $Q$. (For suppose $P'$ is another minimal ideal of $Q$. Then by
Lemma 37 we have $P \subseteq P'$. By the minimality of $P'$ we obtain $P' = P$.) In other words, primary ideals have unique minimal prime ideals.

Let $R$ be a commutative ring, and let $Q$ be an ideal of $R$. In what follows, when we say that $Q$ is $P$-primary we will mean that $Q$ is primary, $P$ is a prime ideal, and $\sqrt{Q} = P$.

**Lemma 38.** Let $R$ be a commutative ring, and let $R$ be an ideal of $R$. Then $I$ is primary if and only if $R/I$ is not trivial and every zero divisor of $R/I$ is nilpotent.

**Proof.** Assume that $I$ is primary. Then $I$ is a proper ideal of $R$. This implies that $R/I \neq 0$, i.e., $R/I$ is non-trivial. Next, let $b \in R$ be such that $b + I$ is a zero divisor of $R/I$. Then there exists $a \in R$ such that $a + I \neq I$ and $(a + I)(b + I) = I$. This implies that $ab + I = I$, i.e., $ab \in I$. Now $a \notin I$; since $Q$ is primary there exists $n \in \mathbb{N}$ such that $b^n \in Q$. This implies that $(b + I)^n = b^n + I = I$, i.e., $b + I$ is nilpotent.

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 $a, b \in R$ 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. □

**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. Let $a, b \in R$ be such that $ab \in Q$ and $a \notin Q$; we need to prove that $b^n \in Q$ for some $n \in \mathbb{N}$. Assume that this does not hold; we will obtain a contradiction. By our assumption $b \notin \sqrt{Q} = M$. Since $M$ is maximal, it follows that $M + (b) = R$. Since $(b) \subset \sqrt{(b)}$, 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,

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

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. □

Let $R$ be a commutative ring. Then we have the following picture:
\[
\begin{array}{c}
\text{all ideals} & \xrightarrow{\text{Rad}} & \text{all ideals} \\
\cup & \cup & \\
\text{primary ideals} & \rightarrow & \text{prime ideals} \\
\cup & \cup & \\
\text{Rad}^{-1}(\text{maximal ideals}) & \rightarrow & \text{maximal ideals}.
\end{array}
\]

**Example.** Let \( R \) be a PID. Then the primary ideals of \( R \) are

\[
0, \quad (p^n) = (p)^n, \quad n \in \mathbb{N}, \, p \text{ an irreducible element}.
\]

**Proof.** The ideal 0 is primary because 0 is prime (recall that \( R \) is an integral domain). Let \( p \in R \) be irreducible, and let \( n \in \mathbb{N} \). By Lemma 22 the ideal \((p)\) is prime and also maximal. By Corollary 40, the ideals \((p^n) = (p)^n\) are primary for \( n \in \mathbb{N} \). Conversely, suppose that \( Q \) is a primary ideal of \( R \). Let \( r \in R \) be such that \( Q = (r) \). Since \( R \) is a UFD by Theorem 25, there exists irreducibles \( p_1, \ldots, p_n \) in \( R \) such that

\[ r = p_1 \cdots p_n. \]

We then have

\[ Q = (r) = (p_1) \cdots (p_n). \]

By Lemma 22 the ideals \((p_1), \ldots, (p_n)\) are prime and maximal. Let \( i \in \{1, \ldots, n\} \). We claim that \((p_i)\) is the unique minimal prime ideal of \( Q \). We have \( Q \subseteq (p_i) \). Assume that \( P \) is a prime ideal such that \( Q \subseteq P \subseteq (p_i) \). Since \( R \) is a PID, \( P \) is also maximal. Hence, \( P = (p_i) \). It follows that \((p_i)\) is a minimal prime ideal of \( Q \), and is hence the unique prime ideal of \( Q \) as \( Q \) is primary. Hence,

\[ (p_1) = \cdots = (p_n) \]

so that

\[ Q = (p_1)^n = (p^n). \]

This completes the proof. \( \square \)

**Lemma 41.** Let \( R \) be a commutative ring and let \( r_1, \ldots, r_t \in R \). Then for \( n \in \mathbb{N} \) we have

\[ (r_1, \ldots, r_t)^n = (r_{i_1} \cdots r_{i_n}, 1 \leq i_1, \ldots, i_n \leq t). \]

**Proof.** Clearly, \( r_{i_1} \cdots r_{i_n} \in (r_1, \ldots, r_t)^n \) for \( 1 \leq i_1, \ldots, i_n \leq t \). Hence

\[ (r_{i_1} \cdots r_{i_n}, 1 \leq i_1, \ldots, i_n \leq t) \subseteq (r_1, \ldots, r_t)^n. \]

Conversely, let \( r \in (r_1, \ldots, r_t)^n \). Then \( r \) is a sum of elements of the form

\[ (a_{11}r_1 + \cdots + a_{1t}r_t) \cdots (a_{n1}r_1 + \cdots + a_{nt}r_t) \]
and is hence a sum of elements of the form
\[ ar_{i_1} \cdots r_{i_n} \]
for \( a \in R \) and \( 1 \leq i_1, \ldots, i_n \leq t \). It follows that \( r \in (r_{i_1} \cdots r_{i_n}, 1 \leq i_1, \ldots, i_n \leq t) \). Hence
\[ (r_1, \ldots, r_t)^n \subseteq (r_{i_1} \cdots r_{i_n}, 1 \leq i_1, \ldots, i_n \leq t). \]

\[ \square \]

**Example.** Let \( K \) be a field and let \( R = K[X,Y] \), where \( X \) and \( Y \) are indeterminates. Let \( M = (X,Y) \) and \( Q = (X,Y^2) \). Then \( M \) is a maximal ideal, \( Q \) is a primary ideal, and \( \sqrt{Q} = M \). However, \( Q \) is not a power of a prime ideal.

**Proof.** The ideal \( M \) is maximal because \( R/M = K[X,Y]/(X,Y) \cong K \) is an integral domain. Now
\[
M^2 = (X^2,XY,Y^2) \subseteq Q = (X,Y^2) \subseteq M = (X,Y).
\]
Taking radicals, we obtain
\[
M = \sqrt{M^2} = \sqrt{(X^2,XY,Y^2)} \subseteq \sqrt{Q} = \sqrt{(X,Y^2)} \subseteq M = \sqrt{M} = \sqrt{(X,Y)}.
\]
It follows that
\[
\sqrt{Q} = M.
\]
Because \( M \) is maximal Proposition 39 now implies that \( Q \) is primary. Finally, we claim that \( Q \) is not a power of a prime ideal. Assume that \( Q = P^n \) for some \( n \in \mathbb{N} \) and prime ideal \( P \); we will obtain a contradiction. Taking radicals of \( Q = P^n \) we obtain
\[
M = \sqrt{Q} = \sqrt{P^n} = P.
\]
That is, \( P = M \). Hence, \( Q = M^n \). This means that
\[
(X,Y^2) = (X^n, X^{n-1}Y, \ldots, XY^{n-1}, Y^n).
\]
Since \( X \) is contained in this ideal there exist \( g_n, \ldots, g_0 \in R \) such that
\[
X = g_nX^n + g_{n-1}X^{n-1}Y + \cdots g_1XY^{n-1} + g_0Y^n.
\]
Substituting \( Y = 0 \), we obtain
\[
X = g_n(X,0)X^n
\]
so that taking degrees yields

\[ 1 = \deg(X) = \deg(g_n(X,0)) + n. \]

This implies that \( n = 1. \) We now have

\[ Q = (X,Y^2) = M = (X,Y). \]

This implies that \( Y \in (X,Y^2). \) Hence, there exist \( g, h \in R \) such that

\[ Y = gX + hY^2. \]

Substituting \( X = 0 \) gives

\[ Y = h(0,Y)Y^2. \]

Taking degrees, we get

\[ 1 = \deg(h(0,Y)) + 2. \]

This is a contradiction because \( \deg(h(0,Y)) \) is a non-negative integer. \( \square \)

**Example.** Let \( K \) be a field and let \( X, Y, Z \) be indeterminates. Let

\[ R = K[X,Y,Z]/I, \quad I = (XZ - Y^2). \]

Also, let

\[ x = X + I, \quad y = Y + I, \quad z = Z + I. \]

Let

\[ P = (x, y). \]

This is an ideal of \( R. \) Then \( P \) is a prime ideal but \( P^2 \) is not primary.

**Proof.** To prove that \( P \) is a prime ideal of \( R \) we first consider the ideal \( P' \) of \( K[X,Y,Z] \) generated by \( X \) and \( Y \), so that \( P' = (X,Y). \) We claim that \( P' \) is a prime ideal of \( K[X,Y,Z]. \) For this, define

\[ K[Z] \longrightarrow K[X,Y,Z]/P' = K[X,Y,Z]/(X,Y) \]

by \( f \mapsto f + P' \). We leave it to the reader to check that this map is a ring isomorphism. Since \( K[Z] \) is an integral domain, so is \( K[X,Y,Z]/P'. \) This implies that \( P' \) is a prime ideal of \( K[X,Y,Z]. \)

Turning to \( P \), we note that \( I \subseteq P'. \) Since \( P' \) is prime, \( P = P'/I \) is a prime ideal of \( K[X,Y,Z]/I \) (see Lemma 19). Next, we prove that \( P^2 \) is not a primary ideal of \( R \). In \( R \) we have

\[ xz = y^2 \in P^2 = (x^2, xy, y^2). \]
We claim that \( x \notin P^2 \) and \( z \notin \sqrt{P^2} = P \). For suppose \( x \in P^2 \). Then
\[
x = ax^2 + bxy + cy^2
\]
for some \( a, b, c \in R \). Recalling the definitions of \( x \) and \( y \), this implies that
\[
X = AX^2 + BXY + CY^2 + D(XZ - Y^2)
\]
for some \( A, B, C, D \in K[X,Y,Z] \). Taking \( Y = Z = 0 \), we get
\[
X = A(X,0,0)X^2.
\]
This is a contradiction. Next, suppose that \( z \in P \). Then
\[
z = ax + by
\]
for some \( a, b \in R \). This implies that
\[
Z = AX + BY + C(XZ - Y^2)
\]
for some \( A, B, C \in K[X,Y,Z] \). Taking \( X = Y = 0 \), we get that \( Z = 0 \), a contradiction. We have proven that \( P^2 \) is not primary.

The previous example also shows that if the radical of an ideal is prime, then it need not be the case that the ideal is primary.

**Lemma 42.** Let \( R \) be a commutative ring, and let \( P \) be a prime ideal of \( R \). Let \( Q_1, \ldots, Q_n \) be \( P \)-primary ideals of \( R \). Then \( \bigcap_{i=1}^n Q_i \) is also \( P \)-primary.

**Proof.** Let \( Q' = \bigcap_{i=1}^n Q_i \). We need to prove that \( Q' \) is \( P \)-primary. First of all, we have \( Q' \subseteq Q_1 \subseteq R \); hence, \( Q' \) is a proper ideal of \( R \). Next, let \( a, b \in R \) be such that \( ab \in Q' \) and \( a \notin Q' \); we need to prove that there exists \( n \in \mathbb{N} \) such that \( b^n \in Q' \), i.e., \( b \in \sqrt{Q'} \). Since \( a \notin Q' \), there exists \( i \in \{1,\ldots,n\} \) such that \( a \notin Q_i \). Now as \( ab \in Q' \) and \( Q' \subseteq Q_i \), we have \( ab \in Q_i \). Since \( Q_i \) is \( P \)-primary, it follows that \( b \in \sqrt{Q_i} \). Moreover,
\[
b \in \sqrt{Q_i} = P = P \cap \cdots \cap P = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_n} = \sqrt{Q_1 \cap \cdots \cap Q_n} = \sqrt{Q'}.
\]
Here, the fourth equality follows by a previous homework exercise. This completes the proof.

Let \( R \) be a commutative ring, and let \( I \) be a proper ideal of \( R \). A **primary decomposition** of \( I \) is a finite sequence of primary ideals of \( R \) such that
\[
I = Q_1 \cap \cdots \cap Q_n.
\]
If \( I \) admits a primary decomposition then we say that \( I \) is a **decomposable ideal** of \( R \). Let \( Q_1, \ldots, Q_n \) be a primary decomposition of \( I \). By Lemma 37 the ideals

\[
\sqrt{Q_1} = P_1, \ldots, \sqrt{Q_n} = P_n
\]

are prime ideals of \( R \); i.e., each \( Q_i \) is a \( P_i \)-primary for \( i = 1, \ldots, n \). We will say that \( Q_1, \ldots, Q_n \) is a **minimal primary decomposition** of \( I \) if

\[
I = Q_1 \cap \cdots \cap Q_n
\]

and

(i) \( P_1, \ldots, P_n \) are pairwise unequal.

(ii) For \( j = 1, \ldots, n \),

\[
\bigcap_{i=1, i \neq j}^{n} Q_i \not\subseteq Q_j.
\]

**Lemma 43.** Let \( R \) be a commutative ring, and let \( I \) be a decomposable ideal of \( R \). Then \( I \) admits a minimal primary decomposition.

**Proof.** Let \( Q_1, \ldots, Q_n \) be a primary decomposition of \( I \). We will alter the primary decomposition \( Q_1, \ldots, Q_n \) to obtain a primary decomposition that is minimal in the following way. First we obtain a primary decomposition that satisfies (i) of the definition of minimal. Let \( P_1 = \sqrt{Q_1}, \ldots, P_n = \sqrt{Q_n} \). Let \( P_{a_1}, \ldots, P_{a_t} \) be a sublist of \( P_1, \ldots, P_n \) such that \( P_{a_1}, \ldots, P_{a_t} \) are pairwise unequal and every member of \( P_1, \ldots, P_n \) is in the list \( P_{a_1}, \ldots, P_{a_t} \). For \( i = 1, \ldots, t \), let \( Q'_i \) be the intersection of the members \( Q_j \) of \( Q_1, \ldots, Q_n \) such that \( \sqrt{Q_j} = P_{a_i} \). Then \( I = Q'_1 \cap \cdots \cap Q'_t \) and by Lemma 37 the ideals \( Q'_1, \ldots, Q'_t \) are primary. Thus, \( Q'_1, \ldots, Q'_t \) is a primary decomposition of \( I \), and we see that this list satisfies (i) of the definition of minimal. Now we will alter \( Q'_1, \ldots, Q'_t \) by deleting some of the \( Q'_i \) to obtain a primary decomposition of \( I \) that satisfies (ii) of the definition of minimal (note that deleting does not change that the list satisfies (i)). We proceed as follows. Consider \( Q'_1 \). If \( \bigcap_{i=2}^{n} Q'_i \subseteq Q'_1 \), then

\[
I = Q'_1 \cap \cdots \cap Q'_t = Q'_2 \cap \cdots \cap Q'_t.
\]

Therefore, if \( \bigcap_{i=2}^{t} Q'_i \subseteq Q'_1 \), then \( Q'_2, \ldots, Q'_t \) is a primary decomposition of \( I \). If indeed \( \bigcap_{i=2}^{n} Q'_i \subseteq Q'_1 \), then we discard \( Q'_1 \), and continue with the primary decomposition \( Q'_2, \ldots, Q'_t \); otherwise, we keep \( Q'_1, \ldots, Q'_n \). We then proceed to the next element in the list, and so on. The resulting primary decomposition of \( I \) satisfies (i) and (ii) of the definition and is thus minimal.

Let \( R \) be a commutative ring, let \( I \) be an ideal of \( R \), and let \( a \in R \). We recall that by definition

\[
(I : a) = \{ r \in R : ra \in I \}.
\]

The set \((I : a)\) is an ideal of \( R \). Evidently, we also have \( I \subseteq (I : a) \).
Lemma 44. Let $R$ be a commutative ring, and let $Q$ be a $P$-primary ideal of $R$. Let $a \in R$. Then

(i) If $a \in Q$, then $(Q : a) = R$.

(ii) If $a \notin Q$, then $(Q : a)$ is $P$-primary and hence $\sqrt{(Q : a)} = P$.

(iii) If $a \notin P$, then $(Q : a) = Q$.

Proof. (i) Assume that $a \in Q$. We need to prove that $1 \in (Q : a)$. Since $a \in Q$, we have $1 \cdot a \in Q$; hence, $1 \in (Q : a)$, so that $(Q : a) = R$.

(ii) Assume that $a \notin Q$. We first will prove that $(Q : a) \subseteq P$. Let $r \in (Q : a)$. Then $ra \in Q$. Since $Q$ is primary and $a \notin Q$ we must have $r \in \sqrt{Q} = P$. This proves that $(Q : a) \subseteq P$. Next, we prove that $\sqrt{(Q : a)} = P$. We have the following inclusions

$$Q \subseteq (Q : a) \subseteq P.$$  

Taking radicals, we obtain

$$P = \sqrt{Q} \subseteq \sqrt{(Q : a)} \subseteq \sqrt{P} = P.$$  

Here, $\sqrt{P} = P$ by a previous homework exercise. It follows that all of these ideals are equal; in particular, $\sqrt{(Q : a)} = P$. Finally, we prove that $(Q : a)$ is primary. Assume that $c, d \in R$ are such that $cd \in (Q : a)$ but $d \notin \sqrt{(Q : a)} = P$; we need to prove that $c \in (Q : a)$. Now $acd \in Q$. Therefore, $ac \in Q$ or $d \in \sqrt{Q} = P$. But $d \notin P$; hence, $ac \in Q$. This means that $c \in (Q : a)$.

(iii) Assume that $a \notin P$. We already have $Q \subseteq (Q : a)$. Let $b \in (Q : a)$. Then $ba \in Q$. Since $Q$ is primary we have $b \in Q$ or $a \in \sqrt{Q} = P$. As $a \notin P$ we must have $b \in Q$. Thus, $(Q : a) \subseteq Q$ and we conclude that $(Q : a) = Q$.

Lemma 45. Let $R$ be a commutative ring, and let $I$ be a decomposable ideal of $R$. Let

$$I = Q_1 \cap \cdots \cap Q_n$$  

be a minimal primary decomposition of $I$. Let $P$ be a prime ideal of $R$. Then the following are equivalent:

(i) $P = P_i$ for some $i \in \{1, \ldots, n\}$.

(ii) There exists $a \in R$ such that $(I : a)$ is $P$-primary.

(iii) There exists $a \in R$ such that $\sqrt{(I : a)} = P$.

Proof. (i) $\implies$ (ii) Assume that $P = P_i$ for some $i \in \{1, \ldots, n\}$. Since $Q_1, \ldots, Q_n$ is a minimal primary decomposition of $I$ we have

$$\bigcap_{j=1}^{n} Q_j \notin Q_i.$$
Hence, there exists $a \in \bigcap_{j=1}^{n} Q_j$ such that $a \notin Q_i$. Now

\[
(I : a) = \left( \bigcap_{j=1}^{n} Q_j : a \right)
\]

\[
= \bigcap_{j=1}^{n} (Q_j : a) \quad \text{(Exercise 2.33)}
\]

\[
= (Q_i : a) \cap \bigcap_{j=1}^{n} (Q_j : a) \quad \text{(Lemma 44)}
\]

\[
(I : a) = (Q_i : a).
\]

Now by Lemma 44 the ideal $(Q : a_i)$ is $P_i = P$-primary. Hence, $(I : a)$ is $P$-primary.

(ii) $\implies$ (iii) This is clear.

(iii) $\implies$ (i) Assume that there exists $a \in R$ such that $\sqrt{(I : a)} = P$. We first note that $a \notin I$ (otherwise, $(I : a) = R$, so that $P = \sqrt{(I : a)} = R$, contradicting $P \subsetneq R$). Since $a \notin I$, there exists at least one $i \in \{1, \ldots, n\}$ such that $a \notin Q_i$. Now

\[
(I : a) = \left( \bigcap_{i=1}^{n} Q_i : a \right)
\]

\[
= \bigcap_{i=1}^{n} (Q_i : a)
\]

\[
= \left( \bigcap_{a \in Q_i} (Q_i : a) \right) \cap \left( \bigcap_{a \notin Q_i} (Q_i : a) \right)
\]

\[
= \left( \bigcap_{i=1}^{n} R \right) \cap \left( \bigcap_{a \notin Q_i} (Q_i : a) \right)
\]

\[
= \bigcap_{a \notin Q_i} (Q_i : a).
\]

Taking radicals (and using the general rule $\sqrt{J_1 \cap J_2} = \sqrt{J_1} \cap \sqrt{J_2}$),

\[
\sqrt{(I : a)} = \bigcap_{a \notin Q_i} (Q_i : a)
\]
\[ P = \bigcap_{i=1}^{n} \sqrt{(Q_i : a)} \]

\[ P = \bigcap_{i=1}^{n} P_i \quad \text{(by Lemma 44).} \]

By Lemma 31 we have \( P = P_i \) for some \( i \in \{1, \ldots, n\} \).

**Theorem 46** (First Uniqueness Theorem for Primary Decomposition). Let \( R \) be a commutative ring, and let \( I \) be a decomposable ideal of \( R \). Let

\[ I = Q_1 \cap \cdots \cap Q_n \text{ with } \sqrt{Q_i} = P_i, \ i \in \{1, \ldots, n\} \]

and

\[ I = Q'_1 \cap \cdots \cap Q'_{n'} \text{ with } \sqrt{Q'_i} = P'_i, \ i \in \{1, \ldots, n'\} \]

be two minimal primary decompositions of \( I \). Then

\[ \{P_1, \ldots, P_n\} = \{P'_1, \ldots, P'_{n'}\}. \]

In particular, \( n = n' \).

**Proof.** By Lemma 45 we have

\[ \{P_1, \ldots, P_n\} = \{P \in \text{Spec}(R) : \text{there exists } a \in R \text{ such that } \sqrt{(I : a)} = P\} \]

and

\[ \{P'_1, \ldots, P'_{n'}\} = \{P \in \text{Spec}(R) : \text{there exists } a \in R \text{ such that } \sqrt{(I : a)} = P\}. \]

Hence, \( \{P_1, \ldots, P_n\} = \{P'_1, \ldots, P'_{n'}\} \).

Let \( R \) be a commutative ring, and \( I \) be a decomposable ideal of \( R \). Let

\[ I = Q_1 \cap \cdots \cap Q_n \text{ with } \sqrt{Q_i} = P_i, \ i \in \{1, \ldots, n\} \]

be minimal primary decomposition of \( I \). By Theorem 46 \( P_1, \ldots, P_n \) are uniquely determined. We refer to \( P_1, \ldots, P_n \) as the **associated prime ideals** of \( I \) and write

\[ \text{ass}_R(I) = \{P_1, \ldots, P_n\}. \]

**Proposition 47.** Let \( R \) be a commutative ring, and let \( I \) be a decomposable ideal of \( R \). Let \( P \in \text{Spec}(R) \). Then \( P \) is a minimal prime ideal of \( I \) if and only if \( P \in \text{ass}_R(I) \) and \( P \) is minimal as a member of \( \text{ass}_R(I) \).
Proof. We begin with some notation. Let

\[ I = Q_1 \cap \cdots \cap Q_n \]

be a minimal primary decomposition of \( I \). Let

\[ P_1 = \sqrt{Q_1}, \ldots, P_n = \sqrt{Q_n} \]

so that

\[ \text{ass}_R(I) = \{P_1, \ldots, P_n\}. \]

We also note that

\[ I \subseteq \sqrt{I} = \sqrt{Q_1 \cap \cdots \cap Q_n} = \sqrt{Q_1} \cap \cdots \cap \sqrt{Q_n} = P_1 \cap \cdots \cap P_n. \]

Here we used the general rule \( \sqrt{J_1 \cap J_2} = \sqrt{J_1} \cap \sqrt{J_2} \) which was a previous homework exercise. It follows that \( I \subseteq P_i \) for \( i \in \{1, \ldots, n\} \).

( \implies \) Now assume that \( P \) is a minimal prime ideal of \( I \). We have \( I \subseteq P \). Hence,

\[ Q_1 \cap \cdots \cap Q_n \subseteq P. \]

By Lemma 31 there exists \( j \in \{1, \ldots, n\} \) such that \( Q_j \subseteq P_j \). Taking radicals, we have:

\[ \sqrt{Q_j} \subseteq \sqrt{P}, \quad P_j \subseteq P. \]

Here, \( \sqrt{P} = P \) by a previous homework exercise. Now \( I \subseteq P_j \subseteq P \). Since \( P \) is a minimal prime ideal of \( I \) we must have \( P = P_j \). Hence, \( P \in \text{ass}_R(I) \). We still need to prove that \( P \) is minimal as a member of \( \text{ass}_R(I) \). Suppose that \( P_i \in \text{ass}_R(I) \) is such that \( P_i \subseteq P \). Then \( I \subseteq P_i \subseteq P \). As \( P \) is a minimal prime ideal of \( I \) we obtain \( P = P_i \), so that \( P \) is minimal as a member of \( \text{ass}_R(I) \).

( \iff \) Assume that \( P \in \text{ass}_R(I) \) and that \( P \) is minimal as a member of \( \text{ass}_R(I) \). We need to prove that \( P \) is a minimal prime ideal of \( I \). Assume that \( P' \) is another prime ideal of \( I \), i.e., \( P' \) is a prime ideal containing \( I \), and \( I \subseteq P' \subseteq P \). By a previous homework exercise there exists a minimal prime ideal \( P'' \) of \( I \) such that \( P'' \subseteq P' \). Arguing as in the last paragraph, there exists \( j \in \{1, \ldots, n\} \) such that \( P_j \subseteq P'' \). We now have \( P_j \subseteq P'' \subseteq P' \subseteq P \). Since \( P_j, P \in \text{ass}_R(I) \) and \( P \) is minimal as a member of \( \text{ass}_R(I) \), we must have \( P_j = P \). Hence also \( P' = P \); this proves that \( P \) is a minimal prime ideal of \( R \).

Corollary 48. Let \( R \) be a commutative ring, and let \( I \) be a decomposable ideal of \( R \). Then \( I \) has finitely many minimal prime ideals.

Proof. By Proposition 47 every minimal prime ideal of \( I \) is contained in \( \text{ass}_R(I) \) which is a finite set.
Let $R$ be a commutative ring, and let $I$ be a decomposable ideal of $R$. We refer to the elements of $\text{ass}_R(I)$ that are minimal as members of $\text{ass}_R(I)$ as the **minimal primes** or **isolated primes** of $I$. The elements of $\text{ass}_R(I)$ that are not minimal are called the **embedded primes** of $I$.

**Example.** Let $K$ be a field and let $R = K[X,Y]$ where $X$ and $Y$ are indeterminates. Let

$$M = (X,Y), \quad P = (Y), \quad Q = (X,Y^2), \quad I = (XY,Y^2).$$

Then

$$I = Q \cap P \quad \text{and} \quad I = M^2 \cap P$$

where

(i) $M$ is maximal so that $M^2$ is primary.

(ii) $Q$ is $M$-primary.

(iii) $P$ is a prime ideal and hence primary.

Moreover, $I = Q \cap P$ and $I = M^2 \cap P$ are minimal primary decompositions and $\text{ass}_R(I) = \{P,M\}$.

**Proof.** First we prove that $I = Q \cap P$ and $I = M^2 \cap P$. We have

$$I = (XY,Y^2) \subseteq P = (Y),$$

$$I = (XY,Y^2) \subseteq M^2 = (X^2,XY,Y^2) \subseteq Q = (X,Y^2).$$

Hence,

$$I \subseteq M^2 \cap P \subseteq Q \cap P.$$

To prove that $I = Q \cap P = M^2 \cap P$ it will suffice to prove that $Q \cap P \subseteq I$. Let $f \in Q \cap P$. Since $f \in P$ we may write

$$f = gY$$

for some $g \in R$. Write

$$g = g_0 + g_1$$

where $g_0 \in K$ and every term of $g_1$ contains a positive power or $X$ or a positive power of $Y$. We claim that $g_0 = 0$. Assume that $g_0 \neq 0$; we will obtain a contradiction. Then

$$g_0Y = f - g_1Y$$

$$Y = g_0^{-1}f - g_0^{-1}g_1Y \in (Q \cap P) + I \subseteq Q \cap P \subseteq Q.$$
That is, \( Y \in Q \). Hence, for some \( a, b \in R \) we have

\[
Y = aX + bY^2.
\]

Taking \( X = 0 \), we find that \( Y = b(0,Y)Y^2 \), which is a contradiction. Since \( g_0 = 0 \), we get \( f = g_1Y \in I \). We have proven that

\[
I = M^2 \cap P = Q \cap P.
\]

The properties (i), (ii), and (iii) were proven in other examples. It is clear that \( I = M^2 \cap P \) and \( I = Q \cap P \) are primary decompositions. Now \( \sqrt{M^2} = M \) and \( \sqrt{P} = P \), and \( \sqrt{Q} = M \) and \( \sqrt{P} = P \). Since \( M \neq P \), these primary decompositions satisfy (i) of the definition of a minimal primary decomposition. It is also clear that

\[
M^2 \notin P, \quad P \notin M^2, \quad Q \notin P, \quad P \notin Q.
\]

Hence, \( I = M^2 \cap P \) and \( I = Q \cap P \) are minimal primary decompositions. Finally, \( \text{ass}_R(I) = \{M,P\} \).

**Theorem 49** (Second Uniqueness Theorem for Primary Decomposition). Let \( R \) be a commutative ring, and let \( I \) be a decomposable ideal of \( R \). Let \( \text{ass}_R(I) = \{P_1, \ldots, P_n\} \). Let

\[
I = Q_1 \cap \cdots \cap Q_n \quad \text{with} \quad \sqrt{Q_i} = P_i, \quad i \in \{1, \ldots, n\}
\]

and

\[
I = Q'_1 \cap \cdots \cap Q'_n \quad \text{with} \quad \sqrt{Q'_i} = P_i, \quad i \in \{1, \ldots, n\}
\]

be minimal primary decompositions of \( I \). If \( i \in \{1, \ldots, n\} \) and \( P_i \) is a minimal prime ideal of \( I \), then

\[
Q_i = Q'_i.
\]

**Proof.** We may assume that \( n > 1 \). Let \( i \in \{1, \ldots, n\} \) and assume that \( P_i \) is a minimal prime ideal of \( R \). Then

\[
\bigcap_{j=1 \atop j \neq i}^n P_j \notin P_i.
\]

(Otherwise \( \bigcap_{j=1 \atop j \neq i}^n P_j \subseteq P_i \) and hence by Lemma 31 we have \( P_j \subseteq P_i \) for some \( j \in \{1, \ldots, n\} \) with \( j \neq i \), contradicting the minimality of \( P_i \).) Hence, there exists \( a \in R \) such that

\[
a \in \bigcap_{j=1 \atop j \neq i}^n P_j \quad \text{and} \quad a \notin P_i.
\]
Let \( j \in \{1, \ldots, n\}, j \neq i \). Since \( a \in P_j = \sqrt{Q_j} \), there exists \( m_j \in \mathbb{N} \) such that \( a^{m_j} \in Q_j \). Let

\[
m = \max(m_1, \ldots, m_{i-1}, m_{i+1}, \ldots, m_n).
\]

Let \( t \geq m \). Since \( P_i \) is prime and \( a \notin P_i \) we also have \( a^t \notin P_i \). Now

\[
(I : a^t) = (\cap_{j=1}^n Q_j : a) = (Q_i : a^t) \cap \bigcap_{j=1}^n (Q_j : a^t) = Q_i \cap \bigcap_{j=1}^n R \quad \text{(Lemma 44)} = Q_i.
\]

Similarly, there exists \( m' \in \mathbb{N} \) such that if \( t \geq m' \), then

\[
(I : a^t) = Q_i'.
\]

Taking \( t \geq \max(m, m') \), we get

\[
Q_i = (I : a^t) = Q_i'.
\]

This completes the proof. \( \square \)

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

(i) \( I \) is proper, i.e., \( I \nsubseteq R \).

(ii) If \( I_1 \) and \( I_2 \) are ideals of \( R \) such that \( I = I_1 \cap I_2 \), then \( I = I_1 \) or \( I = I_2 \).

**Proposition 50.** Let \( R \) be a commutative ring. If \( R \) is Noetherian, then every proper ideal of \( R \) is the intersection of finitely many irreducible ideals.

**Proof.** Assume that \( R \) is Noetherian. Let \( X \) be the set of all proper ideals of \( R \) that are not the intersection of finitely many irreducible ideals of \( R \). We need to prove that \( X \) is empty. Assume that \( X \) is non-empty; we will obtain a contradiction. Since \( R \) is Noetherian \( X \) has a maximal element \( I \). The ideal \( I \) is not irreducible (otherwise \( I = I \cap I \) so that \( I \notin X \)). Since \( I \) is not irreducible, there exist ideals \( I_1 \) and \( I_2 \) of \( R \) such that \( I = I_1 \cap I_2 \) and

\[
I \nsubseteq I_1 \quad \text{and} \quad I \nsubseteq I_2.
\]

The ideals \( I_1 \) and \( I_2 \) are proper (otherwise, if \( I_1 = R \) for example, then \( I = R \cap I_2 = I_2 \), contradicting \( I \nsubseteq I_2 \)). Since \( I \nsubseteq I_1 \) and \( I \nsubseteq I_2 \) the maximality of \( I \) implies that \( I_1 \notin X \) and \( I_2 \notin X \). Since \( I_1 \notin X \) and \( I_2 \notin X \) the ideals \( I_1 \) and \( I_2 \) can be written as intersections of irreducible ideals. This implies that \( I \) is the intersection of irreducible ideals, a contradiction. \( \square \)
Proposition 51. Let $R$ be a commutative ring. Assume that $R$ is Noetherian. If $I$ is an irreducible ideal of $R$, then $I$ is primary.

Proof. Let $I$ be an irreducible ideal of $R$. Then $I \subseteq R$. Let $a, b \in R$ be such that $ab \in I$ and $a \notin I$. We need to prove that $b \in \sqrt{I}$. Consider the sequence of ideals

$$(I : b) \subseteq (I : b^2) \subseteq (I : b^3) \subseteq \cdots$$

Since $R$ is Noetherian, there exists $n \in \mathbb{N}$ such that $(I : b^n) = (I : b^m)$ for $m \geq n$. Using this, we will prove that

$$I = (I + Ra) \cap (I + Rb^n).$$

Clearly, $I \subseteq (I + Ra) \cap (I + Rb^n)$. Let $r \in (I + Ra) \cap (I + Rb^n)$. Then

$$r = x_1 + r_1a = x_2 + r_2b^n$$

for some $x_1, x_2 \in I$ and $r_1, r_2 \in R$. Solving for $r_2b^n$ we have

$$r_2b^n = x_1 + r_1a - x_2.$$  

Multiplying by $b$ we obtain

$$r_2b^{n+1} = x_1b + r_1ab - x_2b.$$  

Since $x_1, x_2 \in I$ and $ab \in I$, it follows that $r_2b^{n+1} \in I$. This means that $r_2 \in (I : b^{n+1}) = (I : b^n)$. Since $r_2 \in (I : b^n)$ we have

$$r = x_2 + r_2b^n \in I.$$  

This proves the equality

$$I = (I + Ra) \cap (I + Rb^n).$$

Since $I$ is irreducible we now have

$$I = I + Ra \quad \text{or} \quad I = I + Rb^n.$$  

We cannot have $I = I + Ra$ (otherwise $a \in I$). Therefore, $I = I + Rb^n$, which implies that $b^n \in I$. □

Theorem 52. Let $R$ be a commutative ring. If $R$ is Noetherian, then every proper ideal of $R$ is decomposable, i.e., has a primary decomposition.

Proof. This follows immediately from Proposition 50 and Proposition 51. □
5 Rings of Fractions

Let $R$ be a commutative ring. We will now consider a method for constructing a new ring from $R$ by “inverting” some of the elements of $F$. The main application of this will be to simplify situations involving prime ideals via a technique called “localization”.

Let $R$ be a commutative ring. Let $S$ be a subset of $R$. We recall that $S$ is said to be \textit{multiplicatively closed} if

(i) $1 \in S$.

(ii) If $s_1, s_2 \in S$, then $s_1 s_2 \in S$.

The following is a very important example of a multiplicatively closed set.

\textbf{Example}. Let $R$ be a commutative ring, and let $P$ be a prime ideal of $R$. Let $S = R - P (= R \setminus P)$. Then $S$ is a multiplicatively closed subset of $R$.

\textit{Proof}. Clearly, $1 \in S$ (otherwise, $1 \in P$ so that $P = R$, a contradiction). Let $s_1, s_2 \in S$. Then $s_1 s_2 \in S$ (otherwise $s_1 s_2 \in P$ so that $s_1 \in P$ or $s_2 \in P$, a contradiction).

\textbf{Lemma 53}. Let $R$ be a commutative ring, and let $S$ be a multiplicatively closed subset of $R$. Define a relation $\sim$ on $R \times S$ by declaring

$$(a, s) \sim (b, t) \text{ if and only if there exists } u \in S \text{ such that } u(at - bs) = 0.$$ 

Then $\sim$ is an equivalence relation.

\textit{Proof}. We need to prove that $\sim$ is reflexive, symmetric, and transitive.

$\sim$ is reflexive. Let $(a, s) \in R \times S$. We need to prove that $(a, s) \sim (a, s)$. Now $1(as - as) = 0$, which means that $(a, s) \sim (a, s)$.

$\sim$ is symmetric. Let $(a, s), (b, t) \in R \times S$, and assume that $(a, s) \sim (b, t)$; we need to prove that $(b, t) \sim (a, s)$. Since $(a, s) \sim (b, t)$, there exists $u \in S$ such that $u(at - bs) = 0$. Hence, $u(bs - at) = 0$. This implies that $(b, t) \sim (a, s)$.

$\sim$ is transitive. Let $(a_1, s_1), (a_2, s_2), (a_3, s_3) \in R \times S$ and assume that $(a_1, s_1) \sim (a_2, s_2)$ and $(a_2, s_2) \sim (a_3, s_3)$. We need to prove that $(a_1, s_1) \sim (a_3, s_3)$. Let $u, v \in S$ be such that $u(a_1 s_2 - a_2 s_1) = 0$ and $v(a_2 s_3 - a_3 s_2) = 0$. Then

$$ua_1 s_2 = ua_2 s_1,$$

$$va_2 s_3 = va_3 s_2.$$ 

Multiplying the first equation by $vs_3$ and the second equation by $us_1$ we obtain:

$$vs_3 ua_1 s_2 = vs_3 ua_2 s_1,$$

$$us_1 va_2 s_3 = us_1 va_3 s_2.$$ 

43
This implies that
\[ vs_3u_1s_2 = us_1va_3s_2, \]
or equivalently,
\[ uvs_2(a_1s_3 - a_3s_1). \]
Since \( uvs_2 \in S \) we obtain \((a_1, s_1) \sim (a_3, s_3)\).

**Proposition 54.** Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset \( R \). For \((a, s) \in R \times S\) we denote the equivalence class determined by \((a, s)\) by \( a/s \) or \( a \cdot s^{-1} \) with respect to the equivalence relation \( \sim \) from Lemma 53. Let \( S^{-1}R \) be the set of all equivalence classes of \( \sim \) on \( S^{-1}R \). Define
\[ + : S^{-1}R \times S^{-1}R \to R, \quad \cdot : S^{-1}R \times S^{-1}R \to R \]
by
\[ a/s + b/t = (at + bs)/st, \]
\[ a/s \cdot b/t = ab/st \]
for \( a/s, b/t \in S^{-1}R \). The binary operations \( + \) and \( \cdot \) are well-defined, and with these binary operations \( S^{-1}R \) is a commutative ring with additive identity \( 0_{S^{-1}R} = 0/1 \) and multiplicative identity \( 1_{S^{-1}R} = 1/1 \).

**Proof.** We first verify that addition is well-defined. Suppose that \( a_1/s_1, a_2/s_2, b_1/t_1 = b_2/t_2 \in S^{-1}R \) with \( a_1/s_1 = a_2/s_2 \) and \( b_1/t_1, b_2/t_2 \); we need to prove that \((a_1t_1 + s_1b_1)/s_1t_1 = (a_2t_2 + s_2b_2)/s_2t_2\). Since \( a_1/s_1 = a_2/s_2 \), there exists \( u \in S \) such that
\[ ua_1s_2 = ua_2s_1 \tag{1} \]
and \( v \in S \) such that
\[ vb_1t_2 = vb_2t_1. \tag{2} \]
Multiplying (1) by \( vt_1t_2 \) we obtain
\[ vt_1t_2ua_1s_2 = vt_1t_2ua_2s_1 \]
and multiplying (2) by \( us_1s_2 \) we get
\[ us_1s_2vt_2b_1 = us_1s_2vt_1b_2. \]
Adding and factoring gives
\[ uvs_2t_2(a_1t_1 + b_1s_1) = uvs_1t_1(a_2t_2 + b_2s_2) \]
or equivalently,
\[ uv(s_2t_2(a_1t_1 + b_1s_1) - s_1t_1(a_2t_2 + b_2s_2)) = 0. \]

This implies that
\[ \frac{(a_1t_1 + b_1s_1)}{s_1t_1} = \frac{(a_2t_2 + b_2s_2)}{s_2t_2} \]
which is the desired result. We leave the remaining checks as an exercise. \( \square \)

We refer to \( S^{-1}R \) as the **ring of fractions of \( R \) with respect to \( S \).**

What happens if we divide by zero?

**Lemma 55.** Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset of \( R \). If \( 0 \in S \), then \( S^{-1}R \) is the trivial ring.

**Proof.** Assume that \( 0 \in S \). Let \( a/s \in S^{-1}R \). Then \( 1 \cdot (a \cdot 0 - 0 \cdot s) = 0 \) so that \( a/s = 0/0 \). Thus \( S^{-1}R \) consists of just one element \( 0/0 \) and is thus \( S^{-1}R \) is the trivial ring. \( \square \)

How is \( R \) related to \( S^{-1}R \)?

**Lemma 56.** Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset of \( R \). Define

\[ f : R \rightarrow S^{-1}R \]

by
\[ f(r) = r/1, \quad r \in R. \]

Then \( f \) is a ring homomorphism and:

(i) If \( s \in S \), then \( f(s) \) is a unit in \( S^{-1}R \).
(ii) If \( a \in \ker(f) \), then there exists \( s \in S \) such that \( sa = 0 \).
(iii) Every element of \( S^{-1}R \) is of the form \( f(a)f(s)^{-1} \) for some \( a \in R \) and \( s \in S \).

**Proof.** First we verify that \( f \) is a ring homomorphism. We have \( f(1) = 1/1 = 1_{S^{-1}R} \). Let \( a, b \in R \).

Then
\[ f(a + b) = (a + b)/1 = a/1 + b/1 = f(a) + f(b) \]

and
\[ f(ab) = ab/1 = a/1 \cdot b/1 = f(a)f(b). \]

This proves that \( f \) is a ring homomorphism.

(i) Let \( s \in S \). Then
\[ f(s) \cdot (1/s) = s/1 \cdot 1/s = s/s = 1/1 = 1_{S^{-1}R}. \]

Thus, \( f(s) \) is a unit.

(ii) Let \( a \in \ker(f) \). Then \( 0/1 = f(a) = a/1 \). This implies that there exists \( s \in S \) such that \( sa = 0 \).

(iii) Let \( a/s \in S^{-1}R \). Then
\[ a/s = a/1 \cdot 1/s = a/1 \cdot (s/1)^{-1} = f(a)f(s)^{-1}. \]
This completes the proof.

We refer to the ring homomorphism \( f : R \rightarrow S^{-1}R \) from Lemma 56 as the **natural map**.

**Lemma 57.** Let \( R \) be an integral domain and let \( S \) be a multiplicatively closed subset of \( R \) such that \( 0 \notin S \). Then the natural map \( f : R \rightarrow S^{-1}R \) is injective.

**Proof.** Let \( a \in \ker(f) \). Then \( f(a) = a/1 = 0/1 \). This implies that there exists \( u \in S \) such that \( u(a \cdot 1 - 0 \cdot 1) = 0 \), i.e., \( ua = 0 \). Since \( R \) is an integral domain and \( 0 \notin S \), we must have \( a = 0 \). Hence, \( \ker(f) = 0 \), and \( f \) is injective.

**Example.** Let \( R \) be an integral domain, and let \( S = R - \{0\} \). If \( a/s, b/t \in S^{-1}R \), then \( a/s = b/t \) if and only if \( at = bs \). In this case \( S^{-1}R \) is called the **quotient field** of \( R \), and by Lemma 57, \( R \) is included in \( S^{-1}R \) via the natural map.

**Proof.** Let \( a/s, b/t \in S^{-1}R \) and assume that \( a/s = b/t \). Then there exists \( u \in S \) such that \( u(at - bs) = 0 \). Since \( R \) is an integral domain, \( u = 0 \) or \( at - bs = 0 \); but \( 0 \notin S \); hence, \( at = bs \). It is clear that \( at = bs \) implies that \( a/s = b/t \).

**Proposition 58 (Universal property of \( S^{-1}R \)).** Let \( R \) be a commutative ring, let \( S \) be a multiplicatively closed subset of \( R \), and let \( f : R \rightarrow S^{-1}R \) be the natural homomorphism. Let \( R' \) be a commutative ring and let \( g : R \rightarrow R' \) be a ring homomorphism such that \( g(s) \) is a unit for \( s \in S \). Then there exists a unique ring homomorphism \( h : S^{-1}R \rightarrow R' \) such that

\[
\begin{array}{ccc}
R & \xrightarrow{f} & S^{-1}R \\
\downarrow & & \downarrow \\
R' & & \\
\end{array}
\]

commutes, i.e., \( h \circ f = g \). We have \( h(a/s) = g(a)g(s)^{-1} \) for \( a/s \in S^{-1}R \).

**Proof.** Define \( h : S^{-1}R \rightarrow R' \) by \( h(a/s) = g(a)g(s)^{-1} \) for \( a/s \in S^{-1}R \). We first prove that \( h \) is well-defined. Let \( a_1/s_1, a_2/s_2 \in S^{-1}R \) be such that \( a_1/s_1 = a_2/s_2 \); we need to prove that \( g(a_1)g(s_1)^{-1} = g(a_2)g(s_2)^{-1} \). Since \( a_1/s_1 = a_2/s_2 \) there exists \( u \in S \) such that \( u(a_1s_2 - a_2s_1) = 0 \). Applying \( g \), we obtain

\[
g(u)(g(a_1)g(s_2) - g(a_2)g(s_1)) = 0.
\]

Since \( g(u) \) is a unit in \( R' \) we may multiply by \( g(u)^{-1} \in R' \) to obtain

\[
g(a_1)g(s_2) - g(a_2)g(s_1) = 0
\]

\[
g(a_1)g(s_2) = g(a_2)g(s_1).
\]

Since \( g(s_1) \) and \( g(s_2) \) are units in \( S \), we have

\[
g(a_1)g(s_1)^{-1} = g(a_2)g(s_2)^{-1}.
\]

46
This proves that \( h \) is well-defined. Next we prove that \( h \) is a ring homomorphism. We have

\[
h(1_{S^{-1}R}) = h(1/1) = g(1)g(1)^{-1} = 1.\]

Let \( a_1/s_1, a_2/s_2 \in S^{-1}R \). Then

\[
h(a_1/s_1 + a_2/s_2) = h((a_1s_2 + a_2s_1)/s_1s_2) = g(a_1s_2 + a_2s_1)g(s_1s_2)^{-1} = g(a_1)g(s_2)g(s_1)^{-1}g(s_2)^{-1} + g(a_2)g(s_1)g(s_1)^{-1}g(s_2)^{-1} = g(a_1)g(s_1)^{-1} + g(a_2)g(s_2)^{-1} = h(a_1/s_1) + h(a_2/s_2).
\]

Also,

\[
h(a_1/s_1 \cdot a_2/s_2) = h(a_1a_2/s_1s_2) = g(a_1a_2)g(s_1s_2)^{-1} = g(a_1)g(a_2)g(s_1)^{-1}g(s_2)^{-1} = h(a_1/s_1)h(a_2/s_2).
\]

This completes the proof that \( h \) is a ring homomorphism. Next, we prove the diagram commutes. Let \( r \in R \). Then

\[
(h \circ f)(r) = h(f(r)) = h(r/1) = g(r)g(1)^{-1} = g(r).
\]

Thus, \( h \circ f = g \). Finally, we prove that \( h \) is unique. Assume that \( h' : S^{-1}R \rightarrow R' \) is a ring homomorphism such that \( h' \circ f = g \). Let \( r \in R \). Then

\[
(h' \circ f)(r) = g(r) \\
h'(r/1) = g(r).
\]

Also, let \( s \in S \). Then

\[
h'(s/1) = g(s) \\
h'(s/1)^{-1} = g(s)^{-1} \\
h'(((s/1)^{-1}) = g(s)^{-1} \\
h'(1/s) = g(s)^{-1}.
\]
Hence, if \( r/s \in S^{-1}R \) we have

\[
h'(r/s) = h'(r/1 \cdot 1/s) = h'(r/1)h'(1/s) = g(r)g(s)^{-1} = h(r/s).
\]

Thus, \( h' = h \). \( \square \)

Let \( R \) be a commutative ring. We recall that an \( R \)-algebra \( A \) is a ring \( A \) (with identity, but not necessarily commutative) along with a ring homomorphism \( f : R \to A \). The homomorphism \( f : R \to A \) is call the \textbf{structural ring homomorphism} of the \( R \)-algebra \( A \). Let \( A_1 \) and \( A_2 \) be \( R \)-algebras with structural ring homomorphisms \( f_1 : R \to A_1 \) and \( f_2 : R \to A_2 \). A \( R \)-\textbf{algebra homomorphism} \( h : A_1 \to A_2 \) is a ring homomorphism such that the

\[
h(f_1(r)) = f_2(r)h(a)
\]

for \( r \in R \) and \( a \in A_2 \); also, \( h \) is an \textbf{isomorphism of \( R \)-algebras} if \( h \) is additionally a bijection.

Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset of \( R \). We may regard \( S^{-1}R \) as an \( R \)-algebra via the structural ring homomorphism given as the natural map \( f : R \to S^{-1}R \). We can characterize \( S^{-1}R \) as an \( R \)-algebra.

**Proposition 59.** Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset of \( R \). Let \( R' \) be a commutative \( R \)-algebra with structural ring homomorphism \( g : R \to R' \) such that

(i) For all \( s \in S \), \( g(s) \) is a unit in \( R' \).

(ii) If \( a \in \ker(g) \), then there exists \( s \in S \) such that \( sa = 0 \).

(iii) Every element of \( R' \) can be written in the form \( g(a)g(s)^{-1} \) for some \( a \in R \) and \( s \in S \).

Then there exists a unique isomorphism of \( R \) algebras \( h : S^{-1}R \to R' \).

**Proof.** Since (i) holds, by Proposition 58 there exists a unique ring homomorphism \( h : S^{-1}R \to R' \) such that

\[
\begin{array}{ccc}
R & \xrightarrow{f} & S^{-1}R \\
g \searrow & & \downarrow \\
& & R'
\end{array}
\]

commutes, i.e., \( h \circ f = g \). We also recall that \( h \) is given by \( h(a/s) = g(a)g(s)^{-1} \) for \( a/s \in S^{-1}R \).

We claim that \( h \) is an isomorphism of \( R \) algebras. We already know that \( h \) is a ring homomorphism. Let \( r \in R \) and \( a/s \in S^{-1}R \). Then

\[
h(f(r) \cdot a/s) = h(r/1 \cdot a/s)
\]

\[
= h(ra/s)
\]

\[
= g(ra)g(s)^{-1}
\]

\[
= g(r)g(a)g(s)^{-1}
\]

\[
= g(r)h(a/s).
\]
This proves that $h$ is a homomorphism of $R$-algebras. It remains to prove that $h$ is injective and surjective. To prove that $h$ is injective it suffices to prove that $\ker(h) = 0$. Let $a/s \in \ker(h)$. Then $h(a/s) = g(a)g(s)^{-1}$ 

$0 = g(a)g(s)^{-1}$ 

$0 = g(a)$.

Since $g(a) = 0$, by (ii) there exists $t \in S$ such that $ta = 0$. Now $a/s = ta/ts = 0/ts = 0$. It follows that $\ker(h) = 0$. To prove that $h$ is surjective, let $x \in R'$. By (iii), there exist $a \in R$ and $s \in S$ such that $g(a)g(s)^{-1} = x$. Now $h(a/s) = g(a)g(s)^{-1} = x$.

This proves that $h$ is surjective. \hfill $\Box$

Let $R$ be a commutative ring. If $R$ has exactly one maximal ideal $M$ then we say that $R$ is a **quasi-local ring** (typically, this is actually called a local ring, though not in our text). If $R$ is a local ring with maximal ideal $M$, then we call $R/M$ the residue field of $R$.

**Example.** If $F$ is a field, then $F$ is a quasi-local ring, with unique maximal ideal 0; the residue field of $F$ is just $F = F/0$.

**Lemma 60.** Let $R$ be a commutative ring. Then $R$ is quasi-local if and only if the set of non-units of $R$ is an ideal; in this case

$$\{ r \in R : r \text{ is a non-unit} \}$$

is the unique maximal ideal of $R$.

**Proof.** Let $J = \{ r \in R : r \text{ is a non-unit} \}$. Assume that $R$ is quasi-local, and let $M$ be the unique maximal ideal of $R$. We claim that $J = M$. Clearly, as $M$ is proper (and hence does not contain a unit), $M \subseteq J$. Let $r \in J$. Consider $(r)$. Since $r$ is a non-unit, $(r)$ is a proper ideal. Therefore, $(r)$ is included in a maximal ideal of $R$ which must be $M$. This means that $r \in M$. We have proven that $M = J$ which implies that $J$ is an ideal. Now assume that $J$ is an ideal. The ideal $J$ must be proper since $1 \notin J$. Let $M$ be a maximal ideal of $R$. Since $M$ is proper, every element of $M$ is a non-unit. Therefore, $M \subseteq J$. But $M$ is maximal; hence, $M = J$. It follows that $R$ is quasi-local. \hfill $\Box$

**Proposition 61.** Let $R$ be a commutative ring, and let $P$ be a prime ideal of $R$. Set $S = R - P$. Then $S^{-1}R$ is a quasi-local ring with maximal ideal

$$\{ x \in S^{-1}R : x = a/s \text{ for some } a \in P \text{ and } s \in S \}.$$

**Proof.** Define

$$J = \{ x \in S^{-1}R : x = a/s \text{ for some } a \in P \text{ and } s \in S \}.$$
By Lemma 60, it will suffice to prove that \( J \) is the set of non-units of \( S^{-1}R \) and that \( J \) is an ideal. Let \( x \in J \), and let \( a \in P \) and \( s \in S \) be such that \( x = a/s \). Assume that \( x \) is a unit; we will obtain a contradiction. Let \( b/t \in S^{-1}R \) be such that \( a/s \cdot b/t = 1 \). Then \( ab/st = 1/1 \). This implies that there exists \( u \in S \) such that \( u(ab - st) = 0 \), i.e., \( uab = ust \). Now \( u, s, t \in S \). Hence, \( ust \in S \). This implies that \( uab \in P \). But \( a \in P \); hence, \( uab \in P \). This is a contradiction. It follows that every element of \( J \) is a non-unit. Now assume that \( a/s \in S^{-1}R \) and \( a/s \) is a non-unit. We claim that \( a \in P \). Assume that \( a \notin P \), i.e., \( a \in S \); we will obtain a contradiction. Since \( a \in S \) we have \( s/a \in S^{-1}R \). Now \( s/a \cdot a/s = as/as = 1/1 = 1_{S^{-1}R} \). Thus, \( a/s \) is a unit, a contradiction. Therefore, \( a/s \in J \). We conclude that \( J \) is the set of non-units. It is straightforward to verify that \( J \) is an ideal, which concludes the proof.

If \( R \) is a commutative ring, \( P \) is a prime ideal of \( R \), and \( S = R - P \), then we denote the ring of fractions \( S^{-1}R \) of \( R \) with respect to \( S \) by \( R_P \), refer to \( R_P \) as the localization of \( R \) at \( P \).

The next lemma shows that localizing at the maximal ideal of a quasi-local ring produces essentially the same ring.

**Lemma 62.** Let \( R \) be a quasi-local commutative ring with maximal ideal \( M \). The natural map \( f : R \rightarrow R_M \) is an isomorphism of rings.

**Proof.** We need to prove that \( f \) is injective and surjective. Assume that \( a \in \ker(f) \). Then \( a/1 = 0 \). This implies that there exists \( u \in S = R - M \) such that \( ua = 0 \). By Lemma 60 the element \( u \) is a unit. This implies that \( a = u^{-1}ua = 0 \). Hence, \( \ker(f) = 0 \). To see that \( f \) is surjective, let \( a/s \in R_M \). Since \( s \in S \), \( s \) is a unit in \( R \). We have

\[
  f(as^{-1}) = f(a)f(s^{-1}) = f(a)f(s)^{-1} = a/1 \cdot (s/1)^{-1} = a/1 \cdot 1/s = a/s.
\]

It follows that \( f \) is surjective, and thus an isomorphism.

Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset of \( R \). Let \( f : R \rightarrow S^{-1}R \) be the natural map. As usual, with respect to \( f \) we have the extension and contraction maps:

- \( I \) ideal of \( R \mapsto I^e = (f(I)) \), an ideal of \( S^{-1}R \),
- \( J^c = f^{-1}(J) \), an ideal of \( R \leftrightarrow J \) an ideal of \( S^{-1}R \).

We will use these maps to understand the ideals of \( S^{-1}R \) and especially the prime and primary ideals of \( S^{-1}R \).

**Lemma 63.** Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset of \( R \). If \( J \) is an ideal of \( S^{-1}R \), then

\[
  J = (J^c)^e.
\]

**Proof.** We have

\[
  (J^c)^e = (f(f^{-1}(J))) \subseteq (J) = J.
\]
For the converse inclusion, let \( a/s \in J \). To prove that \( a/s \in (J^c)^e \) we first prove that \( a \in J^c = f^{-1}(J) \). Since \( a/s \in J \), we have \( s/1 \cdot a/s = a/1 \in J \), that is \( f(a) \in J \). This implies that \( a \in J^c = f^{-1}(J) \). Since \( a \in J^c \), \( 1/s \cdot f(a) \in (f(J^c)) = (J^c)^e \), i.e., \( a/s \in (J^c)^e \). Hence, \( J \subseteq (J^c)^e \). □

From the lemma we see that every ideal in \( S^{-1}R \) is an extension of an ideal in \( R \). We now describe the extensions of ideals of \( R \) more closely.

**Lemma 64.** Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset of \( R \). Let \( f : R \to S^{-1}R \) be the natural map, and define extension of ideals with respect to \( f \). Let \( I \) be an ideal of \( R \). Then

\[
I^e = \{ y \in S^{-1}R : y = a/s \text{ for some } a \in I \text{ and } s \in S \}.
\]

**Proof.** Let \( y \in I^e \). By the definition of \( I^e \), there exist \( a_1/s_1, \ldots, a_n/s_n \in S^{-1}R \) and \( b_1, \ldots, b_n \in I \) such that

\[
y = a_1/s_1 \cdot f(b_1) + \cdots + a_n/s_n \cdot f(b_n)
= a_1/s_1 \cdot b_1/1 + \cdots + a_n/s_n \cdot b_n/1
= a_1b_1/s_1 + \cdots + a_nb_n/s_n
= (a_1b_1s_2 \cdots s_n)/s_1 \cdots s_n + \cdots + (a_nb_n s_1 \cdots s_{n-1})/s_1 \cdots s_n
= (a_1b_1s_2 \cdots s_n + \cdots + a_nb_n s_1 \cdots s_{n-1})/s_1 \cdots s_n
\]

Since \( I \) is an ideal, and \( b_1, \ldots, b_n \in I \),

\[
a_1b_1s_2 \cdots s_n + \cdots + a_nb_n s_1 \cdots s_{n-1} \in I.
\]

This proves that \( I^e \) is contained in \( \{ y \in S^{-1}R : y = a/s \text{ for some } a \in I \text{ and } s \in S \} \). Conversely, let \( y \in \{ y \in S^{-1}R : y = a/s \text{ for some } a \in I \text{ and } s \in S \} \). Let \( a \in I \) and \( s \in S \) be such that \( y = a/s \). Then

\[
y = a/s = a/1 \cdot 1/s = 1/s \cdot f(a) \in (f(I)) = I^e.
\]

Hence, \( \{ y \in S^{-1}R : y = a/s \text{ for some } a \in I \text{ and } s \in S \} \subseteq I^e \). This completes the proof. □

**Example.** Let the notation be as in Lemma 64. It is important to realize that if \( b/t \in I^e \), then it does not follow that \( b \in I \). For example, let \( R = \mathbb{Z} \), and let \( S = \{3^n : n \in \mathbb{N}_0\} \). Then \( S^{-1}R \) is the ring of all rational numbers of the form \( a/3^n \) for some \( a \in \mathbb{Z} \) and \( n \in \mathbb{N}_0 \). Let \( I = (6) = 6\mathbb{Z} \). Then

\[
2/3 = 2/3 \cdot 3/3 = 6/9 \in I^e
\]

where the last step follows from Lemma 64. But \( 2 \notin I \).
Lemma 65. Let $R$ be a commutative ring, let $S$ be a multiplicatively closed subset of $R$, and let $f : R \to S^{-1}R$ be the natural map. Define extension of ideals with respect to $f$. Let $Q$ be a primary ideal of $R$ and assume that $Q \cap S = \emptyset$. If $a/s \in Q^e$, then $a \in Q$. Moreover, $(Q^e)^c = Q$.

Proof. Let $a \in R$ and $s \in S$ be such that $a/s \in Q^e$. By Lemma 64, there exist $b \in Q$ and $t \in S$ such that $a/s = b/t$. Let $u \in S$ be such that $u(at - bs) = 0$. Then $a(ut) = usb \in Q$. Let $n \in \mathbb{N}$, and consider $(ut)^n$. We have $ut \in S$ and so $(ut)^n \in S$. Also, $S \cap Q = \emptyset$. This implies that $(ut)^n \notin Q$. It follows that $ut \notin \sqrt{Q}$. Since $Q$ is primary, we must have $a \in Q$ as desired.

Next, $Q \subseteq f^{-1}(f(Q)) \subseteq (Q^e)^c$. Conversely, let $a \in (Q^e)^c$. Then $f(a) = a/1 \in Q^e$. By the first paragraph, $a \in Q$. Hence $(Q^e)^c \subseteq Q$ and so $Q = (Q^e)^c$. \hfill \Box

Lemma 66. Let $R$ be a commutative ring, let $S$ be a multiplicatively closed subset of $R$, and let $f : R \to S^{-1}R$ be the natural map. Define extension of ideals with respect to $f$. Let $I$ and $J$ be ideals of $R$. Then

(i) $(I + J)^e = I^e + J^e$.
(ii) $(IJ)^e = I^e J^e$.
(iii) $(I \cap J)^e = I^e \cap J^e$.
(iv) $(\sqrt{I})^e = \sqrt{I^e}$.
(v) $I^e = S^{-1}R$ if and only if $I \cap S \neq \emptyset$.

Proof. (i) and (ii) were previous homework exercises and hold generally.

(iii) We first that $(I \cap J)^e \subseteq I^e \cap J^e$. Since $I \cap J \subseteq I$, we have $f(I \cap J) \subseteq f(I)$. Similarly, $f(I \cap J) \subseteq f(J)$. Therefore, $f(I \cap J) \subseteq f(I) \cap f(J) \subseteq I^e \cap J^e$. This implies that $I \cap J)^e \subseteq I^e \cap J^e$.

Next, let $y \in I^e \cap J^e$. By Lemma 64, there exist $a \in I, b \in J$, and $s, t \in S$ such that $y = a/s = b/t$. Since $a/s = b/t$, there exists $u \in S$ such that $u(at - bs) = 0$. Hence, $uat = ubs$. Let $x = uta = usb$. Then $x \in I \cap J$. Moreover,

$$y = a/s = a/s \cdot ut/ut = uta/uts = x/uts \in (I \cap J)^e$$

where the last step follows by Lemma 64. Hence, $I^e \cap J^e \subseteq (I \cap J)^e$. This completes the proof that $(I \cap J)^e = I^e \cap J^e$.

(iv) Let $y \in (\sqrt{I})^e$. Then by Lemma 64, there exist $a \in \sqrt{I}$ and $s \in S$ such that $y = a/s$. Let $n \in \mathbb{N}$ be such that $a^n \in I$. We have $y^n = a^n/s^n \in I^e$ again by Lemma 64. Hence, $y \in \sqrt{I^e}$. Thus, $(\sqrt{I})^e \subseteq \sqrt{I^e}$. Conversely, let $y \in \sqrt{I^e}$. Let $n \in \mathbb{N}$ be such that $y^n \in I^e$. Let $a \in R$ and $s \in S$ be such that $y = a/s$. Then $y^n = a^n/s^n \in I^e$. Hence, by Lemma 64, there exists $b \in I$ and $t \in S$ such that $y^n = a^n/s^n = b/t$. Let $u \in S$ be such that $u(a^n t - bs^n) = 0$, i.e., $u a^n t = u b s^n$. We have $u a^n t = u b s^n \in I$ because $b \in I$. Now

$$(uts)^n = u^{n-1} a^{n-1} (uts^n) \in I.$$
It follows that \( uta \in \sqrt{I} \). Hence,

\[
y = a/s = uta/uts \in (\sqrt{I})^e
\]

where the last step follows by Lemma 64. This proves that \( \sqrt{I^e} \subseteq (\sqrt{I})^e \), so that \( (\sqrt{I})^e = \sqrt{I^e} \).

(v) Assume that \( I^e = S^{-1}R \). Then \( 1/1 \in I^e \). By Lemma 64, this implies that there exists \( a \in I \) and \( s \in S \) such that \( 1/1 = a/s \). Let \( u \in S \) be such that \( us = ua \in I \cap S \). Thus, \( I \cap S \neq \emptyset \). Conversely, assume that \( I \cap S \neq \emptyset \). Let \( s \in I \cap S \). Then \( 1_{S^{-1}R} = 1/1 = s/s \in I^e \) by Lemma 64. Hence, \( I^e = S^{-1}R \). \( \square \)

**Theorem 67.** Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset of \( R \). Let \( f : R \to S^{-1}R \) be the natural map, and define extension and contraction with respect to \( f \). Then the map

\[
\{P \in \text{Spec}(R) : P \cap S = \emptyset\} \xrightarrow{\text{extension}} \text{Spec}(S^{-1}R)
\]

defined by extension of ideals is bijection, with inverse given by the contraction of ideals map

\[
\text{Spec}(S^{-1}R) \xrightarrow{\text{contraction}} \{P \in \text{Spec}(R) : P \cap S = \emptyset\}.
\]

**Proof.** We first prove that the extension map is well-defined. Let \( P \in \text{Spec}(R) \), and assume that \( P \cap S = \emptyset \). We need to prove that \( P^e \in \text{Spec}(S^{-1}R) \). Let \( a/s, b/t \in S^{-1}R \), and assume that \( a/s \cdot b/t = ab/st \in P^e \). By Lemma 65 we have \( ab \in P \). Since \( P \) is prime, \( a \in P \) or \( b \in P \). If \( a \in P \), then \( a/s \in P^e \) by Lemma 64; if \( b \in P \), then \( b/t \in P^e \) by Lemma 64. It follows that \( P^e \) is prime so that the extension map is well-defined.

Next, we prove that the contraction map is well-defined. Let \( P' \in \text{Spec}(S^{-1}R) \); we need to prove that \( (P')^c \) is prime and that \( (P')^c \cap S = \emptyset \). To see that \( (P')^c \) is prime, let \( a, b \in R \) and assume that \( ab \in (P')^c \). Then \( f(ab) = f(a)f(b) \in P' \). Since \( P' \) is prime we have \( f(a) \in P' \) or \( f(b) \in P' \), i.e., \( a \in (P')^e \) or \( b \in (P')^e \); thus, \( (P')^e \) is prime. Assume that \( (P')^c \cap S \neq \emptyset \); we will obtain a contradiction. Since \( (P')^c \cap S \neq \emptyset \), we have \( ((P')^c)^e = S^{-1}R \) by Lemma 66. Also, by Lemma 63, \( ((P')^c)^e = P' \). Hence, \( P' = S^{-1}R \). This is a contradiction because \( P' \) is prime, and hence proper. We have prove that the contraction map is well-defined.

To complete the proof we need to prove that the two maps are inverses of each other. By Lemma 65 we have \( (P')^c = P \) if \( P \in \{P \in \text{Spec}(R) : P \cap S = \emptyset\} \) and by Lemma 63, \( ((P')^c)^e = P' \) if \( P' \in \text{Spec}(S^{-1}R) \). \( \square \)

**Theorem 68.** Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset of \( R \). Let \( f : R \to S^{-1}R \) be the natural map. The map

\[
\{Q \text{ is a primary ideal of } R \text{ such that } Q \cap S = \emptyset\} \xrightarrow{\text{extension}} \{Q' \text{ is a primary ideal of } S^{-1}R\}
\]
defined by extension of ideals is bijection, with inverse given by the contraction of ideals map

\[ \{ Q' \text{ is a primary ideal of } S^{-1}R \} \xrightarrow{\text{contraction}} \{ Q \text{ is a primary ideal of } R \text{ such that } Q \cap S = \emptyset \}. \]

Moreover, if \( Q \) is primary ideal of \( R \) such that \( Q \cap S = \emptyset \), and \( P = \sqrt{Q} \), then \( \sqrt{Q^e} = P^e \).

Proof. We first prove that the extension map is well-defined. Let \( Q \) be a primary ideal of \( R \) such that \( Q \cap S = \emptyset \); we need to prove that \( Q^e \) is primary. Assume that \( a/s, b/t \in S^{-1}R \) are such that \( a/s \cdot b/t = ab/st \in Q^e \). By Lemma 65, \( ab \in Q \). Since \( Q \) is primary, \( a \in Q \) or \( b \in \sqrt{Q} \). If \( a \in Q \), then \( a/s \in Q^e \) by Lemma 64. Assume that \( b \in \sqrt{Q} \). Then \( b/t \in (\sqrt{Q})^e \) by Lemma 64. Now by Lemma 66 we have \( (\sqrt{Q})^e = \sqrt{Q^e} \). Hence, \( b/t \in \sqrt{Q^e} \). We have proven that \( Q^e \) is primary; hence, the extension map is well-defined.

Next, we prove that the contraction map is well-defined. Let \( Q' \) be a primary ideal of \( S^{-1}R \). We need to prove that \( (Q')^c \) is primary and that \( (Q')^c \cap S = \emptyset \). To see that \( (Q')^c \) is primary, assume that \( a, b \in R \) are such that \( ab \in (Q')^c \). Then \( f(ab) = f(a)f(b) \in Q' \). Since \( Q' \) is primary we have \( f(a) \in Q' \) or \( f(b) \in \sqrt{Q} \), i.e., \( a \in (Q')^c \) or \( b \in (\sqrt{Q})^c = \sqrt{(Q')^c} \). It follows that \( (Q')^c \) is primary. Assume that \( (Q')^c \cap S \neq \emptyset \); we will obtain a contradiction. Since \( (Q')^c \cap S \neq \emptyset \), we have \( ((Q')^c)^e = S^{-1}R \) by Lemma 66. Also, by Lemma 63, \( ((Q')^c)^e = Q' \). Hence, \( Q' = S^{-1}R \). This is a contradiction because \( Q' \) is prime, and hence proper. We have proven that the contraction map is well-defined.

To see that the two maps are inverses of each other we note that by Lemma 65 we have \( (Q^e)^c = Q \) if \( Q \) is primary ideal such that \( Q \cap S = \emptyset \), and by Lemma 63, \( ((Q')^c)^e = Q' \) if \( Q' \) is a primary ideal of \( S^{-1}R \).

Finally, assume that \( Q \) is a primary ideal of \( R \) such that \( Q \cap S = \emptyset \), and let \( P = \sqrt{Q} \). Then \( \sqrt{Q^e} = (\sqrt{Q})^e = P^e \) by Lemma 66.

**Theorem 69.** Let \( R \) be a commutative ring, and let \( S \) be a multiplicatively closed subset of \( R \). Let \( I \) be a decomposable ideal of \( R \). Let

\[ I = Q_1 \cap \cdots \cap Q_n \]

be a primary decomposition of \( I \), and let \( P_i = \sqrt{Q_i} \), for \( i = 1, \ldots, n \). Assume that \( m \in \mathbb{N}_0 \) is such that

\[ P_i \cap S = \emptyset \quad \text{for } 1 \leq i \leq m \]

and

\[ P_j \cap S \neq \emptyset \quad \text{for } m < j \leq n. \]

(i) If \( m = 0 \), then \( I^e = S^{-1}R \) and \( (I^e)^c = R \).

(ii) Assume that \( 1 \leq m \leq n \). Then \( I^e \) and \( (I^e)^c \) are decomposable, and

\[ I^e = Q_1^c \cap \cdots \cap Q_m^c \quad \text{and} \quad \sqrt{Q_i^e} = P_i^e \quad \text{for } 1 \leq i \leq m \]
and
\[(I^e)^c = Q_1 \cap \cdots \cap Q_m \quad \text{and} \quad \sqrt{Q_i} = P_i \quad \text{for} \ 1 \leq i \leq m.\]

**Proof.** (i) Assume that \(m = 0\). Let \(1 \leq j \leq n\). We first claim that \(Q_j \cap S \neq \emptyset\). Since \(m = 0\) we have \(P_j \cap S \neq \emptyset\). Let \(x \in P_j \cap S\). Then since \(P_j = \sqrt{Q_j}\), there exists \(t \in \mathbb{N}\) such that \(x^t \in Q_j\). Now \(x^t \in Q_j \cap S\), proving our claim that \(Q_j \cap S \neq \emptyset\). By Lemma 66 we have \(Q_j^e = S^{-1}R\). Since this holds for all \(1 \leq j \leq n\), we obtain by Lemma 66
\[
I^e = (Q_1 \cap \cdots \cap Q_n)^e = Q_1^e \cap \cdots \cap Q_n^e
= S^{-1}R \cap \cdots \cap S^{-1}R
= S^{-1}R.
\]

Finally, since \(I^e = S^{-1}R\) we also have \((I^e)^c = R\).

(ii) Assume that \(1 \leq m \leq n\). Arguing as in (i) we have \(Q_i^e = S^{-1}R\) for \(m < i \leq n\). Hence, by Lemma 66,
\[
I^e = (Q_1 \cap \cdots \cap Q_n)^e = Q_1^e \cap \cdots \cap Q_n^e
= Q_1^e \cap \cdots \cap Q_m^e \cap Q_{m+1}^e \cap \cdots \cap Q_n^e
= Q_1^e \cap \cdots \cap Q_m^e \cap S^{-1}R \cap \cdots \cap S^{-1}R
= Q_1^e \cap \cdots \cap Q_m^e.
\]

By Theorem 68 for \(1 \leq i \leq m\) the ideals \(Q_i^e\) are primary and \(\sqrt{Q_i^e} = P_i^e\). Hence, \(I^e = Q_1^e \cap \cdots \cap Q_m^e\) is a primary decomposition of \(I^e\). Next, applying contraction, we obtain:
\[
(I^e)^c = (Q_1^e \cap \cdots \cap Q_m^e)^c = (Q_1^e)^c \cap \cdots \cap (Q_m^e)^c
= Q_1 \cap \cdots \cap Q_m.
\]

This is a primary decomposition of \((I^e)^c\). Finally, assume that the primary decomposition of \(I\) is minimal. By Theorem 68 the \(P_i^e\) for \(1 \leq i \leq m\) are pairwise distinct. Assume that \(1 \leq j \leq m\) is such that
\[
\bigcap_{\substack{i=1 \atop i \neq j}}^m Q_i^e \subseteq Q_j^e;
\]
we will obtain a contradiction. Applying contraction, we have
\[
\left(\bigcap_{\substack{i=1 \atop i \neq j}}^m Q_i^e\right)^c \subseteq (Q_j^e)^c
\]
The last inclusion implies that
\[ \bigcap_{i=1}^{m} (Q_i^c)^c \subseteq (Q_j^c)^c \]
and
\[ \bigcap_{i=1}^{m} Q_i \subseteq Q_j. \]

This contradicts the minimality of the primary decomposition for \( I \). It follows that the primary decomposition for \( I^e \) is minimal. The primary decomposition for \((I^e)^c\) is similarly proven to be minimal.

We can use these results to prove give another proof of the Second Uniqueness Theorem for Primary Decomposition.

**Theorem 70** (Second Uniqueness Theorem for Primary Decomposition). Let \( R \) be a commutative ring, and let \( I \) be a decomposable ideal of \( R \). Let \( \text{ass}_R(I) = \{P_1, \ldots, P_n\} \). Let

\[ I = Q_1 \cap \cdots \cap Q_n \quad \text{with} \quad \sqrt{Q_i} = P_i, \quad i \in \{1, \ldots, n\} \]

and

\[ I = Q'_1 \cap \cdots \cap Q'_n \quad \text{with} \quad \sqrt{Q'_i} = P_i, \quad i \in \{1, \ldots, n\} \]

be minimal primary decompositions of \( I \). If \( i \in \{1, \ldots, n\} \) and \( P_i \) is a minimal prime ideal of \( I \), then

\[ Q_i = Q'_i. \]

**Proof.** Let \( i \in \{1, \ldots, n\} \) and assume that \( P_i \) is a minimal prime ideal of \( I \). Let \( S = R - P_i \). Then \( S \) is a multiplicatively closed subset of \( R \). Let \( j \in \{1, \ldots, n\} \) with \( j \neq i \); we claim that \( P_j \cap S \neq \emptyset \). Assume that \( P_j \cap S = \emptyset \); we will obtain a contradiction. Since \( P_j \cap S = \emptyset \), we have \( P_j \subseteq P_i \). Since \( P_i \) is a minimal prime ideal of \( R \) we must have \( P_j = P_i \). This contradicts the assumption that the above are minimal primary decompositions of \( I \). We have proven that \( P_j \cap S \neq \emptyset \). Applying now Theorem 69 we have

\[ Q_i = (I^e)^c = Q'_i. \]

This is the desired result.

**Proposition 71.** Let \( R \) be a commutative ring, and let \( P \) be a prime ideal of \( R \). Let \( S = R - P \), and let \( f : R \to S^{-1}R = R_P \) be the natural map. If \( n \in \mathbb{N} \), then \((P^n)^e)^c\) is a primary ideal such that

\[ \sqrt{((P^n)^e)^c} = P. \]
Proof. By Proposition 61, \( R_P \) is a quasi-local ring with maximal ideal \( P^e \). By Lemma 66 we have

\[
(P^n)^e = (P^e)^n.
\]

Since

\[
\sqrt{(P^n)^e} = \sqrt{(P^e)^n} = P^e
\]

and \( P^e \) is maximal, \((P^n)^e\) is a primary ideal of \( R_P \). Since the contraction of any primary ideal is easily seen to be a primary ideal, the ideal \(((P^n)^e)^c\) is a primary ideal of \( R \). Now

\[
\sqrt{((P^n)^e)^c} = \sqrt{(P^n)^e}^c \quad \text{ (see Exercise 2.43)}
\]

\[
= (P^e)^c
\]

\[
= P. \quad \text{ (Theorem 67)}
\]

This completes the proof. \( \square \)

Let the notation be as in Proposition 71. We then refer to \(((P^n)^e)^c\) as the \( n \)-th **symbolic power** of \( P \) and write

\[
P^{(n)} = ((P^n)^e)^c.
\]

It is known that \( P^{(n)} = P^n \) if and only if \( P^n \) is primary. Previously, we say that there exist prime ideals \( P \) such that \( P^n \) is not primary. Thus, in general the \( n \)-th symbolic power of \( P \) is different from \( P^n \).

End of lecture, Wednesday, October 19.