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

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 $b \neq 0$, then there exist $q, r \in R$ such that

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

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

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

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

Proof. We need to prove that (R, ∂) 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

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

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

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

Hence,

$$\begin{aligned} ab^{-1} &= (m + g) + i(n + h) \\ ab^{-1} &= (m + in) + (g + ih) \\ a &= (m + ih)b + (g + ih)b \\ a &= qb + r, \end{aligned}$$

where

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

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

$$\begin{aligned} \partial(r) &= |r|^2 \\ &= |g + ih|^2|b|^2 \\ &= (g^2 + h^2)\partial(b) \\ &\leq (1/4 + 1/4)\partial(b) \\ &< \partial(b). \end{aligned}$$

This completes the proof. □

Let (R, ∂) 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

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

But we also have

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

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

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

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

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

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 ∂ is Euclidean. These values are $D = -1, -2, -3, -7, -11$ and $D = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73$.

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

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

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

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

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

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

$$r = p_1 \cdots p_s.$$

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

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

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

We will often abbreviate "unique factorization domain" as "UFD".

We will prove the following theorem later on.

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

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

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

By repeated use of this theorem, if R is a UFD, then so is $R[X_1, \ldots, X_n]$.
One way to prove Theorem 2 is as follows. Let K be field of fractions of R. We know that $K[X]$ is a Euclidean domain. By Theorem 1 we have that $K[X]$ is a UFD. We now use this to prove that $R[X]$ is a UFD; this uses the Gauss Lemma.
We note that if R is a UFD, then it can happen that $R[[X]]$ is *not* a UFD.
It is fairly common that the existence condition (i) for a UFD holds for a ring R. For example, if R is a Noetherian domain, then (i) holds. The uniqueness condition (ii) is the key point. If R is the ring of integers in an algebraic number field, then (i) does hold, but (ii) usually does not. Let $R = \mathbb{Z}[\omega]$ as above. If $D < 0$, then it is known that R is a UFD for exactly $D = 1, 2-, -3, -7, -11, -19, -43, -67, -163$. If $D > 0$, then it is still an open problem to determine when R is a UFD. It is conjectured that there are infinitely many $D > 0$ such that R is a UFD, but this is not known. Historically, the problem that not all rings are UFDs led to the introduction of the concept of "ideal numbers" or what are nowadays called ideals.

2 Ideals

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

(i) $I \neq \emptyset$.

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

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

Assume that I is an ideal of R. Then I is an additive subgroup of R. To see this it suffices to prove that if $a, b \in I$, then $a - b \in I$. Let $a, b \in I$. Then $-b = (-1)b \in I$ by (iii); we now have $a - b \in I$ by (ii). Besides being an additive subgroup of R, the set I also the property that $ra \in I$ for $r \in R$ and $a \in A$.

Example. Let R be a commutative ring. Then 0 and R are ideals of R.

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

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

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

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

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 $(n) = \mathbb{Z}n = n\mathbb{Z}$. This is the set of all the integers divisible by n.

Let R be an integral domain. We say that R is a ***principal ideal domain*** if every ideal of R is principal. We will abbreviate "principal ideal domain" to "PID".

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

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

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

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

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

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

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

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

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

$$I = \bigcap_{\lambda \in \Lambda} I_\lambda$$

is an ideal of R. The ideal I is called the **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. □

Example. If $m, n \in \mathbb{Z} - 0$, then

$$(m) \cap (n) = \mathbb{Z}m \cap \mathbb{Z}n = (\operatorname{lcm}(m, n)) = \mathbb{Z} \operatorname{lcm}(m, n) = \operatorname{lcm}(m, n)\, \mathbb{Z}.$$

To define more ways of creating ideals we first need some notation. Let R be a commutative ring. Let $A, B, A_1, \ldots, A_n$ be non-empty subsets of R. We define

$$A_1 + \cdots + A_n = \{a_1 + \cdots + a_n : a_1 \in A_1, \ldots, a_n \in A_n\}.$$

We also define

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

More generally, we define

$$A_1 \cdots A_n = \text{the set of all finite sums of elements of the form } a_1 \cdots a_n,\ a_1 \in A_1,\ \ldots,\ a_n \in A_n.$$

We also define

$$A^n = A \cdots A.$$

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

Proof. This is a straightforward verification. □

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. □

Example. Let R be a commutative ring and let $h_1, \ldots, h_t \in R$. Then

$$(h_1, \ldots, h_t) = (h_1) + \cdots + (h_t).$$

Example. If $m, n \in \mathbb{Z} - 0$, then

$$(m) + (n) = \mathbb{Z}m + \mathbb{Z}n = \mathbb{Z} = \mathbb{Z}\gcd(m, n) = (\gcd(m, n)).$$

Finally, we can form products of ideals.

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

Proof. This is again a straightforward verification. □

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

$$IJ \subseteq I \cap J,$$
$$(IJ)K = I(JK),$$
$$IJ = JI,$$
$$RI = I,$$

$$0I = 0,$$
$$I(J + K) = IJ + IK.$$

Example. If $a, b \in R$, then $(a)(b) = (ab)$.
Example. It can happen that $IJ \subsetneqq I \cap J$. For example, take $R = \mathbb{Z}$, $I = (2)$, $J = (4)$. Then $IJ = (8)$, but $(2) \cap (4) = (\mathrm{lcm}(2, 4)) = (4)$. 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

$$\mathrm{Ann}(J) = (0 : J).$$

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

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

$$R/I = \{a + I : a \in R\}.$$

Here,

$$a + I = \{a + c : c \in I\}.$$

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

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

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

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

for $a, b \in R$.

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

$1 + R$.

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

$$a_1 + I = a_2 + I, \qquad b_1 + I = b_2 + I.$$

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

$$\begin{aligned} a_2 b_2 + I &= (a_1 + c)(b_1 + d) + I \\ &= a_1 b_1 + \underbrace{a_1 d + c b_1 + cd}_{\in I} + I \\ &= a_1 b_1 + I. \end{aligned}$$

Here we have used $a_1 d + c b_1 + cd \in I$ 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

$$p : R \longrightarrow R/I$$

by

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

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

$$\begin{aligned} p(r + s) &= r + s + I \\ &= (r + I) + (s + I) \\ &= p(r) + p(s). \end{aligned}$$

And

$$\begin{aligned} p(r)p(s) &= (r+I)(s+I) \\ &= rs+I \\ &= p(rs). \end{aligned}$$

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*

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

defined by

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

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 $s \in \operatorname{im}(f)$. 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. □

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*

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

defined by

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

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

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

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

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

$$x \in x + I = r + I \subseteq r + J_2 = J_2.$$

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

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

$$\begin{aligned}
(\bar{1}) &= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\},\\
(\bar{2}) &= \{\bar{0}, \bar{2}, \bar{4}\},\\
(\bar{3}) &= \{\bar{0}, \bar{3}\},\\
(\bar{6}) &= \{\bar{0}\}.
\end{aligned}$$

We can try to generalize the situation of the previous theorem. Suppose that R and S are commutative rings, and $f : R \to S$ is a ring homomorphism. How can we relate the ideals of R and S via

f? Assume first that J is an ideal of S. We can then consider

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

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

$$f(ra) = f(r)f(a) \in J$$

because $f(a) \in J$ and J is an ideal. It follows that $ra \in f^{-1}(J)$, completing the proof that $f^{-1}(J)$ is an ideal of R. The ideal $f^{-1}(J)$ of R is called the ***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) $I \subseteq I^{ec}$.
(ii) $J^{ce} \subseteq J$.
(iii) $I^e = I^{ece}$.
(iv) $J^{cec} = J^c$.

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

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

(Note that since $f(f^{-1}(J)) \subset J$ and J is an ideal, we have $(f(f^{-1}(J))) \subset J$).
(iii). By (i), $I \subseteq I^{ec}$. This implies that $I^e \subseteq I^{ece}$. By (ii) we have $I^{ece} \subseteq I^e$. It follows that $I^e = I^{ece}$. eq (iv). By (ii), $J^{ce} \subset J$; hence, $J^{cec} \subseteq J^c$. By (i) we have $J^c \subseteq J^{cec}$. We now have $J^{cec} = J^c$. □

As a corollary of this lemma we see that there is bijection

$$C_R = \{\text{all contractions of ideals of } S\} \longleftrightarrow E_S = \{\text{all extensions of ideals of } R\}$$

defined by

$$I \mapsto I^e, \qquad \text{for } I \in C_R,$$
$$J^c \hookleftarrow J, \qquad \text{for } J \in E_S.$$

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

$$\{\text{ideals } J \text{ of } R \text{ such that } M \subseteq J \subseteq R\} \longleftrightarrow \{\text{ideals of } R/M\}.$$

Therefore,

$$\begin{aligned} M \text{ is a maximal ideal} &\iff \text{the first set has two elements} \\ &\iff \text{the second set has two elements} \\ &\iff R/M \text{ is a field (by Lemma 13).} \end{aligned}$$

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

$$\begin{aligned} M \text{ is a maximal ideal of } \mathbb{Z} &\iff \mathbb{Z}/M = \mathbb{Z}/m\mathbb{Z} \text{ is a field} \qquad \text{(Lemma 13)} \\ &\iff m \text{ is a prime} \qquad \text{(elementary number theory).} \end{aligned}$$

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 $(p) \subsetneqq R$. 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 $i = 1, \ldots, n$

$$\begin{aligned} X_i + M &= a_i + M \\ \bar{X}_i &= \bar{a}_i. \end{aligned}$$

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

$$\begin{aligned} \bar{g} &= \sum_{(i_1,\ldots,i_n)\in\Lambda} \bar{c}_{i_1,\ldots,i_n} \bar{X}_1^{i_1} \cdots \bar{X}_n^{i_n} \\ &= \sum_{(i_1,\ldots,i_n)\in\Lambda} \bar{c}_{i_1,\ldots,i_n} \bar{a}_1^{i_1} \cdots \bar{a}_n^{i_n} \\ &= \overline{g(a_1, \ldots, a_n)} \end{aligned}$$

$$= t(g(a_1, \ldots, a_n)).$$

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

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

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

Proof. Using Lemma 13 we have:

$$\begin{aligned} M \text{ maximal ideal of } R &\iff R/M \text{ is as field} \qquad \text{(Lemma 13)} \\ &\iff (R/I)/(M/I) \cong R/M \text{ is a field} \\ &\iff M/I \text{ is a maximal ideal of } R/I \qquad \text{(Lemma 13).} \end{aligned}$$

This completes the proof. □

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

(i) $\leq$ is ***reflexive***: if $x \in X$, then $x \leq x$.
(ii) $\leq$ is ***antisymmetric***: if $x, y \in X$ and $x \leq y$ and $y \leq x$, then $x = y$.
(iii) $\leq$ is ***transitive***: if $x, y, z \in X$ and $x \leq y$ and $y \leq z$, then $x \leq z$.

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

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

Proof. This is equivalent to the axiom of choice of set theory. □

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

Proof. Let X be the set of all proper ideals J of R such that $I \subseteq J \subsetneqq R$. The set X contains I and is thus non-empty. We will use the partial order $\subseteq$ on X. Let Y be a totally ordered subset

of X. Let B be the union of all the elements of Y. We claim that $B \in X$. Since every element of Y contains I, the set B certainly contains I and is thus non-empty. Let $b_1, b_2 \in B$. There exist $J_1, J_2 \in Y$ such that $b_1 \in J_1$ and $b_2 \in J_2$. Since Y is totally ordered we have $J_1 \subseteq J_2$ or $J_2 \subseteq J_1$. Assume that $J_1 \subseteq J_2$. Then $b_1, b_2 \in J_2$, and hence $b_1 + b_2 \in J_2 \subseteq B$ since J_2 is an ideal. Similarly, if $J_2 \subset J_1$, 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 $I \subset B$, $B \in X$. 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. □

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 $\bar{a}\bar{b} = (a + P)(b + P) = P$. 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. □

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:

$$\begin{aligned} P \text{ is a prime ideal of } R &\iff R/P \text{ is an integral domain} \qquad \text{(Lemma 18)} \\ &\iff (R/I)/(P/I) \cong R/P \text{ is an integral domain} \\ &\iff P/I \text{ is a prime ideal of } R/I. \end{aligned}$$

This completes the proof. □

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

Proof. We have

$$\begin{aligned} M \text{ is a maximal ideal of } R &\implies R/M \text{ is a field} \\ &\implies R/M \text{ is an integral domain} \end{aligned}$$

$$\implies M \text{ is a prime ideal.}$$

This completes the proof. □

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

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

(i) If p is prime, then p is irreducible.

(ii) p is prime if and only if (p) is a prime ideal.

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

$$pc = a \implies abc = a \implies bc = 1.$$

Here, the last step follows because R is an integral domain. It follows that b is a unit. Similarly, if $p \mid b$, then a is a unit. It follows that p is irreducible.
(ii). Assume that p is prime. Let $a, b \in R$ be such that $ab \in (p)$. Then $p \mid ab$. Since p is prime we have $p \mid a$ or $p \mid b$, i.e., $a \in (p)$ or $b \in (b)$. Assume that (p) is prime. Let $a, b \in R$ and assume that $p \mid ab$. Then $ab \in (p)$. Since (p) is prime we have $a \in (p)$ or $b \in (p)$. This means that $p \mid a$ or $p \mid b$. □

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

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

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

(iii) p is a prime element of R.

(iv) p is an irreducible element of R.

Proof. (i) $\implies$ (ii). This follows from Lemma 20.
(ii) $\implies$ (iii). This follows from Lemma 21.
(iii) $\implies$ (iv). This follows from Lemma 21.
(iv) $\implies$ (i). Assume that p is an irreducible element of R. Assume that I is an ideal of R such that $(p) \subseteq I \subseteq R$. Since R is a PID, there exists $a \in R$ such that $I = (a)$. Now $(p) \subseteq (a)$; hence, there exists $b \in R$ such that $p = ab$. Since p is irreducible either a is a unit or b is a unit. If a is a unit, then $(a) = R$; if b is a unit, then $(a) = (p)$. It follows that R is maximal. □

Let R be a commutative ring. We will write

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

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

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

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

From the lemmas, we see that:

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

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

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

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

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

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

$$R/(X_1, \ldots, X_k) = K[X_1, \ldots, X_n]/(X_1, \ldots, X_k) \cong K[X_{k+1}, \ldots, X_n].$$

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

It turns out that all these examples of R, (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 be a non-empty set X of ideals of R which does not have a maximal element. Let $I_1 \in X$. Since I_1 is not maximal, there exists an ideal $I_2 \in X$ such that $I_1 \subsetneqq I_2$. Similarly, there exists $I_3 \in X$ such that $I_2 \subsetneqq I_3$. Continuing, we obtain a chain of ideals

$$I_1 \subsetneqq I_2 \subsetneqq I_3 \subsetneqq \cdots .$$

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

$$(x_1) \subsetneqq (x_1, x_2) \subsetneqq (x_1, x_2, x_3) \subsetneqq \cdots .$$

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 $I = \cup_{i=1}^{\infty} I_i$. 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_i}; 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 $I_m \subset I$ 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 $(a) \subset (b)$. Since $r^{-1}a = b$, we also have $(b) \subset (a)$. 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

$$(b) \subsetneqq (c) \subsetneqq R, \qquad (b) \subsetneqq (d) \subsetneqq R.$$

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 $P \subsetneqq R$ we have $1 \neq P$ so that $1 \in S$. Let $s_1, s_2 \in S$. Then $s_1 s_2 \in S$ because otherwise $s_1 s_2 \in P$ which implies $s_1 \in P$ or $s_2 \in P$, a contradiction. □

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

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

Order Ψ be inclusion. Then Ψ has a maximal element P, and P is a prime ideal.

Proof. We will use Zorn's Lemma applied to Ψ. The set Ψ is non-empty because $I \in \Psi$. Let Y be a totally ordered subset of Ψ; we must show that Y has an upper bound in Ψ. 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 Ψ. Thus B is an upper bound for Y in Ψ. By Zorn's Lemma, Ψ 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

$$I \subseteq P \subsetneqq P + (a).$$

By the maximality of P in Ψ 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. □

Proposition 27. *Let R be a commutative ring and let I be an ideal of R. let*

$$\mathrm{Var}(I) = \{P :\in \mathrm{Spec}(R) : I \subseteq P\} \qquad \textit{(the } \textbf{variety} \textit{ of } I\textit{)}.$$

Then

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

Proof. Let $a \in \sqrt{I}$. There exists $n \in \mathbb{N}$ such that $a^n \in I$. Let $P \in \mathrm{Var}(I)$. Since $I \subseteq P$, we have $a^n \in P$. Since a is prime, $a \in P$. It follows that $\sqrt{I} \subseteq \bigcap_{P \in \mathrm{Var}(I)} P$. Conversely, let $a \in \bigcap_{P \in \mathrm{Var}(I)} P$. Assume that $a \notin \sqrt{I}$; we will obtain a contradiction. Let $S = \{a^n : n \in \mathbb{N}_0\}$. Since $a \notin \sqrt{I}$ we have

$S \cap I = \emptyset$. By Theorem 26, there exists a prime ideal Q such that $I \subset Q$ and $Q \cap S = \emptyset$. We have $Q \in \mathrm{Var}(I)$. By assumption, $a \in \bigcap_{P \in \mathrm{Var}(I)} P$; hence, $a \in Q$. This contradicts $Q \cap S = \emptyset$. □

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

Corollary 28. *Let R be a commutative ring. We have*

$$\sqrt{0} = \bigcap_{P \in \mathrm{Spec}(R)} P.$$

Proof. This follows immediately from Proposition 27. □

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., $I \subsetneqq R$. Then $\mathrm{Var}(I)$ contains a minimal element with respect to inclusion, i.e., there exists $P \in \mathrm{Var}(I)$ such that if $P' \in \mathrm{Var}(I)$ 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 $\mathrm{Var}(I)$ is non-empty (because any maximal ideal is a prime ideal by Lemma 20). We define a partial order $\leq$ on $\mathrm{Var}(I)$ by $P_1 \leq P_2$ if and only if $P_2 \subseteq P_1$. Let Y be a totally ordered subset of $\mathrm{Var}(I)$. Let Q be the intersection of all the elements of Y. We claim that $Q \in \mathrm{Var}(I)$. 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 $Q \in \mathrm{Var}(I)$ 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, $Q \in \mathrm{Var}(I)$. Clearly, Q is an upper bound for Y. We may now apply Zorn's Lemma to conclude that $\mathrm{Var}(I)$ has a maximal element P. By the maximality of P, if $P' \in \mathrm{Var}(I)$ is such that $I \subseteq P' \subseteq P$, then $P = P'$. This completes the proof. □

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

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

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

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

Proof. By Proposition 27 we have

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

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

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

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

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

This completes the proof. □

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

(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) $\Longrightarrow$ (ii) This follows from $\bigcap_{i=1}^n I_i \subseteq I_j$ for $j \in \{1, \ldots, n\}$.
(ii) $\Longrightarrow$ (iii) This follows from $\prod_{i=1}^n I_i \subseteq \bigcap_{i=1}^n I_i$.
(iii) $\Longrightarrow$ (i) Assume that $\prod_{i=1}^n I_i \subseteq P$. Suppose that $I_j \nsubseteq P$ for all $j \in \{1, \ldots, n\}$; we will obtain a contradiction. For each $j \in \{1, \ldots, n\}$ there exists $a_j \in I_j$ such that $a_j \notin P$. Now

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

Since P is prime we have a_j for some $j \in \{1, \ldots, n\}$. This is a contradiction.
To prove the final statement, assume that $P = \bigcap_{i=1}^n I_i$. Since (ii) $\Longrightarrow$ (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 $P \subset I_j$. Hence, $P = I_j$. □

Let R be a commutative ring, and let I and J be ideals of R. We say that I and J are ***comaximal*** if $I + J = R$.

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

Proof. Since $IJ \subset I$ and $IJ \subset J$ we have $IJ \subset I \cap J$. Next, let $\in I \cap J$. Since $I + J = R$, there exist $a \in I$ and $b \in J$ such that $a + b = 1$. Hence, $x = xa + xb = ax + xb$. Now $a \in I$, and $x \in I \cap J \subseteq J$ so that $ax \in IJ$.; similarly, $x \in I \cap J \subseteq I$ and $b \in J$, so that $xb \in IJ$. Therefore, $x = xa + xb \in IJ$. It follows that $I \cap J \subseteq IJ$. □

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 $J + I_n \subsetneqq R$. By Proposition 17 there exists a maximal ideal M such that $J + I_n \subseteq M \subsetneqq R$. 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 $J \cap I_n = JI_n$ by Lemma 32. Hence,

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

This completes the proof. □

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

$$x \equiv y \pmod{I}$$

to mean that

$$x + I = y + I$$

or equivalently, $x - y \in I$.

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

$$x \equiv x_i \pmod{I_i}$$

for $i \in \{1, \ldots, n\}$.

Proof. We first prove this when $n = 2$. Since I_1 and I_2 are comaximal we have $I_1 + I_2 = R$. Hence, there exist $a_1 \in I_1$ and $a_2 \in I_2$ such that $a_1 + a_2 = 1$. Set $x = x_2 a_1 + x_1 a_2$. Then

$$\begin{aligned} x &\equiv x_2 a_1 + x_1 a_2 \pmod{I_1} \\ &\equiv x_1 a_2 \pmod{I_1} \qquad (\text{because } x_2 a_1 \in I_1) \\ &\equiv x_1(1 - a_1) \pmod{I_1} \qquad (\text{recall that } a_1 + a_2 = 1) \\ &\equiv x_1 - x_1 a_1 \pmod{I_1} \\ &\equiv x_1 \pmod{I_1} \qquad (\text{because } x_1 a_1 \in I_1). \end{aligned}$$

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

$$x = x_1 y_1 + \cdots + x_n y_n.$$

Let $i \in \{1, \ldots, n\}$. Then

$$\begin{aligned} x &\equiv x_1 y_1 + \cdots + x_n y_n \pmod{I_i} \\ &\equiv x_i y_i \pmod{I_i} \qquad (\text{because } y_j \equiv 0 \pmod{I_i} \text{ for } j \neq i) \\ &\equiv x_i \pmod{I_i} \qquad (\text{because } y_i \equiv 1 \pmod{I_i}). \end{aligned}$$

This completes the proof. □

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

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

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

$$\begin{aligned} f(r) = 0 &\iff r + I_i = I_i \quad \text{for} \quad i \in \{1, \ldots, n\} \\ &\iff r \in I_i \quad \text{for} \quad i \in \{1, \ldots, n\} \\ &\iff r \in \bigcap_{i=1}^{n} I_i. \end{aligned}$$

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

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

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*

$$R/(I_1 \cdots I_n) = R/(I_1 \cap \cdots \cap I_n) \xrightarrow{\sim} R/I_1 \times \cdots \times R/I_n$$

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

$$(n) = (p_1^{e_1}) \cdots (p^{e_t}).$$

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

$$(n) = (p_1^{e_1}) \cap \cdots \cap (p^{e_t}).$$

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., $Q \subsetneqq R$.

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

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

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

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

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

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

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 I 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 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 $Q \subseteq \sqrt{Q} = M \subsetneq R$. 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:

$$\begin{array}{ccc} \text{all ideals} & \xrightarrow{\text{Rad}} & \text{all ideals} \\ \cup & & \cup \\ \text{primary ideals} & \twoheadrightarrow & \text{prime ideals} \\ \cup & & \cup \\ \text{Rad}^{-1}(\text{maximal ideals}) & \twoheadrightarrow & \text{maximal ideals.} \end{array}$$

Example. Let R be a PID. Then the primary ideals of R are

$$0, \qquad (p^n) = (p)^n,\ n \in \mathbb{N},\ p \text{ an irreducible element.}$$

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

$$Q = (p_1)^n = (p_1^n).$$

This completes the proof. □

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

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

□

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

$$X = g_n X^n + g_{n-1} X^{n-1} Y + \cdots g_1 X Y^{n-1} + g_0 Y^n.$$

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. □

Example. Let K be a field and let X, Y, Z be indeterminates. Let

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

Also, let

$$x = X + I, \qquad y = Y + I, \qquad z = Z + I.$$

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 $Q' = \cap_{i=1}^n Q_i$. We need to prove that Q' is P-primary. First of all, we have $Q' \subset Q_1 \subsetneq R$; 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

$$\sqrt{Q_1} = P_1, \cdots, \sqrt{Q_n} = P_n$$

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 $j = 1, \ldots, n$,

$$\bigcap_{\substack{i=1 \\ i \neq j}}^{n} Q_i \not\subseteq Q_j.$$

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 satifies (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*

$$I = Q_1 \cap \cdots \cap Q_n \text{ with } \sqrt{Q_i} = P_i \text{ for } i = 1, \ldots, n$$

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

$$\bigcap_{\substack{j=1 \\ j \neq i}}^{n} Q_j \not\subseteq Q_i.$$

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

$$\begin{aligned}
(I : a) &= \left(\bigcap_{j=1}^{n} Q_j : a \right) \\
&= \bigcap_{j=1}^{n} (Q_j : a) \qquad \text{(Exercise 2.33)} \\
&= (Q_i : a) \cap \bigcap_{\substack{j=1 \\ j \neq i}}^{n} (Q_j : a) \\
&= (Q_i : a) \cap \bigcap_{\substack{j=1 \\ j \neq i}}^{n} R \qquad \text{(Lemma 44)} \\
(I : a) &= (Q_i : a).
\end{aligned}$$

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 $P \subsetneqq R$). Since $a \notin I$, there exists at least one $i \in \{1, \ldots, n\}$ such that $a \notin Q_i$. Now

$$\begin{aligned}
(I : a) &= \left(\bigcap_{i=1}^{n} Q_i : a \right) \\
&= \bigcap_{i=1}^{n} (Q_i : a) \\
&= \left(\bigcap_{\substack{i=1 \\ a \in Q_i}}^{n} (Q_i : a) \right) \cap \left(\bigcap_{\substack{i=1 \\ a \notin Q_i}}^{n} (Q_i : a) \right) \\
&= \left(\bigcap_{\substack{i=1 \\ a \in Q_i}}^{n} R \right) \cap \left(\bigcap_{\substack{i=1 \\ a \notin Q_i}}^{n} (Q_i : a) \right) \\
&= \bigcap_{\substack{i=1 \\ a \notin Q_i}}^{n} (Q_i : a).
\end{aligned}$$

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

$$\sqrt{(I : a)} = \sqrt{\bigcap_{\substack{i=1 \\ a \notin Q_i}}^{n} (Q_i : a)}$$

$$P = \bigcap_{\substack{i=1 \\ a \notin Q_i}}^{n} \sqrt{(Q_i : a)}$$

$$P = \bigcap_{\substack{i=1 \\ a \notin Q_i}}^{n} P_i \qquad \text{(by Lemma 44).}$$

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

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

and

$$\{P_1', \ldots, P_{n'}'\} = \{P \in \operatorname{Spec}(R) : \text{there exists } a \in R \text{ such that } \sqrt{(I : a)} = P\}.$$

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

$$\operatorname{ass}_R(I) = \{P_1, \ldots, P_n\}.$$

Proposition 47. *Let R be a commutative ring, and let I be a decomposable ideal of R. Let $P \in \operatorname{Spec}(R)$. Then P is a minimal prime ideal of I if and only if $P \in \operatorname{ass}_R(I)$ and P is minimal as a member of $\operatorname{ass}_R(I)$.*

Proof. We begin with some notation. Let

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

be a minimal primary decomposition of I. Let

$$P_1 = \sqrt{Q_1}, \quad \ldots, \quad P_n = \sqrt{Q_n}$$

so that

$$\mathrm{ass}_R(I) = \{P_1, \ldots, P_n\}.$$

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:

$$\sqrt{Q_j} \subseteq \sqrt{P}$$
$$P_j \subseteq P.$$

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, $P \in \mathrm{ass}_R(I)$. We still need to prove that P is minimal as a member of $\mathrm{ass}_R(I)$. Suppose that $P_i \in \mathrm{ass}_R(I)$ 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 $\mathrm{ass}_R(I)$.
($\impliedby$) Assume that $P \in \mathrm{ass}_R(I)$ and that P is minimal as a member of $\mathrm{ass}_R(I)$. 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 $P_j, P \in \mathrm{ass}_R(I)$ and P is minimal as a member of $\mathrm{ass}_R(I)$, 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 $\mathrm{ass}_R(I)$ 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 $\mathrm{ass}_R(I)$ that are minimal as members of $\mathrm{ass}_R(I)$ as the ***minimal primes*** or ***isolated primes*** of I. The elements of $\mathrm{ass}_R(I)$ 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

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

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 $\mathrm{ass}_R(I) = \{P, M\}$.

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

$$\begin{aligned} &I = (XY, Y^2) \subseteq P = (Y), \\ &I = (XY, Y^2) \subseteq M^2 = (X^2, XY, Y^2) \subseteq Q = (X, Y^2). \end{aligned}$$

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

$$\begin{aligned} g_0 Y &= f - g_1 Y \\ Y &= g_0^{-1} f - g_0^{-1} g_1 Y \\ &\in (Q \cap P) + I \\ &\subseteq Q \cap P \\ &\subseteq Q. \end{aligned}$$

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 $f = g_1 Y \in I$. 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

$$M^2 \not\subseteq P, \qquad P \not\subseteq M^2, \qquad Q \not\subseteq P, \qquad P \not\subseteq Q.$$

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

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

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

and

$$I = Q_1' \cap \cdots \cap Q_n' \quad \textit{with} \quad \sqrt{Q_i'} = P_i, \quad i \in \{1, \ldots, n\}$$

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

$$\bigcap_{\substack{j=1 \\ j \neq i}} P_j \not\subseteq P_i.$$

(Otherwise $\bigcap_{\substack{j=1 \\ j \neq i}} P_j \subseteq P_i$ 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

$$a \in \bigcap_{\substack{j=1 \\ j \neq i}} P_j \quad \text{and} \quad a \notin P_i.$$

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

$$\begin{aligned}
(I : a^t) &= (\bigcap_{j=1}^{n} Q_j : a) \\
&= (Q_i : a^t) \cap \bigcap_{\substack{j=1 \\ j \neq i}} (Q_j : a^t) \\
&= Q_i \cap \bigcap_{\substack{j=1 \\ j \neq i}} R \qquad \text{(Lemma 44)} \\
&= Q_i.
\end{aligned}$$

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. □

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., $I \subsetneqq R$.

(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

$$I \subsetneqq I_1 \quad \text{and} \quad I \subsetneqq I_2.$$

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 $I \subsetneqq I_2$). Since $I \subsetneqq I_1$ and $I \subsetneqq I_2$ 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. □

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 $I \subsetneqq R$. 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 $(I : b^m) = (I : b^n)$ 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

$$r = x_1 + r_1 a = x_2 + r_2 b^n$$

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

$$r_2 b^n = x_1 + r_1 a - x_2.$$

Multiplying by b we obtain

$$r_2 b^{n+1} = x_1 b + r_1 ab - x_2 b.$$

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

$$r = x_2 + r_2 b^n \in I.$$

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 ***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.

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.

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). □

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.

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:

$$vs_3 ua_1 s_2 = vs_3 ua_2 s_1,$$
$$us_1 va_2 s_3 = us_1 va_3 s_2.$$

This implies that

$$vs_3ua_1s_2 = us_1va_3s_2,$$

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 $\frac{a}{s}$ 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*

$$+ : S^{-1}R \times S^{-1}R \to R, \qquad \cdot : S^{-1}R \times S^{-1}R \to R$$

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

$$(a_1t_1 + b_1s_1)/s_1t_1 = (a_2t_2 + b_2s_2)/s_2t_2$$

which is the desired result. We leave the remaining checks as an exercise. □

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. □

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*

$$f : R \longrightarrow S^{-1}R$$

by

$$f(r) = r/1, \qquad r \in R.$$

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 $f : R \to S^{-1}R$ 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 $f : R \to S^{-1}R$ 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 $at = bs$. 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 multiplicative subset of R, and let $f : R \to S^{-1}R$ be the natural homomorphism. Let R' be a commutative ring and let $g : R \to R'$ be a ring homomorphism such that $g(s)$ is a unit for $s \in S$. Then there exists a unique ring homomorphism $h : S^{-1}R \to R'$ such that*

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

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 $h : S^{-1}R \to R'$ 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

$$\begin{aligned} g(a_1)g(s_2) - g(a_2)g(s_1) &= 0 \\ g(a_1)g(s_2) &= g(a_2)g(s_1). \end{aligned}$$

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

$$g(a_1)g(s_1)^{-1} = g(a_2)g(s_2)^{-1}.$$

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

$$\begin{aligned} h(a_1/s_1 + a_2/s_2) &= h((a_1s_2 + a_2s_1)/s_1s_2) \\ &= g(a_1s_2 + a_2s_1)g(s_1s_2)^{-1} \\ &= g(a_1)g(s_2)g(s_1)^{-1}g(s_2)^{-1} + g(a_2)g(s_1)g(s_1)^{-1}g(s_2)^{-1} \\ &= g(a_1)g(s_1)^{-1} + g(a_2)g(s_2)^{-1} \\ &= h(a_1/s_1) + h(a_2/s_2). \end{aligned}$$

Also,

$$\begin{aligned} h(a_1/s_1 \cdot a_2/s_2) &= h(a_1a_2/s_1s_2) \\ &= g(a_1a_2)g(s_1s_2)^{-1} \\ &= g(a_1)g(a_2)g(s_1)^{-1}g(s_2)^{-1} \\ &= h(a_1/s_1)h(a_2/s_2). \end{aligned}$$

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

$$\begin{aligned} (h \circ f)(r) &= h(f(r)) \\ &= h(r/1) \\ &= g(r)g(1)^{-1} \\ &= g(r). \end{aligned}$$

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

$$\begin{aligned} (h' \circ f)(r) &= g(r) \\ h'(r/1) &= g(r). \end{aligned}$$

Also, let $s \in S$. Then

$$\begin{aligned} h'(s/1) &= g(s) \\ h'(s/1)^{-1} &= g(s)^{-1} \\ h'((s/1)^{-1}) &= g(s)^{-1} \\ h'(1/s) &= g(s)^{-1}. \end{aligned}$$

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, $h' = h$. □

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 ***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-algebra homomorphism*** $h : A_1 \to A_2$ is a ring homomorphism such that the

$$h(f_1(r)a) = f_2(r)h(a)$$

for $r \in R$ and $x \in A_2$; also, h is an ***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

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

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

$$\begin{aligned} h(f(r) \cdot a/s) &= h(r/1 \cdot a/s) \\ &= h(ra/s) \\ &= g(ra)g(s)^{-1} \\ &= g(r)g(a)g(s)^{-1} \\ &= g(r)h(a/s). \end{aligned}$$

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

$$\begin{aligned} h(a/s) &= g(a)g(s)^{-1} \\ 0 &= g(a)g(s)^{-1} \\ 0 &= g(a). \end{aligned}$$

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. □

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. □

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 $f : R \to R_M$ 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 $f : R \to S^{-1}R$ be the natural map. As usual, with respect to f we have the extension and contraction maps:

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

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

$$(J^c)^e = \big(f(f^{-1}(J))\big) \subseteq (J) = J.$$

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

$$\begin{aligned} y &= a_1/s_1 \cdot f(b_1) + \cdots + a_n/s_n \cdot f(b_n) \\ &= a_1/s_1 \cdot b_1/1 + \cdots + a_n/s_n \cdot b_n/1 \\ &= a_1 b_1/s_1 + \cdots + a_n b_n/s_n \\ &= (a_1 b_1 s_2 \cdots s_n)/s_1 \cdots s_n + \cdots + (a_n b_n s_1 \cdots s_{n-1})/s_1 \cdots s_n \\ &= \left(a_1 b_1 s_2 \cdots s_n + \cdots + a_n b_n s_1 \cdots s_{n-1}\right)/s_1 \cdots s_n \end{aligned}$$

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

$$a_1 b_1 s_2 \cdots s_n + \cdots + a_n b_n s_1 \cdots s_{n-1} \in I.$$

This proves that I^c is contained in $\{y \in S^{-1}R : y = a/s$ for some $a \in I$ and $s \in S\}$. Conversely, let $y \in \{y \in S^{-1}R : y = a/s$ for some $a \in I$ 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, $\{y \in S^{-1}R : y = a/s$ for some $a \in I$ 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, $Q \subseteq f^{-1}(f(Q)) \subset (Q^e)^c$. 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 $Q = (Q^e)^c$. □

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, $f(I \cap J) \subset f(J)$. 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., $ua^n t = ubs^n$. We have $ua^n t = ubs^n \in I$ because $b \in I$. Now

$$(uta)^n = u^{n-1}t^{n-1}(uta^n) \in I.$$

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, $I^e = S^{-1}R$. □

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*

$$\{P \in \operatorname{Spec}(R) : P \cap S = \emptyset\} \overset{\text{extension}}{\longrightarrow} \operatorname{Spec}(S^{-1}R)$$

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

$$\operatorname{Spec}(S^{-1}R) \overset{\text{contraction}}{\longrightarrow} \{P \in \operatorname{Spec}(R) : P \cap S = \emptyset\}.$$

Proof. We first prove that the extension map is well-defined. Let $P \in \operatorname{Spec}(R)$, and assume that $P \cap S = \emptyset$. We need to prove that $P^e \in \operatorname{Spec}(S^{-1}R)$. 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 $P' \in \operatorname{Spec}(S^{-1}R)$; 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., $a \in (P')^c$ or $b \in (P')^c$; thus, $(P')^c$ 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 $(P^e)^c = P$ if $P \in \{P \in \operatorname{Spec}(R) : P \cap S = \emptyset\}$ and by Lemma 63, $((P')^c)^e = P'$ if $P' \in \operatorname{Spec}(S^{-1}R)$. □

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*

$$\{Q \text{ is a primary ideal of } R \text{ such that } Q \cap S = \emptyset\} \overset{\text{extension}}{\longrightarrow} \{Q' \text{ is a primary ideal of } S^{-1}R\}$$

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

$$\{Q' \text{ is a primary ideal of } S^{-1}R\} \overset{\text{contraction}}{\longrightarrow} \{Q \text{ is a primary ideal of } R \text{ such that } Q \cap S = \emptyset\}.$$

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 prove 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

$$I^e = Q_1^e \cap \cdots \cap Q_m^e \quad \text{and} \quad \sqrt{Q_i^e} = P_i^e \quad \text{for } 1 \leq i \leq m$$

and

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

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

$$\begin{aligned} I^e &= (Q_1 \cap \cdots \cap Q_n)^e \\ &= Q_1^e \cap \cdots \cap Q_n^e \\ &= S^{-1}R \cap \cdots \cap S^{-1}R \\ &= S^{-1}R. \end{aligned}$$

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,

$$\begin{aligned} I^e &= (Q_1 \cap \cdots \cap Q_n)^e \\ &= Q_1^e \cap \cdots \cap Q_m^e \cap Q_{m+1}^e \cap \cdots \cap Q_n^e \\ &= Q_1^e \cap \cdots \cap Q_m^e \cap S^{-1}R \cap \cdots \cap S^{-1}R \\ &= Q_1^e \cap \cdots \cap Q_m^e. \end{aligned}$$

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:

$$\begin{aligned} (I^e)^c &= (Q_1^e \cap \cdots \cap Q_m^e)^c \\ &= (Q_1^e)^c \cap \cdots \cap (Q_m^e)^c \\ &= Q_1 \cap \cdots \cap Q_m. \end{aligned}$$

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

$$\bigcap_{\substack{i=1 \\ i \neq j}}^{m} Q_i^e \subseteq Q_j^e;$$

we will obtain a contradiction. Applying contraction, we have

$$\left(\bigcap_{\substack{i=1 \\ i \neq j}}^{m} Q_i^e \right)^c \subseteq (Q_j^e)^c$$

$$\bigcap_{\substack{i=1\\ i\neq j}}^{m}(Q_i^e)^c \subseteq (Q_j^e)^c$$

$$\bigcap_{\substack{i=1\\ i\neq j}}^{m} Q_i \subseteq Q_j.$$

The last inclusion implies that

$$\bigcap_{\substack{i=1\\ i\neq j}}^{n} Q_i \subseteq \bigcap_{\substack{i=1\\ i\neq j}}^{m} Q_i \subseteq Q_j;$$

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 $\operatorname{ass}_R(I) = \{P_1, \ldots, P_n\}$. Let*

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

and

$$I = Q_1' \cap \cdots \cap Q_n' \quad \textit{with} \quad \sqrt{Q_i'} = P_i, \quad i \in \{1, \ldots, n\}$$

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 $P_i = P_j$. 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

$$\begin{aligned}\sqrt{((P^n)^e)^c} &= (\sqrt{(P^n)^e})^c \qquad \text{(see Exercise 2.43)} \\ &= (P^e)^c \\ &= P. \qquad \text{(Theorem 67)}\end{aligned}$$

This completes the proof. □

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.

6 Modules

Let R be a commutative ring. An ***R-module*** or ***module over*** R, is an abelian group M (written additively) and a function

$$\cdot : R \times M \to M$$

such that for all $r, r' \in R$ and $m, m' \in M$ we have

(i) $r \cdot (m + m') = r \cdot m + r \cdot m'$;

(ii) $(r + r') \cdot m = r \cdot m + r' \cdot m$;

(iii) $r \cdot (r' \cdot m) = (rr') \cdot m$;

(iv) $1 \cdot m = m$.

Usually, we omit the dot $\cdot$ from the notation. The definition of an R-module is analogous to that of a vector space. In fact, if R is a field, then an R-module is a vector space over R.

Example. Let R be a commutative ring, and let I be an ideal of R. Then I is an R-module with the usual multiplication $R \times I \to I$. In particular, R is an R-module over itself. Also, R/I is an R-module with multiplication $R \times R/I \to R/I$ given by $r \cdot (r' + I) = rr' + I$ for $r, r' \in R$.

Example. Let A be an abelian group, written additively. Then A is naturally a $\mathbb{Z}$-module with multiplication $\mathbb{Z} \times A \to A$ given by

$$n \cdot a = \text{sign}(a) \underbrace{(a + \cdots + a)}_{|n| \text{ times}}$$

for $n \in \mathbb{Z}$ and $a \in A$. The proof this is an assigned exercise.

Example. Let K be a field, and let $R = K[X]$ where X is an indeterminate. Let V be a K-vector space, and let $T : V \to V$ be a K-linear map. Define

$$K[X] \times V \longrightarrow V$$

by

$$p(X) \cdot v = p(T)v$$

for $p(X) \in R$ and $v \in V$. Then with this definition, V is an R-module. This is an important example that can be used to study T.

Example. Let R and S be commutative rings, and let $f : R \to S$ be a ring homomorphism. Let M be an S-module. Define $R \times M \to M$ by $r \cdot m = f(r)m$ for $r \in R$ and $m \in M$. With this definition, M is an R-module, call the ***restriction of scalars*** from the original S-module M.

Let R be a commutative ring, and let M be an R-module. Let N be a subset of M. We say that N is a ***R-submodule*** of M if

(i) N is an addtive subgroup of M;

(ii) If $r \in R$ and $n \in N$, then $rn \in N$.

Clearly if N is an R-submodule of M, then N is an R-module.

Lemma 72. *Let R be a commutative ring, and let M be an R-module. Let N be a subset of M. Then N is an R-submodule of M if and only if*

(i) $N \neq \emptyset$;

(ii) If $r, r' \in R$ *and* $n, n' \in N$, *then* $rn + r'n' \in N$.

Proof. The proof of this is straightforward. □

Let R be a commutative ring, and let M be an R-module. Let J be a subset of M. By definition, the ***R-submodule generated by*** J is the intersection of all the submodules of M that contain J; note that there is at least one submodule containing J, namely M.

Lemma 73. *Let R be a commutative ring, and let M be an R-module. Let J be a subset of M, and let N be the R-submodule of M generated by J.*

(i) If $J = \emptyset$, *then* $N = 0$.

(ii) If $J \neq \emptyset$, *then*

$$N = \{\sum_{i=1}^{n} r_i a_i : n \in \mathbb{N}, r_1, \ldots, r_n \in R, a_1, \ldots, a_n \in J\}.$$

Proof. The proof is an assigned exercise. □

Let the notation be as in the previous lemma. In the case that J is finite, we say that N is ***finitely generated***. Assume that J is finite and $J = \{a_1, \ldots, a_n\}$. Then by the lemma N consists of all the possible sums

$$r_1 a_1 + \cdots r_n a_n$$

for $r_1, \ldots, r_n \in R$ and $a_1, \ldots, a_n \in J$. If J has just one element a, then we say that N is ***cyclic***; in this case, N consists of the elements ra for $r \in R$ and we write $N = Ra$.

Next, let R be a commutative ring, and let M be an R-module. Let $(N_\lambda)_{\lambda \in \Lambda}$ be a collection of R-submodules of M. The ***sum***

$$\sum_{\lambda \in \Lambda} N_\lambda$$

is defined to be R-submodule of M generated by the union

$$\bigcup_{\lambda \in \Lambda} N_\lambda$$

By Lemma 73, the elements of the sum $\sum_{\lambda \in \Lambda} N_\lambda$ are

$$a_{\lambda_1} + \cdots + a_{\lambda_t}$$

where $t \in \mathbb{N}$, $\lambda_1, \ldots, \lambda_t \in \Lambda$, and $a_{\lambda_1} \in N_{\lambda_1}, \ldots, a_{\lambda_t} \in N_{\lambda_t}$. We can write every element of $\sum_{\lambda \in \Lambda} N_\lambda$ in the form

$$\sum_{\lambda \in \Lambda} a_\lambda$$

where it is understood that $a_\lambda = 0$ for all but finitely many $\lambda \in \Lambda$. We note that if $J = \{a_1, \ldots, a_n\} \subseteq M$, then the R-submodule N generated by J is

$$N = Ra_1 + \cdots + Ra_n.$$

Let R be a commutative ring, let I be an ideal of R, and let M be an R-module. We let IM be the submodule of M generated by $\{rm : r \in I, m \in M\}$. By Lemma 73 we may deduce that

$$IM = \{\sum_{i=1}^{n} r_i a_i : n \in \mathbb{N}, r_1, \ldots, r_n \in R, a_1, \ldots, a_n \in M\}.$$

In the case that I is a principal ideal $I = (a)$, then

$$IM = (Ra)M = \{am : m \in M\};$$

in this case we write $IM = aM$.
Let R be a commutative ring, let M be an R-module, let N be an R-submodule of N, and let J be a subset of M. Assume that J is non-empty. Then

$$(N : J) = \{r \in R : ra \in N \text{ for all } a \in J\}$$

is an ideal of R. We have

$$(0 : J) = \{r \in R : ra = 0 \text{ for all } a \in J\}.$$

This ideal is called the ***annihilator*** of J. We write

$$\mathrm{Ann}(J) = (0 : J).$$

Lemma 74. *Let R be a commutative ring, and let M be an R-module. Let I be an ideal of R such that $I \subseteq \mathrm{Ann}(M)$. Define*

$$R/I \times M \longrightarrow M$$

by

$$(r + I, m) \mapsto rm.$$

With this definition, M is an R/I-module.

Proof. We first prove that $R/I \times M \to M$ is well-defined. Assume that $r + I = r' + I$ and $m \in M$. We need to prove that $rm = r'm$. Since $r + I = r' + I$, there exists $a \in I$ such that $r = r' + a$. Now

$$rm = (r' + a)m = r'm + am = r'm$$

because $a \in I \subseteq \mathrm{Ann}(M)$. It follows that $R/I \times M \to M$ is well-defined. It is straightforward to

verify that M is an R/I-module with this action. □

Let R be a commutative ring, and let M be an R-module. Let N be an R-submodule of M. Regarding M and N as abelian groups, we form the quotient module M/N. This consists of all the cosets of N:

$$M/N = \{m + N : m \in M\}.$$

The addition for M/N is given by

$$(m + N) + (m' + N) = (m + m') + N$$

for $m, m' \in M$. We define an R action

$$R \times M/N \longrightarrow M/N$$

by

$$r \cdot (m + N) = rm + N$$

for $r \in R$ and $m \in M$. The map $R \times M/N \to M/N$ is well-defined: assume that $m + N = m' + N$ and $r \in R$. Since $m + N = m' + N$, there exists $n \in N$ such that $m = m' + n$. Then

$$\begin{aligned} rm + N &= r(m' + n) + N \\ &= rm' + rn + N \\ &= rm' + N. \end{aligned}$$

because $rn \in N$. It is straightforward to verify that with this definition M/N is an R-module. We call M/N the ***residue class module*** of M by N or M modulo N.

Proposition 75. *Let R be a commutative ring, and let M be an R-module. Let N be an R-submodule of M. Then there exists a bijection*

$$\{R\text{-submodules } N' \text{ of } M \text{ such that } N \subseteq N'\} \xrightarrow{\sim} \{R\text{-submodules of } M/N\}$$

that sends N' to N'/N.

Proof. The proof is left as an assigned exercise. □

Let R be a commutative ring, and let M_1 and M_2 be R-modules, and let $f : M_1 \to M_2$ be a function. We say that f is an ***R-homomorphism*** if for all $r \in R$ and $m, m' \in M$ we have

(i) $f(m + m') = f(m) + f(m')$;

(ii) $f(rm) = rf(m)$.

Assume that f is an R-homomorphism. If f is injective, then we say that f is an ***monomorphism***. If f is surjective, we say that f is an ***epimorphism***. If f is both injective and surjective, then we

say that f is an isomorphism. If f is an isomorphism, then we say that M and N are isomorphic, and we write $M \cong N$.

Lemma 76. *Let R be a commutative ring, let M and N be R-modules, and let $f : M \to N$ be a homomorphism. Let $\ker(f) = \{m \in M : f(m) = 0\}$. Then $\ker(f)$ is an R-submodule of M. Moreover, f is a monomorphism, i.e., f is injective, if and only if $\ker(f) = 0$.*

Proof. Now

$$f(0) = f(0+0) = f(0) + f(0).$$

This implies that $f(0) = 0$, so that $0 \in \ker(f)$ and $\ker(f)$ is non-empty. Let $r, r' \in R$ and $m, m' \in \ker(f)$. Then

$$f(rm + r'm) = rf(m) + r'f(m') = r \cdot 0 + r' \cdot 0 = 0.$$

By Lemma 72 the set $\ker(f)$ is an R-submodule of M.
Next, assume that f is injective. Let $m \in \ker(f)$. Then $f(m) = 0 = f(0)$. Since f is injective, we must have $m = 0$. Hence, $\ker(f) = 0$. Conversely, assume that $\ker(f) = 0$. Suppose that $m, m' \in M$ are such that $f(m) = f(m')$; then $f(m - m') = 0$. Thus, $m - m' \in \ker(f) = 0$. This implies that $m = m'$ so that f is injective. □

Example. Let R be a commutative ring, let M be an R-module, and let N be an R-submodule of M. Define

$$f : M \longrightarrow M/N$$

by $f(m) = m + N$ for $m \in M$. It is straightforward to verify that f is an epimorphism. As usual, we refer to f as the ***natural map*** or ***natural homomorphism***.
Example. Let R be a commutative ring, and let M and N be R-modules. Consider the set

$$\mathrm{Hom}_R(M, N)$$

of all R-homomorphisms from M to N. Let $f_1, f_2 \in \mathrm{Hom}_R(M, N)$. Define

$$f_1 + f_2 : M \longrightarrow N$$

by

$$(f_1 + f_2)(m) = f_1(m) + f_2(m)$$

for $m \in M$. It is straightforward to verify that $f_1 + f_2 \in \mathrm{Hom}_R(M, N)$. The function $0 : M \to N$ that sends every element of M to $0 \in N$ is an R-homomorphism. Moreover,

$$0 + f = f + 0$$

for all $f \in \mathrm{Hom}_R(M,N)$. Also, if $f \in Hom_R(M,N)$, define

$$-f : M \longrightarrow N$$

by

$$(-f)(m) = -f(m)$$

for $m \in M$. Then $-f \in \mathrm{Hom}_R(M,N)$ for $f \in \mathrm{Hom}_R(M,N)$. We have

$$f + (-f) = 0 = (-f) + f$$

for $f \in \mathrm{Hom}_R(M,N)$. With this addition, $\mathrm{Hom}_R(M,N)$ is an abelian group. But $\mathrm{Hom}_R(M,N)$ has even more structure. Define an R-action

$$R \times \mathrm{Hom}_R(M,N) \longrightarrow \mathrm{Hom}_R(M,N)$$

by $(r,f) \mapsto rf$ for $r \in R$ and $f \in \mathrm{Hom}_R(M,N)$, where

$$rf : M \longrightarrow N$$

is defined by

$$(rf)(m) = rf(m)$$

for $r \in R$ and $m \in M$. It is straightforward to verify that this function is well-defined and that with this definition $\mathrm{Hom}_R(M,N)$ is an R-module.

Theorem 77 (First Isomorphism Theorem)**.** *Let R be a commutative ring, let M and N be R-modules, and let $f \in \mathrm{Hom}_R(M,N)$. Then f induces a well-defined isomorphism*

$$\bar{f} : M/\ker(f) \xrightarrow{\sim} \mathrm{im}(f)$$

such that $\bar{f}(m + \ker(f)) = f(m)$ for $m \in M$.

Proof. We first prove that f is well-defined. Let $m, m' \in M$ be such that $m + \ker(f) = m' + \ker(f)$. Then there exists $k \in \ker(f)$ such that $m = m' + k$. We have

$$\begin{aligned} f(m) &= f(m' + k) \\ &= f(m') + f(k) \\ &= f(m') + 0 \\ &= f(m'). \end{aligned}$$

It follows that f is well-defined. Next, let $m, m' \in M$ and $r \in R$. Then

$$\bar{f}((m + \ker(f)) + (m' + \ker(f)) = f((m + m') + \ker(f))$$

$$\begin{aligned} &= f(m+m') \\ &= f(m)+f(m') \\ &= \bar{f}(m+\ker(f))+\bar{f}(m'+\ker(f)). \end{aligned}$$

And

$$\begin{aligned} \bar{f}(r(m+\ker(f))) &= \bar{f}(rm+\ker(f)) \\ &= f(rm) \\ &= rf(m) \\ &= rf(m+\ker(f)). \end{aligned}$$

It follows that $\bar{f}$ is an R-homomorphism. The definition of $\bar{f}$ implies that $\ker(\bar{f})=0$; also, it is clear that $\bar{f}$ is surjective. Hence, $\bar{f}$ is an isomorphism. □

Theorem 78 (Second Isomorphism Theorem)**.** *Let R be a commutative ring, let M be an R-module, and let N_1 and N_2 be R-submodules of M such that $N_2 \subseteq N_1$. Then there is an isomorphism*

$$g : (M/N_2)/(N_1/N_2) \xrightarrow{\sim} M/N_1.$$

such that $g((m+N_2)+N_1/N_2) = m+N_2$ for $m \in M$.

Proof. Define $f : M/N_2 \to M/N_1$ by $f(m+N_2) = m+N_1$. It is straightforward to verify that f is a well-defined R-homomorphism. If $m \in M$, then $f(m+N_2) = m+N_1$; this implies that f is surjective. To determine the kernel of f, let $m \in M$. Then

$$\begin{aligned} f(m+N_2)=0 &\iff m+N_1 = 0_{M/N_1} \\ &\iff m+N_1 = N_1 \\ &\iff m \in N_1 \\ &\iff m+N_2 \in N_1/N_2. \end{aligned}$$

Thus, $\ker(f) = N_1/N_2$. The proof is now completed by applying the First Isomorphism Theorem to f; we have $\bar{f} = g$. □

Theorem 79 (Third Isomorphism Theorem)**.** *Let R be a commutative ring, and let M be an R-module. Let N_1 and N_2 be R-submodules of M. Then there is an isomorphism*

$$g : N_1/(N_1 \cap N_2) \xrightarrow{\sim} (N_1+N_2)/N_2$$

such that $g(n+N_1 \cap N_2) = n+N_2$ for $n \in N_1$.

Proof. Define $f : N_1 \to (N_1+N_2)/N_2$ by $f(n) = n+N_2$ for $n \in N_1$. It is straightforward to verify that f is an R-homomorphism. To see that f is surjective, let $y \in N_1+N_2$. Then there exist

$n_1 \in N_1$ and $n_2 \in N_2$ such that $y = n_1 + n_2$. Now

$$\begin{aligned} f(n_1) &= n_1 + N_2 \\ &= n_1 + n_2 + N_2 \\ &= y + N_2. \end{aligned}$$

Thus, f is surjective. Next, we determine the kernel of f. let $n \in N_1$. Then

$$\begin{aligned} f(n) = 0 &\iff n + N_2 = 0_{(N_1+N_2)/N_2} \\ &\iff n + N_2 = N_2 \\ &\iff n \in N_2 \\ &\iff n \in N_1 \cap N_2. \end{aligned}$$

Hence, $\ker(f) = N_1 \cap N_2$. The proof is now completed by applying the First Isomorphism Theorem to f; then $\bar{f} = g$. □

We introduce some further concepts concerning homomorphisms. Let R be a commutative ring, and let A, B, and C be R-modules. Let

$$A \xrightarrow{g} B \xrightarrow{f} C$$

be a sequence of R-homomorphisms. We say that this sequence is ***exact*** if $\mathrm{im}(g) = \ker(f)$. More generally, let

$$M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} \cdots \xrightarrow{f_{n-2}} M_{n-1} \xrightarrow{f_{n-1}} M_n$$

be a sequence of R-homomorphisms. We say that this sequence is ***exact*** if it is exact at each joint, i.e.,

$$\mathrm{im}(f_i) = \ker(f_{i+1})$$

for $i = 1, \ldots, n-2$. The exactness concept can be used to characterize injectivity and surjectivity.

Lemma 80. *Let R be a commutative ring, let M and N be R-modules, and let $f : M \to N$ be an R-homomorphism. Then*

(i) f is injective if and only if $0 \to M \xrightarrow{f} N$ is exact.

(ii) f is surjective if and only if $M \xrightarrow{f} N \to 0$ is exact.

Here, $0 \to M$ and $N \to 0$ are the uniquely determined R-homomorphisms.

Proof. For (i), we have:

$$\begin{aligned} f \text{ is injective} &\iff \ker(f) = 0 \\ &\iff \ker(f) = \mathrm{im}(0 \to M) \\ &\iff 0 \to M \xrightarrow{f} N \text{ is exact.} \end{aligned}$$

For (ii), we have:

$$\begin{aligned} f \text{ is surjective} &\iff \text{im}(f) = N \\ &\iff \text{im}(f) = \ker(N \to 0) \\ &\iff M \xrightarrow{f} N \to 0 \text{ is exact.} \end{aligned}$$

This completes the proof. □

Example. Let R be a commutative ring, let M be an R-module, and let N be an R-submodule of M. Then the following sequence is exact:

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

is exact. Here, $N \to M$ is the inclusion map, and $M \to M/N$ is the natural map.

Let R be a commutative ring, and let $(M_\lambda)_{\lambda \in \Lambda}$ be a non-empty collection of R-modules. There are two fundamental constructions of R-modules from $(M_\lambda)_{\lambda \in \Lambda}$ which we will define. First, we define the ***direct product***

$$\prod_{\lambda \in \Lambda} M_\lambda$$

of $(M_\lambda)_{\lambda \in \Lambda}$ to be the Cartesian product of the M_λ, $\lambda \in \Lambda$; the typical element of the direct product has the form

$$(m_\lambda)_{\lambda \in \Lambda}$$

where $m_\lambda \in M_\lambda$ for $\lambda \in \Lambda$. We define an addition on the direct product by

$$(m_\lambda)_{\lambda \in \Lambda} + (m'_\lambda)_{\lambda \in \Lambda} = (m_\lambda + m'_\lambda)_{\lambda \in \Lambda}$$

for $(m_\lambda)_{\lambda \in \Lambda}, (m'_\lambda)_{\lambda \in \Lambda}$ in the direct product, and we define an R-action on the direct product by

$$r \cdot (m_\lambda)_{\lambda \in \Lambda} = (r m_\lambda)_{\lambda \in \Lambda}$$

for $(m_\lambda)_{\lambda \in \Lambda}$. With these definitions, it straightforward to verify that the direct product is an R-module.

The ***external direct sum***

$$\bigoplus_{\lambda \in \Lambda} M_\lambda$$

is the subset of the direct product consisting of all the elements $(m_\lambda)_{\lambda \in \Lambda}$ such that $m_\lambda = 0$ for all but finitely many $\lambda \in \Lambda$. It is straightforward to verify that the external direct sum is an R-submodule of the external direct product.

Example. Let $R = \mathbb{Z}$, $\Lambda = \mathbb{N}$, and for $\lambda \in \Lambda$, let $M_\lambda = \mathbb{Z}$. Then the direct product is

$$\prod_{\lambda \in \Lambda} M_\lambda = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots ,$$

so that the direct product consists of all sequences of integers, with addition and the $\mathbb{Z}$-action being defined component-wise. The external direct sum consists of all the integer sequences where all but finitely many of the elements of the sequence are zero.

There is also the concept of an internal direct sum. Let R be a commutative ring, and let M be an R-module. Let $(M_\lambda)_{\lambda \in \Lambda}$ be a collection of R-submodules of M. Assume that

$$M = \sum_{\lambda \in \Lambda} M_\lambda.$$

Then every element of M can be written in the form

$$m = \sum_{\lambda \in \Lambda} m_\lambda$$

where $m_\lambda = 0$ for all but finitely many $\lambda \in \Lambda$. We say that M is the ***internal direct sum*** of $(M_\lambda)_{\lambda \in \Lambda}$ if

(i) $M = \sum_{\lambda \in \Lambda} M_\lambda$;

(ii) every element m of M has a unique expression in the form $m = \sum_{\lambda \in \Lambda} m_\lambda$.

Lemma 81. *Let R be a commutative ring, and let M an R-module, and let K and Q be R-submodules of M. Then M is the internal direct sum of K and Q if and only if $M = K + Q$ and $K \cap Q = 0$.*

Proof. Assume that M is the internal direct sum of K and Q. Because M is the internal direct sum of K and Q, every element of M can be written as $m = k + q$ for some $k \in K$ and $q \in Q$, and this representation is unique. It follows that $M = K + Q$. Let $m \in K \cap Q$. Then $m = m + 0$ with $m \in K$ and $0 \in Q$; but we also have $m = 0 + m$ with $0 \in K$ and $m \in Q$. By the uniqueness of the representation of m we must have $m = 0$, so that $K \cap Q = 0$.

Next, assume that $M = K + Q$ and $K \cap Q = 0$. To prove that M is the internal direct sum of Q and K we need to prove that every element $m \in M$ can be uniquely written in the form $m = k + q$ where $k \in K$ and $q \in Q$. Since $M = K + Q$ we see that every element $m \in M$ can be written in the form $m = k + q$ where $k \in K$ and $q \in Q$. To see that this representation is unique, assume that $k_1, k_2 \in K$ and $q_1, q_2 \in Q$ are such that $k_1 + q_1 = k_2 + q_2$. Then

$$k_1 - k_2 = q_2 - q_1 \in K \cap Q = 0.$$

Therefore, $k_1 = k_2$ and $q_1 = q_2$, as desired. □

External and internal direct sums are related by the following proposition.

Proposition 82. *Let R be a commutative ring, let M be an R-module, and let $(M_\lambda)_{\lambda\in\Lambda}$ be a collection of R-submodules of M. Assume that M is the internal direct sum of $(M_\lambda)_{\lambda\in\Lambda}$. Then the function*

$$f : \bigoplus_{\lambda\in\Lambda} M_\lambda \xrightarrow{\sim} M$$

defined by

$$f((m_\lambda)_{\lambda\in\Lambda}) = \sum_{\lambda\in\Lambda} m_\lambda$$

for $(m_\lambda)_{\lambda\in\Lambda}$ in the external direct sum is a well-defined R-isomorphism.

Proof. The function f is well-defined because if $(m_\lambda)_{\lambda\in\Lambda}$ is in the external direct sum, then $m_\lambda = 0$ for all but finitely many $\lambda \in \Lambda$; hence the sum $\sum_{\lambda\in\Lambda} m_\lambda$ is meaningful. Next, let $(m_\lambda)_{\lambda\in\Lambda}$ and $(m'_\lambda)_{\lambda\in\Lambda}$ be in the extenal direct sum, and let $r \in R$. Then

$$\begin{aligned} f((m_\lambda)_{\lambda\in\Lambda} + (m'_\lambda)_{\lambda\in\Lambda}) &= f((m_\lambda + m'_\lambda)_{\lambda\in\Lambda} \\ &= \sum_{\lambda\in\Lambda} (m_\lambda + m'_\lambda) \\ &= \sum_{\lambda\in\Lambda} m_\lambda + \sum_{\lambda\in\Lambda} m'_\lambda \\ &= f((m_\lambda)_{\lambda\in\Lambda}) + f((m'_\lambda)_{\lambda\in\Lambda}). \end{aligned}$$

And

$$\begin{aligned} f(r \cdot (m_\lambda)_{\lambda\in\Lambda}) &= f((rm_\lambda)_{\lambda\in\Lambda}) \\ &= \sum_{\lambda\in\Lambda} rm_\lambda \\ &= r \sum_{\lambda\in\Lambda} m_\lambda \\ &= rf((m_\lambda)_{\lambda\in\Lambda}). \end{aligned}$$

This proves that f is an R-homomorphism. To see that f is injective, assume that $(m_\lambda)_{\lambda\in\Lambda}$ and $(m'_\lambda)_{\lambda\in\Lambda}$ are in the external direct sum and

$$f((m_\lambda)_{\lambda\in\Lambda}) = f((m'_\lambda)_{\lambda\in\Lambda}).$$

Then

$$\sum_{\lambda\in\Lambda} m_\lambda = \sum_{\lambda\in\Lambda} m'_\lambda.$$

Since M is the internal direct sum of $(M_\lambda)_{\lambda\in\Lambda}$ we must have $m_\lambda = m'_\lambda$ for $\lambda \in \Lambda$. This proves that f is injective. The R-homomorphism f is surjective because M is, by hypothesis, $\sum_{\lambda\in\Lambda} M_\lambda$. □

Let R be a commutative ring, and let $(M_\lambda)_{\lambda\in\Lambda}$ be a collection of R-modules. Let

$$M = \bigoplus_{\lambda\in\Lambda} M_\lambda.$$

Let $\mu \in \Lambda$. The ***canonical projection***

$$p_\mu : M \longrightarrow M_\mu$$

is defined by

$$p_\mu((m_\lambda)_{\lambda\in\Lambda}) = m_\lambda$$

for $(m_\lambda)_{\lambda\in\Lambda} \in M$. The ***canonical injection***

$$q_\mu : M_\mu \longrightarrow M$$

is defined by

$$q_\mu(m) = (m_\lambda)_{\lambda\in\Lambda}$$

where

$$m_\lambda = \begin{cases} m & \text{if } \lambda = \mu, \\ 0 & \text{if } \lambda \neq \mu. \end{cases}$$

The canonical projections and injections are easily seen to be R-homomorphisms. We have

$$p_\nu \circ q_\mu = \begin{cases} \mathrm{id}_{M_\mu} & \text{if } \nu = \mu, \\ 0 & \text{if } \nu \neq \mu. \end{cases}$$

Canonical projections and injections may also be defined for direct products. In addition, canonical projections and injections may be used to show that the direct product and external direct sum have certain universal properties.

Let R be a commutative ring, and let

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be a sequence of R-modules. If this sequence is exact, then we say that this is a ***short exact sequence***.

Example. Let R be a commutative ring, and let M be an R-module, and let N be an R-submodule of M. Then the sequence

$$0 \longrightarrow N \longrightarrow M \longrightarrow M/N \longrightarrow 0$$

is a short exact sequence.

Let R be a commutative ring, and let

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a short exact sequence of R-modules. We say that this sequence is ***split*** if

$$K = \ker(g) = \mathrm{im}(f)$$

is a direct summand of B, i.e., there exists an R-submodule Q of B such that B is the internal direct sum of K and Q:

$$B \cong K \oplus Q.$$

Lemma 83. *Let R be a commutative ring, and let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a short exact sequence of R-modules. Then the following are equivalent:

(i) The sequence is split.

(ii) There exists an R-homomorphism $t : C \to B$ such that $g \circ t = \mathrm{id}_C$.

(iii) There exists an R-homomorphism $s : B \to A$ such that $s \circ f = \mathrm{id}_A$.

Proof. Let $K = \ker(g)$.
(i) $\implies$ (ii). Assume that the sequence is split. Then there exists an R-submodule Q of B such that B is the internal direct sum of K and Q. By Lemma 81 we have $B = K + Q$ and $K \cap Q = 0$. By the First Isomorphism Theorem the map

$$\bar{g} : B/K \xrightarrow{\sim} C, \qquad b + K \mapsto g(b),$$

is an isomorphism. Now define

$$i : Q \longrightarrow B/K$$

by $i(q) = q + K$ for $q \in Q$. We claim that i is an R-isomorphism. Since i is the restriction of the natural map $B \to B/K$, i is an R-homomorphism. To see that i is injective, assume that $q \in Q$ is such that $i(q) = 0$. Then

$$0 = i(q) = q + K = 0_{B/K} = K$$

so that $q \in K$. We now have $q \in K \cap Q = 0$. Thus, i is injective. To see that i is surjective, let $b \in B$. Then $b = k + q$ for some $k \in K$ and $q \in Q$. We have

$$i(q) = q + K = q + k + K = b + K.$$

Thus, i is surjective, and hence an R-isomorphism. We now define t be the composition:

$$t : C \xrightarrow{\bar{g}^{-1}} B/K \xrightarrow{i^{-1}} Q \xrightarrow{\text{inclusion}} B.$$

Now we prove that $g \circ t = \mathrm{id}_C$. Let $x \in C$. Then since the sequence $0 \to A \to B \to C \to 0$ is exact, there exists $b \in B$ such that $g(b) = x$. Write $b = k + q$ for some $k \in K$ and $q \in Q$. We now have

$$\begin{aligned}
(g \circ t)(x) &= g(\mathrm{inc}(i^{-1}(\bar{g}^{-1}(x)))) \\
&= g(\mathrm{inc}(i^{-1}(b + K))) \\
&= g(\mathrm{inc}(i^{-1}(q + k + K))) \\
&= g(\mathrm{inc}(i^{-1}(q + K)) \\
&= g(\mathrm{inc}(q)) \\
&= g(q) \\
&= g(q) + 0 \\
&= g(q) + g(k) \\
&= g(q + k) \\
&= g(b) \\
&= x.
\end{aligned}$$

This proves (ii).
(ii) $\implies$ (i). Assume that there exists an R-homomorphism $t : C \to B$ such that $g \circ t = \mathrm{id}_C$. Define $Q = \mathrm{im}(t)$. We claim that $B = K \oplus Q$. First we prove that $B = K + Q$. Let $b \in B$. Let $q = t(g(b))$, and set $k = b - q$. Clearly, $q \in Q$. And:

$$\begin{aligned}
g(k) &= g(b - q) \\
&= g(b) - g(q) \\
&= g(b) - g(t(g(b))) \\
&= g(b) - (g \circ t)(g(b)) \\
&= g(b) - \mathrm{id}_C(g(b)) \\
&= g(b) - g(b) \\
&= 0.
\end{aligned}$$

Thus, $k \in K = \ker(g)$. Since $b = k + q$, with $k \in K$ and $q \in Q$, we have $B = K + Q$. Finally, let $x \in K \cap Q$. Then $x = t(c)$ for some $c \in C$ by the definition of Q. Also, $g(x) = 0$ since $K = \ker(g)$. Hence,

$$\begin{aligned}
0 &= g(x) \\
&= g(t(c)) \\
&= (g \circ t)(c) \\
&= (\mathrm{id}_C(c) \\
&= c.
\end{aligned}$$

Thus, $c = 0$, so that $x = t(c) = 0$. This proves that $K \cap Q = 0$, completing the proof that $B = K \oplus Q$.
The equivalence (i) $\iff$ (iii) has a similar proof. □

Lemma 84. *Let R be a commutative ring, and let*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

be a split exact sequence of R-modules; by Lemma 83 there exists an R-homomorphism $t : C \to B$ such that $g \circ t = \mathrm{id}_C$. Then the map

$$h : A \oplus C \xrightarrow{\sim} B$$

defined by $g(a, c) = f(a) + t(c)$ is an R-isomorphism. In particular, $B \cong A \oplus C$.

Proof. It is straightforward to verify that h is an R-homomorphism. Let $(a, c) \in \ker(h)$. Then

$$\begin{aligned} 0 &= h(a, c) \\ &= f(a) + t(c). \end{aligned}$$

Applying g to this equation, we obtain:

$$\begin{aligned} 0 &= g(f(a)) + g(t(c)) \\ &= 0 + c. \end{aligned}$$

Thus, $c = 0$. We now have $f(a) = 0$. But f is injective; hence, $a = 0$. It follows that h is injective. To see that h is surjective, let $b \in B$. Let $c = g(b)$, and set $k = b - t(g(b))$. Then $k \in \ker(g) = \mathrm{im}(f)$; let $a \in A$ be such that $f(a) = k$. We now have

$$\begin{aligned} h(a, c) &= f(a) + t(c) \\ &= k + t(g(b)) \\ &= b - t(g(b)) + t(g(b)) \\ &= b. \end{aligned}$$

This proves that g is surjective. □

Example. Let R be a commutative ring, and let A and C be R-modules. Let $B = A \oplus C$, the external direct sum. Let $A \to B$ be the canonical inclusion, and let $B \to C$ be the canonical projection. Then the sequence

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

is a split short exact sequence.

Example. Consider the sequence

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathbb{Z}/4\mathbb{Z} \longrightarrow 2\mathbb{Z}/4\mathbb{Z} \longrightarrow 0$$

where $\mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ is defined by $m + 2\mathbb{Z} \mapsto 2m + 4\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \to 2\mathbb{Z}/4\mathbb{Z}$ is defined by $m + 4\mathbb{Z} \mapsto 2m + 4\mathbb{Z}$. This is a short exact sequence which is not split.

Proof. Assume that this sequence is split; we will obtain a contradiction. By Lemma 84 we have

$$\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus 2\mathbb{Z}/4\mathbb{Z}.$$

In other words, the cyclic group of order 4 is isomorphic to the direct product of two cyclic groups of order 2. This is a contradiction (the cyclic group of order 4 has one element of order 2 while the direct product of two cyclic groups of order 2 has 3 elements of order 2). □

Let R be a commutative ring, and let P be an R-module. Let $(e_\lambda)_{\lambda\in\Lambda}$ be a collection of elements of P. Then we say that $(e_\lambda)_{\lambda\in\Lambda}$ is a ***base*** for P if every element p of P can be uniquely expressed as a finite R-linear combination of the elements in the collection $(e_\lambda)_{\lambda\in\Lambda}$, i.e., for every $p \in P$ there exists a collection $(r_\lambda)_{\lambda\in\Lambda}$ with $r_\lambda = 0$ for all but finitely many $\lambda \in \Lambda$ such that

$$p = \sum_{\lambda\in\Lambda} r_\lambda e_\lambda.$$

If P admits a base, then we say that P is a ***free R-module***. The next lemma proves that a free R-module is a direct sum of copies of R.

Lemma 85. *Let R be a commutative ring, and let P be a free R-module with base $(e_\lambda)_{\lambda\in\Lambda}$. For $\lambda \in \Lambda$, define $P_\lambda = R$. Then there is an isomorphism*

$$f : \bigoplus_{\lambda\in\Lambda} P_\lambda \xrightarrow{\sim} M$$

defined by

$$f((r_\lambda)_{\lambda\in\Lambda}) = \sum_{\lambda\in\Lambda} r_\lambda e_\lambda$$

for $(r_\lambda)_{\lambda\in\Lambda} \in \bigoplus_{\lambda\in\Lambda} P_\lambda$.

Proof. It is straightforward to verify that f is an R-homomorphism. Assume that $f((r_\lambda)_{\lambda\in\Lambda}) = 0$ for some $(r_\lambda)_{\lambda\in\Lambda} \in \bigoplus_{\lambda\in\Lambda} P_\lambda$. Then

$$0 = \sum_{\lambda\in\Lambda} r_\lambda e_\lambda.$$

Since we also have

$$0 = \sum_{\lambda\in\Lambda} 0 \cdot e_\lambda$$

by the definition of a base we must have $r_\lambda = 0$ for $\lambda \in \Lambda$. This proves that f is injective. The surjectivity of f follows form the assumption that $(e_\lambda)_{\lambda\in\Lambda}$ is a base for P. □

Now suppose that R is a commutative ring, and that Λ is non-empty set. For $\lambda \in \Lambda$, let e_λ be a symbol. Consider the set P of all formal sums

$$\sum_{\lambda\in\Lambda} r_\lambda e_\lambda$$

where $r_\lambda \in R_\lambda$ and $r_\lambda = 0$ for all but finitely many $\lambda \in \Lambda$. We define an addition on P by

$$(\sum_{\lambda\in\Lambda} r_\lambda e_\lambda) + (\sum_{\lambda\in\Lambda} r'_\lambda e_\lambda) = \sum_{\lambda\in\Lambda} (r_\lambda + r'_\lambda)e_\lambda.$$

for $\sum_{\lambda\in\Lambda} r_\lambda e_\lambda, \sum_{\lambda\in\Lambda} r'_\lambda e_\lambda \in P$. We also define R-action on P by

$$r \cdot (\sum_{\lambda\in\Lambda} r_\lambda e_\lambda) = \sum_{\lambda\in\Lambda} r r_\lambda e_\lambda$$

for $r \in R$ and $\sum_{\lambda\in\Lambda} r_\lambda e_\lambda \in P$. It is straightforward to verify that with these definitions, P is a free R-module with base $(e_\lambda)_{\lambda\in\Lambda}$. We say that P is the ***free R-module on the symbols*** $(e_\lambda)_{\lambda\in\Lambda}$.

Theorem 86. *Let R be a commutative ring and let P be a free R-module with base $(e_\lambda)_{\lambda\in\Lambda}$. Let M be an R-module, and let $(m_\lambda)_{\lambda\in\Lambda}$ be a collection of elements of M. Then there exists a unique R-homomorphism $f : P \to M$ such that $f(e_\lambda) = m_\lambda$ for $\lambda \in \Lambda$.*

Proof. Define $f : P \to M$ by

$$f(\sum_{\lambda\in\Lambda} r_\lambda e_\lambda) = \sum_{\lambda\in\Lambda} r_\lambda m_\lambda$$

for $\sum_{\lambda\in\Lambda} r_\lambda e_\lambda \in P$. It is straightforward to verify that f is an R-homomorphism such that $f(e_\lambda) = m_\lambda$ for $\lambda \in \Lambda$. Moreover, it is clear that f is the unique such R-homomorphism such that $f(e_\lambda) = m_\lambda$ for $\lambda \in \Lambda$. □

Corollary 87. *Let R be a commutative ring, and let M be an R-module. Then there exists a free R-module P and a surjective R-homomorphism $f : P \to M$.*

Proof. Let $(m_\lambda)_{\lambda\in\Lambda}$ be any collection of elements of M that generate M (such an collection clearly exists). Let $(e_\lambda)_{\lambda\in\Lambda}$ be a collection of symbols, and let P be the free R-module on $(e_\lambda)_{\lambda\in\Lambda}$. By Theorem 86 there exists an R-homomorphism $f : P \to M$ such that $f(e_\lambda) = m_\lambda$ for $\lambda \in \Lambda$. Since $(m_\lambda)_{\lambda\in\Lambda}$ generates M it follows that f is surjective. □

Example. Let R be a commutative ring, and let M be an R-module generated by the finite set $\{g_1, \ldots, g_n\}$. Then by Theorem 86 there exists a free R-module P with base $(e_i)_{i\in\{1,\ldots,n\}}$ and a homomorphism $f : P \to M$ such that $f(e_i) = g_i$ for $i \in \{1, \ldots, n\}$. Let $K = \ker(f)$. Then the

following sequence is exact:

$$0 \longrightarrow K \longrightarrow P \xrightarrow{f} M \longrightarrow 0.$$

This suggests that finitely generated R-modules could be investigated by studying quotients of the form P/K.

Theorem 88. *Let R be a non-trivial commutative ring, and let P be a free R-module. Then all bases of P have the same cardinality.*

Proof. Since R is non-trivial, R has a maximal ideal M. Earlier, we introduced the R-submodule MP, the submodule of P generated by the elements rx for $r \in R$ and $x \in P$. Let $V = P/MP$. if $y = x + MP \in V$ and $r \in M$, then

$$ry = r(x + MP) = rx + MP = MP.$$

Thus, $M \subseteq \text{Ann}(P/MP)$. By a previous result, the quotient ring $V = P/MP$ is an R/M-module with R/M action defined by

$$(r + M) \cdot (x + MP) = rx + MP$$

for $r \in R$ and $x \in P$. Let $F = R/M$. Then V is an F-module. Since F is a field, V is actually an F-vector space. Now let $(e_\lambda)_{\lambda\in\Lambda}$ be a base for P. For $\lambda \in \Lambda$ define $v_\lambda = e_\lambda + MP$. To prove the theorem it will suffice to prove that the collection $(v_\lambda)_{\lambda\in\Lambda}$ is a basis for the F-vector space V (because all bases for a vector space have the same cardinality). We need prove that $(v_\lambda)_{\lambda\in\Lambda}$ spans V and is linearly independent. Let $v \in V$. Let $x \in P$ be such that $v = x + MP$. Since $(e_\lambda)_{\lambda\in\Lambda}$ is a base for P, there exists a collection $(r_\lambda)_{\lambda\in\Lambda}$ such that $r_\lambda = 0$ for all but finitely many $\lambda \in \Lambda$ and

$$x = \sum_{\lambda\in\Lambda} r_\lambda e_\lambda.$$

Hence,

$$\begin{aligned} v &= x + MP \\ &= \sum_{\lambda\in\Lambda} r_\lambda e_\lambda + MP \\ &= \sum_{\lambda\in\Lambda} (r_\lambda + P)(e_\lambda + MP) \\ &= \sum_{\lambda\in\Lambda} (r_\lambda + P)v_\lambda. \end{aligned}$$

It follows that $(v_\lambda)_{\lambda\in\Lambda}$ spans V. Now suppose that $(a_\lambda)_{\lambda\in\Lambda}$ is a collection of elements of F such that $a_\lambda = 0$ for all but finitely many $\lambda \in \Lambda$ and

$$0 = \sum_{\lambda\in\Lambda} a_\lambda v_\lambda$$

For each $\lambda \in \Lambda$ let $r_\lambda \in \Lambda$ be such that $a_\lambda = r_\lambda + M$ and $r_\lambda = 0$ if $a_\lambda = 0$. Then

$$\begin{aligned} 0 &= \sum_{\lambda \in \Lambda} (r_\lambda + P)(e_\lambda + MP) \\ &= \sum_{\lambda \in \Lambda} r_\lambda e_\lambda + MP \\ &= (\sum_{\lambda \in \Lambda} r_\lambda e_\lambda) + MP. \end{aligned}$$

It follows that

$$\sum_{\lambda \in \Lambda} r_\lambda e_\lambda \in MP.$$

Let $a_1, \ldots, a_n \in M$ and $p_1, \ldots, p_n \in P$ be such that

$$\sum_{\lambda \in \Lambda} r_\lambda e_\lambda = \sum_{i=1}^{n} a_i p_i.$$

Next, for each $i \in \{1, \ldots, n\}$, let

$$p_i = \sum_{\lambda \in \Lambda} b_{i\lambda} e_\lambda$$

where $b_{i\lambda} \in R$ for $\lambda \in \Lambda$ and $b_{i\lambda} = 0$ for all but finitely many $\lambda \in \Lambda$. Then

$$\begin{aligned} \sum_{\lambda \in \Lambda} r_\lambda e_\lambda &= \sum_{i=1}^{n} a_i (\sum_{\lambda \in \Lambda} b_{i\lambda} e_\lambda) \\ &= \sum_{\lambda \in \Lambda} (\sum_{i=1}^{n} a_i b_{i\lambda}) e_\lambda. \end{aligned}$$

Since $(e_\lambda)_{\lambda \in \Lambda}$ is a base for P, we have

$$r_\lambda = \sum_{i=1}^{n} a_i b_{i\lambda}$$

for $\lambda \in \Lambda$. Since M is an ideal and $a_1, \ldots, a_n \in M$, we conclude that $r_\lambda \in M$ for $\lambda \in \Lambda$. Therefore, $a_\lambda = r_\lambda + M = M = 0_F$ for $\lambda \in \Lambda$. Hence, $(v_\lambda)_{\lambda \in \Lambda}$ is linear independent. $\square$

7 Chain conditions on modules

In this section we consider the idea of understanding modules through composition series. We first consider chain conditions on modules.

Lemma 89. *Let R be a commutative ring, and let M be an R-module. Then the following are equivalent:*

(i) If

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

is an ascending sequence of R-submodules of M, then there exists $n \in \mathbb{N}$ such that $M_{n+k} = M_n$ for $k \in \mathbb{N}$. (This is called the **ascending chain condition***, or ACC).*

(ii) Every non-empty set of submodules of M contains a maximal element with respect to inclusion.

Proof. (i) $\implies$ (ii) Assume (i). Assume that (ii) does not hold, so that there exists a non-empty set of submodules of M that does not contain a maximal element with respect to inclusion. Let $M_1 \in X$. Then M_1 is not maximal, so that there exists $M_2 \in X$ such that $M_1 \subsetneqq M_2$. Similarly, there exists $M_3 \in X$ such that $M_2 \subsetneqq M_3$. Continuing, we obtain a sequence

$$M_1 \subsetneqq M_2 \subsetneqq M_3 \subsetneqq \cdots$$

This contradicts (i).
(ii) $\implies$ (i) Assume that (ii) holds. Let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

be a sequence R-submodules of M. Let $X = \{M_1, M_2, M_3, \dots\}$. Then X contains a maximal element, say M_n. Assume that $k \in \mathbb{N}$ and consider M_{n+k}. We have $M_n \subseteq M_{n+k}$. Since M_n is maximal, we must have $M_n = M_{n+k}$. This proves (i). □

Let R be a commutative ring, and let M be an R-module. If M satisfies one of the two equivalent conditions of Lemma 89 then we say that M is ***Noetherian***.

Lemma 90. *Let R be a commutative ring, and let M be an R-module. Then the following are equivalent:*

(i) If

$$\cdots \subseteq M_3 \subseteq M_2 \subseteq M_1$$

is a descending sequence of R-submodules of M, then there exists $n \in \mathbb{N}$ such that $M_{n+k} = M_n$ for $k \in \mathbb{N}$.(This is called the **descending chain condition***, or DCC).*

(ii) Every non-empty set of submodules of M contains a minimal element with respect to inclusion.

Proof. The proof is very similar to the proof of Lemma 89. □

Let R be a commutative ring, and let M be an R-module. If M satisfies one of the two equivalent conditions of Lemma 90 then we say that M is ***Artinian***.

Let R be a commutative ring. We can consider R as an R-module. The R-submodules of R are exactly the ideals of R. It follows that the R-module R is Noetherian if and only if R is a Noetherian ring. We will say that R is an ***Artinian ring*** if R is an Artinian R-module. This means that R satisfies the descending chain conditoion on ideals, or equivalently, every set of ideals of R has a minimal element.

Example. Let $R = \mathbb{Z}$. Then R is a Euclidean domain, and hence is a PID. Thus, R is Noetherian. However, R is not Artinian. The following descending chain of ideals does not terminate:

$$\cdots \subsetneqq 4\mathbb{Z} \subsetneqq 2\mathbb{Z} \subsetneqq \mathbb{Z}.$$

Example. If $N \in \mathbb{N}$, then $\mathbb{Z}/N\mathbb{Z}$ is Artinian.

Later, we will prove that every Artinian commutative ring is a Noetherian commutative ring. Combining this fact with the above example we have the proper inclusion

$$\text{Artinian rings} \subsetneqq \text{Noetherian rings}.$$

In light of this inclusion, it is natural to ask if every Artinian R-module is a Noetherian R-module. The answer is no.

Example. There exist $\mathbb{Z}$-modules that are Artinian but not Noetherian.

Proof. Let p be a prime. Let

$$N = \{r/p^n : r \in \mathbb{Z}, n \in \mathbb{N}_0\}.$$

Then N is a $\mathbb{Z}$-module. Also, N contains $\mathbb{Z}$ as a submodule. We define

$$M = N/\mathbb{Z}.$$

We define a sequence of submodules of M as follows. Let $t \in \mathbb{N}_0$. We define

$$N_t = \{r/p^t : r \in \mathbb{Z}\} = \frac{1}{p^t}\mathbb{Z}.$$

Evidently, we have

$$N_0 \subsetneqq N_1 \subsetneqq N_2 \subsetneqq N_3 \subsetneqq \cdots$$

Let $f : N \to N/\mathbb{Z} = M$ be the natural map, and for $t \in \mathbb{N}_0$ define

$$M_t = f(N_t) = N_t/\mathbb{Z}.$$

We have

$$M_0 \subsetneqq M_1 \subsetneqq M_2 \subsetneqq M_3 \subsetneqq \cdots$$

It follows that M is not Noetherian. Next we will prove that M is Artinian. Let

$$\cdots \subseteq W_3 \subseteq W_2 \subseteq W_1$$

be a descending sequence of submodules of M. We need to understand the W_t. Let W be a proper submodule of M. We will prove that $W = M_t$ for some $t \in \mathbb{N}$. If $W = 0$, then $W = M_0$. Assume that $W \neq 0$. Then there exists $n \in \mathbb{N}$ and $r \in \mathbb{Z}$ such that $r/p^n + \mathbb{Z} \in W$ and $r/p^n \notin \mathbb{Z}$. We may assume that r and p are relatively prime. We claim that $M_n \subseteq W$. Let $a/p^n + \mathbb{Z} \in M_n$, where $a \in \mathbb{Z}$. Since r and p^n are relatively prime, there exist $x, y \in \mathbb{Z}$ such that $rx + p^n y = 1$. Hence

$$rxa + p^n ya = a$$

so that

$$\begin{aligned} rxa/p^n + p^n ya/p^n &= a/p^n \\ rxa/p^n + ya &= a/p^n \\ rxa/p^n + ya + \mathbb{Z} &= a/p^n + \mathbb{Z} \\ rxa/p^n + \mathbb{Z} &= a/p^n + \mathbb{Z} \\ xa\,(r/p^n + \mathbb{Z}) &= a/p^n + \mathbb{Z}. \end{aligned}$$

Since $r/p^n + \mathbb{Z} \in W$, we find that $a/p^n + \mathbb{Z} \in W$. This proves that $M_n \subseteq W$. Now since W is proper, and since M is the union of the M_i, it follows that there exists $m \in \mathbb{N}$ such that $M_m \nsubseteq W$; this implies that $M_j \nsubseteq W$ for all $j \geq m$. It follows that there exists a largest element n of $\mathbb{N}$ such that $M_n \subseteq W$. We claim that in fact $M_n = W$. Let $r/p^k + \mathbb{Z} \in W$; we will prove that $r/p^k + \mathbb{Z} \in M_n$. We may assume that $r/p^k \notin \mathbb{Z}$ and that r and p are relatively prime. Arguing as above, we find that $M_k \subseteq W$. By the definition of n we must have $k \leq n$. Therefore,

$$\begin{aligned} r/p^k + \mathbb{Z} &= rp^{n-k}/p^k + \mathbb{Z} \\ &= p^{n-k}(r/p^n + \mathbb{Z}) \\ &\in M_n. \end{aligned}$$

Thus, $W \subseteq M_n$, so that $W = M_n$.
We now consider again our descending chain

$$\cdots \subseteq W_3 \subseteq W_2 \subseteq W_1.$$

For each $i \in \mathbb{N}$, let $n_i \in \mathbb{N}$ be such that $W_i = M_{n_i}$. Our chain is then

$$\cdots \subseteq M_{n_3} \subseteq M_{n_2} \subseteq M_{n_1}.$$

In general, $M_k \subseteq M_j$ if and only if $k \leq j$. Thus,

$$\cdots \leq n_3 \leq n_2 \leq n_1.$$

Since each of these integers is non-negative, there exists $k \in \mathbb{N}$ such that

$$n_k = n_{k+1} = n_{k+2} = \cdots .$$

This means that

$$W_k = W_{k+1} = W_{k+2} = \cdots .$$

Thus, M satisfies the descending chain condition and is thus Artinian. □

Lemma 91. *Let R be a commutative ring, and let M be an R-module. Then M is Noetherian if and only if every submodule of M is finitely generated.*

Proof. The argument is very similar to the proof of Lemma 23. □

Lemma 92. *Let R be a commutative ring. Let M be an R-module, and let N be an R-submodule of M. Then:*

(i) M is Noetherian if and only if N and M/N are Noetherian.

(ii) M is Artinian if and only if N and M/N are Artinian.

Proof. (i) Assume that M is Noetherian. Let

$$N_1 \subseteq N_2 \subseteq N_3 \subseteq \cdots$$

be an ascending chain of R-submodules of N. Since this is also an ascending chain of R-submodules of M, and since M is Noetherian, there exists $n \in \mathbb{N}$ such that $N_{n+k} = N_n$ for $k \in \mathbb{N}$. Next, let

$$W_1 \subseteq W_2 \subseteq W_3 \subseteq \cdots$$

be an ascending chain of R-submodules of M/N. let $f : M \to M/N$ be the natural map. then

$$f^{-1}(W_1) \subseteq f^{-1}(W_2) \subseteq f^{-1}(W_3) \subseteq \cdots$$

is an ascending chain of R-submodules of M. Since M is Noetherian, there exists $n \in \mathbb{N}$ such that $f^{-1}(W_{n+k}) = f^{-1}9W_n)$ for $k \in \mathbb{N}$. Now $f(f^{-1}(W_m)) = W_m$ for $m \in \mathbb{N}$. Hence, $W_{n+k} = W_n$ for $k \in \mathbb{N}$.

Now assume that N and M/N are Noetherian. Let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

be an ascending chain of R-submodules of M. We may consider the chain

$$M_1 \cap N \subseteq M_2 \cap N \subseteq M_3 \cap N \subseteq \cdots .$$

This is an ascending chain of R-submodules of N. Since N is Noetherian, there exists $n \in \mathbb{N}$ such that $M_{n+k} \cap N = M_n \cap N$ for $k \in \mathbb{Z}$. Again let $f : M \to M/N$ be the natural map. Then

$$f(M_1) \subseteq f(M_2) \subseteq f(M_3) \subseteq \cdots$$

is an ascending chain of R-submodules of M/N. Since M/N is Noetherian, there exists $m \in \mathbb{N}$ such that $f(M_{m+k}) = f(M_m)$ for $k \in \mathbb{N}$. Let $t = \max(m, n)$. We claim that $M_{t+k} = M_t$ for $k \in \mathbb{N}$. Let $k \in \mathbb{N}$. Let $x \in M_{t+k}$; we need to prove that $x \in M_t$. Now $f(M_{t+k}) = f(M_k)$. Therefore,

$$f(x) = x + N \in f(M_t).$$

This implies that there exists $y \in M_t$ such that $x + N = y + N$. Let $n \in N$ be such that $x = y + n$. Then

$$x - y = n \in M_{t+k} \cap N = M_t \cap N.$$

So

$$x = y + n \in M_t$$

as desired.
The proof of (ii) is similar and will be omitted. □

Corollary 93. *Let R be a commutative ring, and let $M_1, \ldots, M_n$ be R-modules. Then:*
(i) The direct sum $\bigoplus_{i=1}^n M_i$ is Noetherian if and only if $M_1, \ldots, M_n$ are Noetherian.
(ii) The direct sum $\bigoplus_{i=1}^n M_i$ is Artinian if and only if $M_1, \ldots, M_n$ are Artinian.

Proof. We prove these statements by induction on n. The statements are trivial if $n = 1$. Assume that $n > 1$ and that the statements hold for $m < n$. Let $j \in \{1, \ldots, n\}$. Assume that $\bigoplus_{i=1}^n M_i$ is Noetherian (Artinian). We may view M_j as an R-submodule of $\bigoplus_{i=1}^n M_i$ via the canonical injection. By Lemma 92, M_j is Noetherian (Artinian). Next, assume that $M_1, \ldots, M_n$ are Noetherian (Artinian). Regard M_1 as an R-submodule of $\bigoplus_{i=1}^n M_i$ via the canonical inclusion. Then

$$\left(\bigoplus_{i=1}^{n} M_i \right) / M_1 \cong \bigoplus_{i=2}^{n} M_i$$

Also, M_1 is Noetherian (Artinian), and by the induction hypothesis,

$$\bigoplus_{i=2}^{n} M_i$$

is Noetherian (Artinian). Lemma 92 now implies that $\bigoplus_{i=1}^{n} M_i$ is Noetherian (Artinian). □

From Corollary 93 we see that if R is a Noetherian (Artinian) ring, then a free R-module with a finite base is Noetherian (Artinian). In fact, more is true:

Lemma 94. *Let R be a commutative ring.*

(i) If R is a Noetherian ring, then every finitely-generated R-module is Noetherian.

(ii) If R is an Artinian ring, then every finitely-generated R module is Artinian.

Proof. Let M be an R-module, and assume that M is finitely-generated. By the example on page 74 there exists a free R-module P with a finite base and a surjective R-homomorphism $f : P \to M$. Let $K = \ker(f)$. Then $M \cong P/K$. Assume that R is Noetherian (Artinian). Then by Corollary 93, P is Noetherian (Artinian). Hence, by Lemma 92, P/K is Noetherian (Artinian). This implies that M is Noetherian (Artinian). □

Lemma 95. *Let K be a field, and let V be a K-vector space. Then the following are equivalent:*

(i) V is a finite-dimensional K-vector space.

(ii) V is a Noetherian K-module.

(iii) V is an Artinian K-module.

Proof. (i) $\implies$ (ii), (i) $\implies$ (iii). Assume (i). Let

$$V_1 \subseteq V_2 \subseteq V_3 \subseteq$$

be an ascending chain of K-submodules of V, i.e., K-subspaces of V. Then

$$\dim_K V_1 \leq \dim_K V_2 \leq \dim_K V_3 \leq \cdots .$$

Since $\dim_K V$ is finite, there exists $n \in \mathbb{N}$ such that $\dim V_{n+k} = \dim V_n$ for $k \in \mathbb{N}$. This implies that $V_{n+k} = V_n$ for $k \in \mathbb{N}$. Next, assume that

$$\cdots \subseteq V_3 \subseteq V_2 \subseteq V_1$$

is a descending chain of K-submodules of V, i.e., K-subspaces of V. Then

$$\cdots \leq \dim_K V_3 \leq \dim_K V_2 \leq \dim_K V_1.$$

This implies that there exists $n \in \mathbb{N}$ such that $\dim_K V_{n+k} = \dim V_n$ for $k \in \mathbb{N}$. Therefore, $V_{n+k} = V_n$ for $k \in \mathbb{N}$.

(ii) $\implies$ (i). Assume that (ii) holds, and that V is not finite-dimensional; we will obtain a contradiction. Since V is infinite dimensional, there exist a collection of vectors $(v_i)_{i\in\mathbb{Z}}$ in V that are linearly independent. For $k \in \mathbb{N}$, let V_k be the K-span of $v_1, \ldots, v_k$. Then

$$V_1 \subsetneqq V_2 \subsetneqq V_3 \subsetneqq \cdots .$$

This contradicts (ii).
(iii) $\implies$ (i). Assume that (iii) holds, and that V is not finite-dimensional; we will obtain a contradiction. Since V is infinite dimensional, there exist a collection of vectors $(v_i)_{i\in\mathbb{Z}}$ in V that are linearly independent. For $k \in \mathbb{N}$, let W_k be the span of $v_{k+1}, v_{k+2}, v_{k+3}, \ldots$. We then have

$$\cdots \subsetneqq W_3 \subsetneqq W_2 \subsetneqq W_1.$$

This contradicts (iii). □

Theorem 96. *Let R be a commutative ring, and let N be an R-module. Let $M_1, \ldots, M_n$ be maximal ideals of R such that*

$$M_1 \cdots M_n N = 0.$$

Then N is Noetherian if and only if N is Artinian.

Proof. We will prove this theorem by induction on n. Assume that $n = 1$ so that $M_1 N = 0$. Then $M_1 \subseteq \mathrm{Ann}(N)$. We then may consider N as an R/M_1 module via the action

$$(r + M_1) \cdot n = rn$$

for $r \in R/M_1$ and $n \in N$. We note that R/M_1 is a field since M_1 is a maximal ideal of R; also, any R-subspace of N is also an R/M_1 subspace, and vice-versa. Hence:

$$\begin{aligned} N \text{ is Noetherian} &\iff N \text{ satisfies the ACC for } R\text{-submodules} \\ &\iff N \text{ satisfies the ACC for } R/M_1\text{-subspaces} \\ &\iff N \text{ satisfies the DCC for } R/M_1\text{-subspaces} \\ &\iff N \text{ satisfies the DCC for } R\text{-submodules} \\ &\iff N \text{ is Artinian.} \end{aligned}$$

For the third " $\iff$ " we used Lemma 95. This proves the $n = 1$ case. Now assume that the theorem holds for all m with $m < n$; we will prove that it holds for n. Now $M_n N$ is an R-submodule of N. By Lemma 92

$$N \text{ is Noetherian (Artinian)} \iff M_n N,\ N/M_n N \text{ are Noetherian (Artinian).}$$

We also have

$$\begin{aligned}(M_1 \cdots M_{n-1}) \cdot M_n N &= 0 \\ M_n(N/M_n N) &= 0.\end{aligned}$$

By the induction hypothesis we therefore have

$$M_n N,\ N/M_n N \text{ are Noetherian} \iff M_n N,\ N/M_n N \text{ are Artinian.}$$

Combining together implications, we obtain

$$N \text{ is Noetherian} \iff N \text{ is Artinian.}$$

This completes the proof. □

With the above preparation we begin the consideration of composition series. Let R be a commutative ring, and let M be an R-module. We say that M is ***simple*** if $M \neq 0$ and the only submodules of M are 0 and M.

Lemma 97. *Let R be a commutative ring, and let N be an R-module. Then N is simple if and only if N is isomorphic to R/M for some maximal ideal M of R.*

Proof. Assume that N is simple. Let $x \in N$ with $x \neq 0$. Define $f : R \to N$ by $f(r) = rx$ for $r \in R$. It is straightforward to check that f is an R-homomorphism. We have $f(R) = Rx$, which is an R-submodule of N. Since N is simple and $Rx \neq 0$, we must have $Rx = N$. Thus, f is surjective. Let $M = \ker(f)$. Then M is an R-submodule of R, i.e., an ideal of R. Also, by the First Isomorphism Theorem, $R/M \cong N$ as an R-module. Assume that I is an ideal of R such that $M \subseteq I$. Then $I/M \subseteq R/M$, and $f(I/M)$ is an R-submodule of R of N. We must have $f(I/M) = 0$ or $f(I/M) = N$. If $f(I/M) = 0$, then $I = M$; if $f(I/M) = N$, then $I/M = R/M$ so that $I = R$. Thus, M is maximal.
Now assume that N is isomorphic to R/M for some maximal ideal M of R. Let $f : R/M \to N$ be such an isomorphism. Let N' be a submodule of N. Let $J = f^{-1}(N')$. Then J is a submodule of R/M, i.e., and ideal of R/M. By Theorem 11, $J = I/M$ for some ideal I of R that contains M. Since M is maximal we have $I = M$ or $I = R$. This means that $J = 0$ or $J = R/M$, so that $N' = 0$ or $N' = N$. Hence, N is simple. □

Let R be a commutative ring. Let M be a non-zero R-module. A ***strict-chain*** of submodules of M is a chain of submodules of M of the form

$$0 = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_{n-1} \subsetneqq M_n = M$$

where $n \in \mathbb{N}$. We define the ***length*** of this strict-chain to be n. Such a strict-chain is said to be a ***composition series*** for M if M_i/M_{i-1} is simple for $i = 1, \ldots, n$. Assume that the above chain is

a composition series. Then there exists no $i \in \{1, \ldots, n\}$ and submodule M' of M such that

$$M_{i-1} \subsetneqq M' \subsetneqq M_i.$$

This is because M_i/M_{i-1} is simple, and hence contains no submodules other than 0 and M_i/M_{i-1}. If M has a composition series, then we let

$$\ell(M) = \text{minimum of all lengths of all composition series.}$$

If M does not admit a composition series, then we set $\ell(M) = \infty$.

Lemma 98. *Let R be a commutative ring, let M be an R-module, and let N be a proper non-zero submodule of M. If M admits a composition series, then so does N, and $\ell(N) < \ell(M)$.*

Proof. Let $n = \ell(M)$. Let

$$0 = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_{n-1} \subsetneqq M_n = M$$

be a composition series for M. For $i = 0, \ldots, n$, define $N_i = N \cap M_i$. We then have

$$0 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_{n-1} \subseteq N_n = N.$$

Now let $i \in \{1, \ldots, n\}$. Consider the composition

$$N_i = N \cap M_i \longrightarrow M_i \longrightarrow M_i/M_{i-1}.$$

This is an R-homomorphism. The kernel of this map is

$$N \cap M_i \cap M_{i-1} = N \cap M_{i-1} = N_{i-1}.$$

Thus, there is a monomorphism

$$N_i/N_{i-1} \hookrightarrow M_i/M_{i-1}.$$

Since M_i/M_{i-1} is simple, N_i/N_{i-1} is either 0 or $N_i/N_{i-1} \neq 0$ and N_i/N_{i-1} is simple. It follows that we may obtain a composition series for N from

$$0 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_{n-1} \subseteq N_n = N.$$

by deleting N_{i-1} if $N_{i-1} = N_i$. This implies that $\ell(N) \leq \ell(M)$. Assume that $\ell(N) = \ell(M)$; we will obtain a contradiction. Since $\ell(N) = \ell(M)$, we must have

$$0 = N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_{n-1} \subsetneqq N_n = N.$$

Let $i \in \{1, \ldots, n\}$. Since M_i/M_{i-1} is simple, since $N_i/N_{i-1} \neq 0$, and since $N_i/N_{i-1} \hookrightarrow M_i/M_{i-1}$

is injective, the map $N_i/N_{i-1} \hookrightarrow M_i/M_{i-1}$ is an isomorphism. Taking $i = 0$, we obtain $N_1/N_0 = N_1/0 = N_1$ and $M_1/M_0 = M_1/0 = M_1$; since $N_1/N_0 \xrightarrow{\sim} M_1/M_0$, this implies that $N_1 = M_1$. Next, since $N_2/N_1 = N_2/M_1 \xrightarrow{\sim} M_2/M_1$, we must have $N_2 = M_2$. Continuing, we find that $N = N_n = M_n = M$, contradicting that N is proper in M. □

Lemma 99. *Let R be a commutative ring, and let M be an R-module. Assume that M has a composition series of length n. Then:*

(i) No strict-chain of submodules of M can have length greater than n.

(ii) Every composition series of M has length n.

(iii) Every strict-chain of submodules of M of length n is a composition series of M.

(iv) Every strict-chain of submodules of M of length $n' \leq n$ can be extended to a composition series for M by insertion of $n - n'$ modules.

Proof. (i). Let

$$0 = M_0' \subsetneqq M_1' \subsetneqq \cdots \subsetneqq M_{r-1}' \subsetneqq M_r' = M$$

be a strict-chain. By Lemma 98 we have

$$0 < \ell(M_1') < \cdots < \ell(M_{r-1}') < \ell(M_r') = \ell(M).$$

From this we obtain $r \leq \ell(M)$. Since $\ell(M) \leq n$, we get $r \leq n$.
(ii). Let

$$0 = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_{n-1} \subsetneqq M_n = M,$$
$$0 = M_0' \subsetneqq M_1' \subsetneqq \cdots \subsetneqq M_{n'-1}' \subsetneqq M_n' = M$$

be two composition series for M. By (i) we have $n' \leq n$; also, we have $n \leq n'$. Hence, $n = n'$.
(iii). Let

$$0 = M_0' \subsetneqq M_1' \subsetneqq \cdots \subsetneqq M_{n-1}' \subsetneqq M_n' = M$$

be a strict-chain of length n. We claim that this is a composition series. Suppose not; we will obtain a contradiction. Since this is not a composition series, there exists $i \in \{1, \ldots, n\}$ such that M_i'/M_{i-1}' is not simple. This implies that there exist that submodule M' of M_i' such that $M_{i-1}' \subsetneqq M' \subsetneqq M_i'$. Then the following is a strict-chain:

$$0 = M_0' \subsetneqq \cdots \subsetneqq M_{i-1}' \subsetneqq M' \subsetneqq M_i' \subsetneqq \cdots \subsetneqq M_n' = M.$$

This strict-chain has length $n + 1$ which contradicts (i).
(iv). Let

$$0 = M_0' \subsetneqq M_1' \subsetneqq \cdots \subsetneqq M_{n'-1}' \subsetneqq M_{n'}' = M$$

be a strict-chain of length n'. If $n' = n$, then this strict-chain is a composition series by (iii). Assume that $n' < n$. Then by (ii) this strict-chain cannot be a composition series. Therefore,

for some $i \in \{1, \ldots, n\}$ the module M_i'/M_{i-1}' is not simple. Arguing as for (iii), we may insert a submodule in this strict-chain and obtain a strict-chain of length $n'+1$. If $n'+1 = n$, then by (iii) the new strict-chain is a composition series. If $n'+1 < n$, then we can repeat this procedure. Continuing, we may insert $n - n'$ submodules in our strict-chain to obtain a composition series for M. This completes the proof. □

Let R be a commutative ring, and let M be an R-module. If M admits a composition series, then we say that M has ***finite length***; in this case we let $\ell(M)$ be the common length of all composition series for M. If M does not admit a composition series, then we let $\ell(M) = \infty$.

Theorem 100. *Let R be a commutative ring, and let M be a non-zero R-module. Then M has finite length if and only if M is both Noetherian and Artinian, i.e., satisfies the ACC and the DCC.*

Proof. Assume that M has finite length. Let

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

be an ascending chain of R-submodules of M. Assume that this chain is not eventually stationary; we will obtain a contradiction. Since the chain is not eventually stationary this chain has infinitely many strict inclusions. This means that M admits a strict-chain of length greater than $\ell(M)$. This contradicts (i) of Lemma 99. Hence, M satisfies the ACC. Similarly, M satisfies the DCC. Hence, M is Noetherian and Artinian.
Now assume that M is Noetherian and Artinian. Assume that M does not have finite length; we will obtain a contradiction. Let

$$X = \{\text{submodules } N \text{ of } M \text{ such that } N \neq 0 \text{ and } \ell(N) = \infty\}.$$

The set X is non-empty since $M \in X$. Since M is Artinian, X contains a minimal element N. Next, let

$$Y = \{\text{non-zero proper submodules } Q \text{ of } N\}.$$

Since $\ell(N) = \infty$, the module N contains a non-zero proper submodule (otherwise, N is simple, and $0 = N_0 \subsetneqq N_1 = N$ is a composition series for N) so that Y is non-empty. Since M is Noetherian, Y contains a maximal element Q. We now have

$$0 \subseteq Q \subsetneqq N \subseteq M.$$

By the minimality of N, we have $\ell(Q) < \infty$. Let

$$0 = Q_0 \subsetneqq Q_1 \subsetneqq \cdots \subsetneqq Q_n = Q$$

be a composition series for Q. Consider N/Q. By the maximality of Q, N/Q must be simple. It

follows that

$$0 = Q_0 \subsetneqq Q_1 \subsetneqq \cdots \subsetneqq Q_n = Q \subsetneqq N$$

is a composition series for N. This contradicts $\ell(N) = \infty$. □

Let R be a commutative ring, and let M be an R-module. Assume that $M \neq 0$, and assume that M has a composition series:

$$0 = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_{n-1} \subsetneqq M_n = M.$$

By definition, the modules

$$M_i/M_{i-1}, \qquad i \in \{1, \ldots, n\}$$

are simple. We refer the M_i/M_{i-1} as the ***composition factors*** of the above composition series. If two composition series for M have the same composition factors, not taking order into account, then we will say that these composition series are ***isomorphic***. We will prove that any two composition series for M are isomorphic. First we need a lemma.

Lemma 101. *Let R be a commutative ring, and let M be an R-module. Let N and N' be submodules of M such that $N \neq N'$ and M/N and M/N' are simple. Then*

$$N'/(N \cap N' \cong M/N, \quad \textit{and} \quad N/(N \cap N') \cong M/N'.$$

Proof. Define $f : N' \to M/N$ by $f(n') = n' + N$ for $n' \in N'$. Then f is an R-homomorphism and $\ker(f) = N \cap N'$. Consider $\mathrm{im}(f)$. Since M/N is simple we have $\mathrm{im}(f) = 0$ or $\mathrm{im}(f) = M/N$. Assume that $\mathrm{im}(f) = 0$; we will obtain a contradiction. Since $\mathrm{im}(f) = 0$ we have $\ker(f) = N'$, i.e., $N \cap N' = N'$. This implies that $N' \subseteq N$. Since $N' \subseteq N$ and $N \neq N'$ we have $N' \subsetneqq N$. Therefore, $N/N' \neq 0$. Now $N/N' \subseteq M/N'$. Since $N/N' \neq 0$ and M/N is simple we must have $N/N' = M/N'$. This implies that $N = M$. Then $M/N = 0$, a contradiction (recall that M/N is simple and hence non-zero). It follows that $\mathrm{im}(f) = M/N$. By the First Isomorphism Theorem we now have $N'/(N \cap N') \cong M/N$. Similarly, $N/(N \cap N') \cong M/N'$. □

Theorem 102 (Jordan-Hölder Theorem)**.** *Let R be a commutative ring, and let M be a non-zero R-module. Then any two composition series of M are isomorphic, i.e., have the same composition factors (not taking order into account).*

Proof. We will prove this by induction on $n = \ell(M)$. If $n = 1$, then M is simple. Hence, the only composition series of M is $0 = M_0 \subsetneqq M_1 = M$, and the only composition factor for M is $M/0 = M$. Thus, the theorem holds for the $n = 1$ case. Suppose that $n > 1$ and that the theorem holds for all R-modules with composition series with length strictly less than n; we will prove that it holds for M.

Assume that

$$(C_1) \qquad 0 = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_{n-1} \subsetneqq M_n = M,$$

$$(C_2) \qquad 0 = M_0' \subsetneqq M_1' \subsetneqq \cdots \subsetneqq M_{n-1}' \subsetneqq M_n' = M$$

are two composition series for M.
Assume first that $M_{n-1} = M_{n-1}'$. Then:

comp. factors of C_1: comp. factors of $0 = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_{n-1}$ and $M/M_{n-1} = M/M_{n-1}'$,
comp. factors of C_1: comp. factors of $0 = M_0' \subsetneqq M_1' \subsetneqq \cdots \subsetneqq M_{n-1}$ and $M/M_{n-1} = M/M_{n-1}'$.

By the induction hypothesis, these are the same.
Assume now that $M_{n-1} \neq M_{n-1}'$. Since M/M_{n-1} and M/M_{n-1}' are simple we have by Lemma 101 we have

$$M_{n-1}/(M_{n-1} \cap M_{n-1}') \cong M/M_{n-1}', \qquad M_{n-1}'/(M_{n-1}' \cap M_{n-1}) \cong M/M_{n-1}.$$

Assume that $M_{n-1} \cap M_{n-1}' = 0$. Then

$$M_{n-1} = M_{n-1}/(M_{n-1} \cap M_{n-1}') \cong M/M_{n-1}',$$
$$M_{n-1}' = M_{n-1}'/(M_{n-1}' \cap M_{n-1}) \cong M/M_{n-1}.$$

In particular, M_{n-1} and M_{n-1}' are simple. This implies that $n = 2$, so that C_1 and C_2 are

$$(C_1) \qquad 0 = M_0 \subsetneqq M_1 \subsetneqq M_2 = M,$$
$$(C_2) \qquad 0 = M_0' \subsetneqq M_1' \subsetneqq M_2' = M$$

and we have

$$M_1 \cong M/M_1', \qquad M_1' \cong M/M_1.$$

This proves the theorem for this case. Finally, assume that $M_{n-1} \cap M_{n-1}' \neq 0$. Let $N = M_{n-1} \cap M_{n-1}'$. Consider N. By Lemma 98 we have $\ell(N) < \ell(M) = n$. Let $m = \ell(N)$ and let

$$0 = N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_{m-1} \subsetneqq N_m = N$$

be a composition series for N. Then

$$0 = N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_{m-1} \subsetneqq N_m = N \subsetneqq M_{n-1} \subsetneqq M_n = M$$

is a composition series for M. Hence, by Lemma 99 we have

$$m + 2 = \ell(M) = n$$

so that $m = n - 2$. It follows that

$$(C_3) \qquad 0 = N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_{m-1} \subsetneqq N_{n-2} = N \subsetneqq M_{n-1} \subsetneqq M_n = M,$$
$$(C_4) \qquad 0 = N_0 \subsetneqq N_1 \subsetneqq \cdots \subsetneqq N_{m-1} \subsetneqq N_{n-2} = N \subsetneqq M'_{n-1} \subsetneqq M'_n = M,$$

are two composition series for M. Since $M/M_{n-1} \cong M'_{n-1}/N$ and $M/M'_{n-1} \cong M_{n-1}/N$ we have

$$\text{comp factors of } (C_3) = \text{comp. factors of } (C_4).$$

By the first case we considered, we also have

$$\text{comp factors of } (C_1) = \text{comp. factors of } (C_3),$$
$$\text{comp factors of } (C_2) = \text{comp. factors of } (C_4).$$

We now conclude that

$$\text{comp factors of } (C_1) = \text{comp. factors of } (C_2),$$

which completes the proof. □

Theorem 103. *Let R be a commutative ring, and let*

$$0 \longrightarrow L \xrightarrow{f} M \xrightarrow{g} N \longrightarrow 0$$

be a short exact sequence of non-zero R-modules.

(i) M has a finite length if and only if L and N have finite length.

(ii) If L, M, and N have finite length, then

$$\ell(M) = \ell(L) + \ell(N).$$

Proof. (i). We have:

$$\begin{aligned} &M \text{ has finite length} \\ &\quad \iff M \text{ is Noetherian and Artinian} \\ &\quad \iff L \text{ and } M/L \text{ are Noetherian and Artinian (Lemma 92)} \\ &\quad \iff L \text{ and } N \text{ are Noetherian and Artinian } (N \cong M/L) \\ &\quad \iff L \text{ and } N \text{ have finite length.} \end{aligned}$$

(ii). Assume that L, M, and N have finite length. Since $N \cong M/L$ we have $\ell(N) = \ell(M/L)$. It

therefore suffices to prove that

$$\ell(M) = \ell(L) + \ell(M/L).$$

If $L = 0$ or $M/L = 0$ then we clearly have $\ell(M) = \ell(L) + \ell(M/L)$. Since $L \neq 0$ and $M/L \neq 0$

$$0 \subsetneqq L \subsetneqq M$$

is a strict-chain. By Lemma 99 we an extend this strict chain to a composition series for M:

$$0 = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_{t-1} \subsetneqq L = M_t \subsetneqq M_{t+1} \subsetneqq \cdots \subsetneqq M_n = M.$$

Now

$$0 = M_0 \subsetneqq M_1 \subsetneqq \cdots \subsetneqq M_{t-1} \subsetneqq L = M_t$$

is a composition series for L; hence,

$$\ell(L) = t.$$

We also have

$$0 = L/L \subsetneqq M_{t+1}/L \subsetneqq \cdots \subsetneqq M_n/L = M/L.$$

In this strict-chain each successive quotient is isomorphic to M_i/M_{i-1} for some $i \in \{t+1, \ldots, n\}$, and is hence simple. It follows that the above strict-chain is a composition series. Hence,

$$\ell(M/L) = n - t.$$

Adding, we obtain

$$\ell(L) + \ell(M/L) = t + (n - t) = n = \ell(M).$$

This completes the proof. □

We consider composition series for some examples. First we consider PIDs.

Lemma 104. *Let R be a PID that is not a field. Let M be an R-module. Then M has finite length if and only if M is finitely generated and there exists $r \in R$, $r \neq 0$, such that $rM = 0$.*

Proof. This is an assigned homework problem. □

Example. Let $R = \mathbb{Z}$. Let M be a finitely generated $\mathbb{Z}$-module. Then M has finite length if and only if M is finite.

Proof. Assume that M has finite length. Let M be generated by $m_1, \ldots, m_t$. By the example on page 74 there exists an epimorphism

$$\mathbb{Z}^t \xrightarrow{f} M.$$

Let $K = \ker(f)$. We have a short exact sequence

$$0 \longrightarrow K \longrightarrow \mathbb{Z}^t \longrightarrow M \longrightarrow 0$$

so that $M \cong \mathbb{Z}^t/K$. By Lemma 104 there exists $r \in \mathbb{N}$ such that $rM = 0$. This implies that $r\mathbb{Z}^t \subseteq \ker(f) = K$. Now

$$K/r\mathbb{Z}^t \subseteq \mathbb{Z}^t/r\mathbb{Z}^t.$$

Since $\mathbb{Z}^t/r\mathbb{Z}^t$ is finite, so is $K/r\mathbb{Z}^t$. Hence

$$M \cong \mathbb{Z}^t/K \cong (\mathbb{Z}^t/r\mathbb{Z}^t)/(K/r\mathbb{Z}^t)$$

is also finite.
Now suppose that M is finite. Since M is a finite abelian group we have $rM = 0$ where $r = \#M$. □

Example. Let $R = \mathbb{Z}$, and let $M = \mathbb{Z}/60\mathbb{Z}$. Determine a composition series for M.

Proof. We have

$$0 \underbrace{\subsetneq}_{\mathbb{Z}/2\mathbb{Z}} 30\mathbb{Z}/60\mathbb{Z} \underbrace{\subsetneq}_{\mathbb{Z}/2\mathbb{Z}} 15\mathbb{Z}/60\mathbb{Z} \underbrace{\subsetneq}_{\mathbb{Z}/5\mathbb{Z}} 3\mathbb{Z}/60\mathbb{Z} \underbrace{\subsetneq}_{\mathbb{Z}/3\mathbb{Z}} \mathbb{Z}/60\mathbb{Z}.$$

This is a composition series because each quotient is simple. The following is also a composition series:

$$0 \underbrace{\subsetneq}_{\mathbb{Z}/5\mathbb{Z}} 12\mathbb{Z}/60\mathbb{Z} \underbrace{\subsetneq}_{\mathbb{Z}/3\mathbb{Z}} 4\mathbb{Z}/60\mathbb{Z} \underbrace{\subsetneq}_{\mathbb{Z}/2\mathbb{Z}} 2\mathbb{Z}/60\mathbb{Z} \underbrace{\subsetneq}_{\mathbb{Z}/2\mathbb{Z}} \mathbb{Z}/60\mathbb{Z}.$$

Note that we get the same composition factors. □

In the previous example we used the following elementary lemma:

Lemma 105. *Let R be an integral domain. Let $r, s \in R$ with $r \neq 0$. Then*

$$R/(s) \cong (r)/(rs) = rR/rsR.$$

Proof. Define $f : R \to (r)/(rs)$ by $f(x) = rx + (rs)$ for $x \in R$. Then f is an R-homomorphism. Clearly, f is surjective. Assume $x \in R$ is such that $f(x) = 0$. Then $rx \in (rs)$. Hence, there exists $a \in R$ such that $rx = ars$. Since R is an integral domain and $r \neq 0$, $x = as$. Hence, $x \in (s)$. Clearly, $(s) \subseteq \ker(f)$. Hence, $R/(s) \cong (r)/(rs)$ by the First Isomorphism Theorem. □

Example. Let K be a field and let X be an indeterminate. Let $R = K[X]$. Then R is a PID and hence Noetherian. Let $p(X) = X^3 + X^2 - X - 1$. Let $I = (p(X))$ and set $M = R/I$. Show that the R-module M has finite length and determine a composition series for M.

Proof. The module M is clearly finitely generated. We have $p(X) \cdot M = 0$. Lemma 104 now implies that M has finite length. To find a composition series for M we first factor $p(X)$:

$$p(X) = X^3 + X^2 - X - 1 = (X + 1)^2(X - 1).$$

We then have:

$$0 \underbrace{\subsetneq}_{R/(X-1)\cong K} ((X+1)^2)/(p(X)) \underbrace{\subsetneq}_{R/(X+1)\cong K} (X+1)/(p(X)) \underbrace{\subsetneq}_{R/(X+1)\cong K} R/(p(X)).$$

For this, we repeatedly used Lemma 105. □

If R is a PID and I is a non-zero ideal of R, then similar reasoning proves that R/I has finite length, and calculates a composition series for R/I (factor I as a product of powers of prime ideals). What if R is not a PID?

Lemma 106. *Let R be a Noetherian ring and assume $R \neq 0$. Let N be an R-module. Then R has finite length if and only if N is finitely generated and there exist maximal ideals $M_1, \ldots, M_n$ of R such that*

$$M_1 \cdots M_n \cdot N = 0.$$

Proof. This is an assigned homework exercise. □

Example. Let K be a field and let X and Y be indeterminates. Let $R = K[X,Y]$; then R is Noetherian. Let $I = (X^2 - X, XY - X, XY - Y, Y^2 - Y)$ and $N = R/I$. Show that N has finite length and compute a composition series for N.

Proof. It is clear that N is finitely generated. We first note that if $M_1 = (X,Y)$ and $M_2 = (X-1, Y-1)$, then

$$I = M_1 M_2 = (X,Y)(X-1,Y-1).$$

The ideals M_1 and M_2 are maximal. We have $M_1 M_2 \cdot N = 0$. Hence, N has finite length. We have

$$0 \underbrace{\subsetneq}_{R/M_2\cong K} M_1/I \underbrace{\subsetneq}_{R/M_1\cong K} N = R/I.$$

We used that M_1 and M_2 are comaximal so that:

$$M_1/I = M_1/M_1M_2 \cong M_1/(M_1 \cap M_2) \cong (M_1 + M_2)/M_2 = R/M_2$$

This completes the argument. □

Example. Let K be a field and let X and Y be indeterminates. Let $R = K[X,Y]$; then R is Noetherian. Let $I = (X)$. Show that $N = R/I$ does not have finite length.

Proof. Assume that $N = R/I$ has finite length; we will obtain a contradiction. By Theorem 100 the R-module N must satisfy both the ACC and DCC. For $k \in \mathbb{N}$ define $N_k = R(Y^k + I)$. We then have

$$\cdots \subseteq N_3 \subseteq N_2 \subseteq N_1 \subseteq N_0 = N.$$

Since N satisfies the DCC there exists $k \in \mathbb{N}$ such that $N_{k+1} = N_k$, i.e., $R(Y^k + I) = R(Y^{k+1} + I)$. This implies that there exist $p(X,Y), q(X,Y) \in R$ such that

$$Y^k = p(X,Y)Y^{k+1} + q(X,Y)X.$$

Letting $X = 0$ in this equation we get

$$Y^k = p(0,Y)Y^{k+1}.$$

This is a contradiction. □

8 Noetherian rings

Let R be a commutative ring, and let X be an indeterminate. Our first goal is to prove the Hilbert Basis Theorem, which asserts that if R is Noetherian, then $R[X]$ is Noetherian. For the proof of this theorem we will follow some exposition of Emil Artin.

Let R be a commutative ring. To prove the Hilbert Basis Theorem we will need to relate ideals in $R[X]$ to ideals in R. We make the following definition. Let I be an ideal of $R[X]$, and let $n \in \mathbb{N}_0$. We let I_n be the subset of $r \in I$ such that there exists $p(X) \in I$ such that

$$p(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + r X^n$$

for some $a_0, \ldots, a_{n-1} \in R$.

Lemma 107. *Let R be a commutative ring, and let X be an indeterminate. Let I be an ideal of $R[X]$.*

(i) For $n \in \mathbb{N}_0$ the set I_n is an ideal of R.

(ii) For $n \in \mathbb{N}_0$, we have $I_n \subseteq I_{n+1}$.

Proof. (i) Let $n \in \mathbb{N}_0$. Let $r_1, r_2 \in I_n$, and let $r \in R$; to prove that I_n is an ideal of R it will suffice to prove that $r_1 + r r_2 \in I_n$. By definition, there exist polynomials $p_1(X), p_2(X) \in I$ with the form

$$p_1(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + r_1 X^n,$$
$$p_2(X) = b_0 + b_1 X + \cdots + b_{n-1} X^{n-1} + r_2 X^n.$$

We have

$$p_1(X) + r p_2(X) = (a_0 + r b_0) + (a_1 + r b_1) X + \cdots (a_{n-1} + r b_{n-1}) X^{n-1} + (r_1 + r r_2) X^n.$$

Since I is an ideal we have $p_1(X) + r p_2(X) \in I$. By the above expression for $p_1(X) + r p_2(X)$ and the definition of I_n we obtain $r_1 + r r_2 \in I_n$.

(ii) Let $n \in \mathbb{N}_0$. Let $r \in I_n$. Then there exists $p(X) \in I$ of the form

$$p(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1} + r X^n.$$

We have

$$p(X) X = a_0 X + a_1^2 + \cdots + a_{n-1} X^n + r X^{n+1}.$$

Using the definition of I_{n+1} we see that $r \in I_{n+1}$. □

Lemma 108. *Let R be a commutative ring, and let X be an indeterminate. Let I and J be ideals of $R[X]$ such that $I \subseteq J$.*

(i) For $n \in \mathbb{N}_0$ we have $I_n \subseteq J_n$.

(ii) If $I_n = J_n$ for all $n \in \mathbb{N}_0$ then $I = J$.

Proof. (i) This follows immediately from the definitions of I_n, J_n, and the assumption that $I \subseteq J$. (ii) Assume that $I_n = J_n$ for all $n \in \mathbb{N}_0$. We need to prove that $J \subseteq I$. For $n \in \mathbb{N}_0$, let

$$\mathrm{S}(n)\text{: If } f(X) \in J \text{ and } \deg(f(X)) = n, \text{ then } f(X) \in I.$$

To prove that $J \subseteq I$ it will suffice to prove that $\mathrm{S}(n)$ is true for all $n \in \mathbb{N}_0$; we will prove this by induction on n. Assume first that $n = 0$, and let $f(X) \in J$ with $\deg(f(X)) = 0$, so that $f(X) = b_0$ is a constant. Considering the definitions of I_0 and J_0, we see that

$$I_0 = \text{constant polynomials contained in } I,$$
$$J_0 = \text{constant polynomials contained in } J.$$

Since $f(X) = b_0 \in J$, we see from the second equality that $f(X) \in J_0$. By hypothesis, $I_0 = J_0$. Hence, $f(X) \in I_0$. By the first equality, $f(X) \in I$. This proves $\mathrm{S}(0)$. Now assume that $\mathrm{S}(n-1)$ holds for some $n \in \mathbb{N}$; we will prove that that $\mathrm{S}(n)$ holds. Let $f(X) \in J$ with $\deg(f(X)) = n$. Write

$$f(X) = b_0 + b_1 X + \cdots + b_n X^n.$$

Since $f(X) \in J$ we have $b_n \in J_n$. Since $I_n = J_n$, we have $b_n \in I_n$. Hence, there exists $g(X) \in I$ of the form

$$g(X) = a_0 + a_1 X + \cdots + b_n X^n.$$

Since $I \subseteq J$ we also have $g(X) \in J$. Now

$$f(X) - g(X) = (b_0 - a_0) + (b_1 - a_1)X + \cdots + (b_{n-1} - a_{n-1})X^{n-1}.$$

This polynomial is in J. Since $\mathrm{S}(n-1)$ holds we have $f(X) - g(X) \in I$. Since $g(X) \in I$, we get $f(X) = (f(X) - g(x)) + g(X) \in I$, proving $\mathrm{S}(n)$. □

Theorem 109 (Hilbert Basis Theorem)**.** *Let R be a Noetherian commutative ring, and let X be an indeterminate. Then $R[X]$ is Noetherian.*

Proof. Let

$$I(0) \subseteq I(1) \subseteq I(2) \subseteq \cdots$$

be an ascending chain of ideals in $R[X]$; we need to prove that this chain eventually becomes stationary. By Lemma 107 and Lemma 108 we have the following diagram of inclusions of ideals

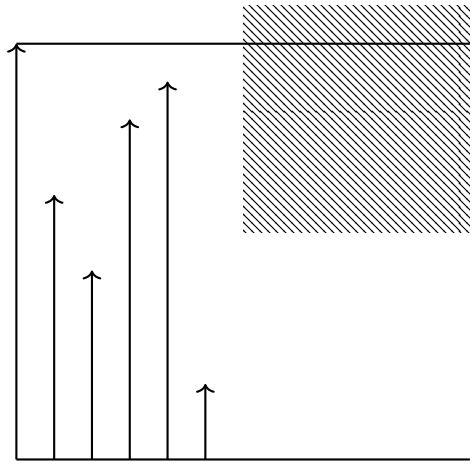
of R:

$$\begin{array}{ccccccccc}
\vdots & & \vdots & & \vdots & & \vdots & & \\
\cup & & \cup & & \cup & & \cup & & \\
I(3)_0 & \subseteq & I(3)_1 & \subseteq & I(3)_2 & \subseteq & I_3^{(3)} & \subseteq & \cdots \\
\cup & & \cup & & \cup & & \cup & & \\
I(2)_0 & \subseteq & I(2)_1 & \subseteq & I(2)_2 & \subseteq & I(2)_3 & \subseteq & \cdots \\
\cup & & \cup & & \cup & & \cup & & \\
I(1)_0 & \subseteq & I(1)_1 & \subseteq & I(1)_2 & \subseteq & I(1)_3 & \subseteq & \cdots \\
\cup & & \cup & & \cup & & \cup & & \\
I(0)_0 & \subseteq & I(0)_1 & \subseteq & I(0)_2 & \subseteq & I(0)_3 & \subseteq & \cdots
\end{array}$$

The ideals on the diagonal form an ascending chain:

$$I(0)_0 \subseteq I(1)_1 \subseteq I(2)_2 \subseteq \cdots .$$

Since R is Noetherian, this chain eventually becomes stationary. In terms of the diagram this implies that all the ideals in an infinite square region are equal:



To the left of this region there are finitely many ascending vertical chains of ideals. Each of these vertical chains eventually becomes stationary because R is Noetherian. It follows that there is a horizontal line above which each vertical chain becomes stationary. That is, there exists $N \in \mathbb{N}$ such that

$$\begin{array}{cccc}
\vdots & \vdots & \vdots & \\
= & = & = & \\
I(N+2)_0 & I(N+2)_1 & I(N+2)_2 & \cdots \\
= & = & = & \\
I^(N+1)_0 & I(N+1)_1 & I(N+1)_2 & \cdots \\
= & = & = & \\
I(N)_0 & I(N)_1 & I(N)_2 & \cdots
\end{array}$$

By (ii) of Lemma 108, from the bottom two rows we get

$$I(N) = I(N+1),$$

from the second and third from the bottom rows we get

$$I(N+1) = I(N+2),$$

and so on. In conclusion, we obtain

$$I(N) = I(N+1) = I(N+2) = \cdots .$$

This completes the proof. □

Corollary 110. *Let R be a Noetherian commutative ring. If $X_1, \ldots, X_n$ are indeterminates, then $R[X_1, \ldots, X_n]$ is Noetherian.*

Proof. By the Hilbert Basis Theorem the ring $R[X_1]$ is Noetherian. Since $(R[X_1])[X_2] \cong R[X_1, X_2]$, the Hilbert Basis Theorem again implies that $R[X_1, X_2]$ is Noetherian. Continuing, it follows that $R[X_1, \ldots, X_n]$ is Noetherian. □

One may similarly prove the following theorem (we omit the proof):

Theorem 111. *Let R be a Noetherian commutative ring, and let $X_1 \ldots, X_n$ be indeterminates. Then the ring $R[[X_1, \ldots, X_n]]$ is Noetherian.*

Let R be a Noetherian commutative ring. Let S be a multiplicatively closed subset of R. Earlier, in a homework exercise, we proved that $S^{-1}R$ is Noetherian. We also have the following result:

Proposition 112. *Let R be a Noetherian commutative ring. Let R' be a commutative ring, and let $f : R \to R'$ be a surjective ring homomorphism. Then R' is Noetherian.*

Proof. Let

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

be an ascending chain of ideals of R'. Then

$$f^{-1}(I_1) \subseteq f^{-1}(I_2) \subseteq f^{-1}(I_3) \subseteq \cdots$$

is an ascending chain of ideals of R. Since R is Noetherian, there exists $n \in \mathbb{N}$ such that $f^{-1}(I_{n+k}) = f^{-1}(I_n)$ for $k \in \mathbb{N}$. Let $k \in \mathbb{N}$. Since f is surjective, we have

$$I_{n+k} = f(f^{-1}(I_{n+k})) = f(f^{-1}(I_n)) = I_n.$$

It follows that R' is Noetherian. □

Corollary 113. *Let R be a Noetherian commutative ring, and let I be an ideal of R. Then R/I is a Noetherian ring.*

We now develop some ideas that will result in proofs of two important results about commutative rings: Nakayama's Lemma and Krull's Intersection Theorem.

Lemma 114. *Let R be a commutative ring, and let I be an ideal of R. Assume that $\sqrt{I}$ is finitely generated. Then there exists $n \in \mathbb{N}$ such that $(\sqrt{I})^n \subseteq I$.*

Proof. Let $a_1, \ldots, a_k \in \sqrt{I}$ be generators for $\sqrt{I}$. For $i \in \{1, \ldots, k\}$ let $n_i \in \mathbb{N}$ be such that $a_i^{n_i} \in I$. Define

$$n = 1 + \sum_{i=1}^{k} (n_i - 1).$$

To prove that $(\sqrt{I})^n \subset I$ it suffices to prove that if $r_1, \ldots, r_n \in \sqrt{I}$, then $r_1 \cdots r_n \in I$. Let $r_1, \ldots, r_n \in \sqrt{I}$. For $1 \leq i \leq n$ write

$$r_i = \sum_{j=1}^{k} s_{ij} a_j$$

for some $s_{ij} \in R$. Then

$$r_1 \cdots r_n = \sum_{\substack{e_1, \ldots, e_k \in \mathbb{N}_0 \\ e_1 + \cdots + e_k = n}} c_{e_1, \ldots, e_k} a_1^{e_1} \cdots a_k^{e_k}$$

where $c_{e_1}, \ldots, c_{e_k} \in R$. Consider a term $c_{e_1, \ldots, e_k} a_1^{e_1} \cdots a_k^{e_k}$ of this sum. We claim that for some i with $1 \leq i \leq k$ we have $e_i \geq n_i$. Suppose that $e_1 < n_1, \ldots, e_k < n_k$; we will obtain a contradiction. We have

$$n = e_1 + \cdots + e_k < n_1 - 1 + \cdots + n_k - 1 = n - k + 1 = n - 1.$$

This is a contradiction. It follows that for some i with $1 \leq i \leq k$ we have $e_i \geq n_i$. Hence,

$$c_{e_1, \ldots, e_k} a_1^{e_1} \cdots a_k^{e_k} = \left(c_{e_1, \ldots, e_k} \prod_{\substack{j=1 \\ j \neq i}}^{k} a_j^{e_j} \right) a_i^{n_i} \in I$$

since $a_i^{n_i} \in I$. It follows that $r_1 \cdots r_n \in I$, as desired. □

Let R be a commutative ring. We define the ***Jacobson radical*** of R to be

$$\mathrm{Jac}(R) = \bigcap_{M \text{ maximal ideal of } R} M.$$

Clearly, $\mathrm{Jac}(R)$ is an ideal of R.

Example. If K is a field, then K has only one maximal ideal, namely 0. Hence, $\mathrm{Jac}(K) = 0$.

Example. Assume R is quasi-local commutative ring. Then $\mathrm{Jac}(R) = M$, the unique maximal ideal of R.

Lemma 115. *Let R be a commutative ring, and let $r \in R$. Then $r \in \mathrm{Jac}(R)$ if and only if for every $a \in R$ the element $1 - ra$ is a unit of R.*

Proof. Assume that $r \in \mathrm{Jac}(R)$. Let $a \in R$, and assume that $1 - ra$ is not a unit; we will obtain a contradiction. Since $1 - ra$ is not a unit, there exists a maximal ideal M of R such that $1 - ra \in M$. Since $r \in \mathrm{Jac}(R)$, we obtain $ra \in M$. This implies that $1 = 1 - ra + ra \in M$, a contradiction.
Now assume that $1 - ra$ is a unit of R for all $a \in R$. Let M be a maximal ideal of R; we need to prove that $r \in M$. Assume that $r \notin M$; we will obtain a contradiction. Now $M + Rr$ is an ideal of R and we have

$$M \subsetneqq M + Rr \subseteq R.$$

Since M is maximal we must have $M + Rr = R$. Hence, there exists $b \in M$ and $a \in R$ such that $b + ar = 1$. Now $b = 1 - ar \in M$, and $1 - ar$ is a unit; this implies that $M = R$, a contradiction. □

Theorem 116. *Let R be a Noetherian commutative ring. Let I be an ideal of R, and define $J = \cap_{n=1}^{\infty} I^n$. Then $J = IJ$.*

Proof. If $I = R$, then this is clear. Assume that I is proper. Since $IJ \subseteq J$, it will suffice to prove that $J \subseteq IJ$. Now $IJ \subseteq J \subseteq I$. Hence, IJ is also proper. Since R is Noetherian, IJ has a primary decomposition (see Theorem 52). Let

$$IJ = Q_1 \cap \cdots \cap Q_n$$

be a primary decomposition of IJ. To prove that $J \subseteq IJ$ it will suffice to prove that $J \subset Q_i$ for $1 \leq i \leq n$. Suppose that for some i with $1 \leq i \leq n$ we have $J \not\subseteq Q_i$; we will obtain a contradiction. Since $J \not\subseteq Q_i$, there exists $a \in J$ such that $a \notin Q_i$. Now

$$aI \subset IJ = Q_1 \cap \cdots \cap Q_n \subseteq Q_i.$$

Let $b \in I$. Then $ab \in Q_i$; since Q_i is primary and since $a \notin Q_i$ we have $b \in \sqrt{Q_i}$. Hence, $I \subseteq \sqrt{Q_i}$. By Lemma 114, there exists $t \in \mathbb{N}$ such that $(\sqrt{Q_i})^t \subseteq Q_i$. We now have

$$J = \bigcap_{n=1}^{\infty} I^n \subseteq I^t \subseteq (\sqrt{Q_t})^t \subseteq Q_i.$$

This is a contradiction. □

Theorem 117 (Nakayama's Lemma)**.** *Let R be a commutative ring, and let M be a finitely generated R-module. Let I be an ideal of R such that $I \subseteq \mathrm{Jac}(R)$. If $M = IM$, then $M = 0$.*

Proof. Assume that $M = IM$, and that $M \neq 0$; we will obtain a contradiction. Let $m_1, \ldots, m_n$ be a minimal set of generators for M. Since $M \neq 0$, we must have $n \geq 1$. Now $m_1 \in M = IM$. Hence, there exist $a_1, \ldots, a_n \in I$ such that

$$m_1 = a_1 m_1 + \cdots + a_n m_n$$

$$(1-a_1)m_1 = a_2m_2 + \cdots + a_nm_n.$$

Since $I \subseteq \mathrm{Jac}(R)$ we have $a_1 \in \mathrm{Jac}(R)$. By Lemma 115, the element $1-a_1$ is a unit of R. Hence,

$$m_1 = (1-a_1)^{-1}a_2m_2 + \cdots + (1-a_1)^{-1}a_nm_n.$$

This implies that M is generated by $m_2, \ldots, m_n$, contradicting the minimality of $m_1, \ldots, m_n$. □

Theorem 118 (Krull's Intersection Theorem)**.** *Let R be a Noetherian commutative ring. Let I be an ideal of R such that $I \subseteq \mathrm{Jac}(R)$. Then*

$$\bigcap_{n=1}^{\infty} I^n = 0.$$

Proof. Let $J = \cap_{n=1}^{\infty} I^n$. By Theorem 115 we have $IJ = J$. Since R is Noetherian, J is a finitely generated ideal and hence a finitely generated R-module. We have $J = 0$ by Nakayama's Lemma, which completes the proof. □

Let R be a non-trivial Noetherian commutative ring. We say that R is ***local*** if R contains a unique maximal ideal. We say that R is ***semi-local*** if R has finitely many maximal ideals.

Corollary 119. *If R is a local ring, and M is the maximal ideal of R, then $\bigcap_{n=1}^{\infty} M^n = 0$.*

Proof. We have $\mathrm{Jac}(R) = M$. Since $M \subseteq \mathrm{Jac}(R)$, by Krull's Intersection Theorem (Theorem 118), we have $\bigcap_{n=1}^{\infty} M^n = 0$. □

We will now prove a series of results that will show that every Artinian commutative ring is Noetherian; we will also characterize Artinian rings among Noetherian rings.

Proposition 120. *Let R be a non-trivial Noetherian commutative ring. Assume that every prime ideal of R is maximal. Then*

(i) R is semi-local.

(ii) R is Artinian.

Proof. (i). Since R is non-trivial, 0 is a proper ideal of R. By Theorem 52, since R is Noetherian, 0 has a primary decomposition. Since every minimal prime ideal of 0 is contained in $\mathrm{ass}_R(0)$, and since $\mathrm{ass}_R(0)$ is finite, it follows that there are finitely many minimal prime ideals of 0. To prove that R is semi-local it will now suffice to prove that every maximal ideal of R is a minimal prime ideal of R. Let M be a maximal ideal of R. Let P be a prime ideal of R such that $0 \subseteq P \subseteq M$. By hypothesis, P is also maximal; since $P \subseteq M \subsetneqq R$, we must have $P = M$. Thus, M is a minimal prime ideal of 0, as desired.

(ii). By (i), R has finitely many maximal ideals $M_1, \ldots, M_n$. Now

$$\sqrt{0} = \bigcap_{\substack{P \text{ prime ideal} \\ \text{of } R}} P \qquad \text{(by Lemma 28)}$$

$$= \bigcap_{\substack{M \text{ maximal ideal} \\ \text{of } R}} M \qquad \text{(maximal ideals = prime ideals by hypothesis)}$$
$$= M_1 \cap \cdots \cap M_n.$$

Also, by Lemma 114, there exists $t \in \mathbb{N}$ such that $(\sqrt{0})^t = 0$. Hence,

$$\begin{aligned} M_1^t \cdots M_n^t &= (M_1 \cdots M_n)^t \\ &\subseteq (M_1 \cap \cdots \cap M_n)^t \\ &= (\sqrt{0})^t \\ &= 0. \end{aligned}$$

This trivially implies that $M_1^t \cdots M_n^t R = 0$. Since R is Noetherian as an R-module (we are assuming that R is a Noetherian commutative ring), we conclude by Theorem 96 that R is an Artinian R-module. This means that R is an Artinian ring. □

Proposition 121. *Let R be an Artinian commutative ring. Then every prime ideal of R is maximal.*

Proof. Let P be a prime ideal of R. Let $R' = R/P$. Since P is a prime ideal of R, R' is an integral domain. Also, since R is Artinian, so is R' (see Lemma 92). By Exercise 7.8, R' is a field (note that the hypothesis that R is a PID is unnecessary). Since R' is a field, P is maximal. □

Lemma 122. *Let R be an Artinian commutative ring. Then R has finitely many maximal ideals.*

Proof. We may assume that R is non-trivial. Let X be the set of all ideals of R that are intersections of finitely many maximal ideals of R. Since R is Artinian, X contains a minimal element J. Since $J \in X$, there exist maximal ideals $M_1, \ldots, M_n$ of R such that

$$J = M_1 \cap \cdots \cap M_n.$$

We claim that $M_1, \ldots, M_n$ are the maximal ideals of R. Let M be a maximal ideal of R. Consider

$$I = M \cap M_1 \cap \cdots \cap M_n.$$

We have $I \in X$ and $I \subseteq J$. By the minimality of J we must have $I = J$, i.e.,

$$M_1 \cap \cdots \cap M_n = M \cap M_1 \cap \cdots \cap M_n.$$

This implies that

$$M_1 \cap \cdots \cap M_n \subseteq M.$$

Since M is a prime ideal of R, this implies that $M_i \subseteq M$ for some $i \in \{1, \ldots, n\}$ (see Lemma 31). Since $M_i \subseteq M \subsetneq R$, and since M_i is maximal, we obtain $M_i = M$. This completes the proof. □

Proposition 123. *Let R be an Artinian commutative ring. Let $N = \sqrt{0}$, the nilradical of R. Then there exists $t \in \mathbb{N}$ such that $N^t = 0$, i.e., $(\sqrt{0})^t = 0$.*

Proof. Consider the descending chain

$$\cdots \subseteq N^3 \subseteq N^2 \subseteq N.$$

Since R is Artinian, this chain becomes stationary. Let $t \in \mathbb{N}$ be such that $N^t = N^{t+n}$ for $n \in \mathbb{N}$. We claim that $N^t = 0$. Suppose that $N^t \neq 0$; we will obtain a contradiction. Let

$$Y = \{\text{ideals } I \text{ of } R \text{ such that } IN^t \neq 0\}.$$

We have $N^n \in Y$ for $n \in \mathbb{N}$. Hence, Y is non-empty. Since R is Artinian, Y contains a minimal element J. By definition, $JN^t \neq 00$. Hence, there exists $a \in J$ such that $aN^t \neq 0$. This implies that $(aR)N^t \neq 0$, so that $aR \in Y$. Since $aR \subseteq J$ and J is minimal, we must have $J = aR$. We also have

$$\begin{aligned}(aN^t)N^t &= aN^{2t} \\ &= aRN^{2t} \\ &= aRN^t \\ &= JN^t \\ &\neq 0.\end{aligned}$$

This implies that $aN^t \in Y$. Since $aN^t \subseteq aR = J$, the minimality of J implies that $J = aN^t$. Since $a \in J$, there exists $b \in N^t$ such that $a = ab$. Since $b \in N^t$ and $N^t \subseteq N$, by the definition of N there exists $m \in \mathbb{N}$ such that $b^m = 0$. Now

$$a = ab = abb = \cdots = ab^m = 0.$$

Hence, $JN^t = aRN^t = 0$, a contradiction. This completes the proof. □

Theorem 124. *Let R be an Artinian commutative ring. Then R is Noetherian.*

Proof. We may assume that R is non-trivial. By Proposition 121, every prime ideal of R is maximal, and by Lemma 122, R has only finitely many maximal ideals $M_1, \ldots, M_n$. It follows that:

$$\begin{aligned}\sqrt{0} &= \bigcap_{\substack{P \text{ prime ideal} \\ \text{of } R}} P \qquad \text{(by Lemma 28)} \\ &= \bigcap_{\substack{M \text{ maximal ideal} \\ \text{of } R}} M \qquad \text{(maximal ideals = prime ideals)} \\ &= M_1 \cap \cdots \cap M_n.\end{aligned}$$

Also, by Proposition 123, there exists $t \in \mathbb{N}$ such that $(\sqrt{0})^t = 0$. Hence,

$$\begin{aligned} M_1^t \cdots M_n^t &= (M_1 \cdots M_n)^t \\ &\subseteq (M_1 \cap \cdots \cap M_n)^t \\ &= (\sqrt{0})^t \\ &= 0. \end{aligned}$$

This trivially implies that $M_1^t \cdots M_n^t R = 0$. Since R is Artinian as an R-module (we are assuming that R is an Artinian commutative ring), we conclude by Theorem 96 that R is an Noetherian R-module. This means that R is a Noetherian ring. □

Corollary 125. *Let R be a commutative ring. Then R is Artinian if and only if R is Noetherian and every prime ideal of R is maximal.*

Proof. Assume that R is Artinian. Then R is Noetherian by Theorem 124, and every prime ideal of R is maximal by Proposition 121.
Assume that R is Noetherian and every prime ideal of R is maximal. Then R is Artinian by Proposition 120. □

9 Modules over PIDs

In this section we consider the structure of finitely generated modules over a PID. Our first goal is to prove the Elementary Divisors Theorem.

Lemma 126. *Let R be a non-trivial commutative ring, and let F be a non-zero free R-module with finite base $(e_i)_{i=1}^n$. If $y \in F$, write*

$$y = \sum_{i=1}^n r_i e_i$$

and let $C(y) = (r_1, \ldots, r_n) = \sum_{i=1}^n Rr_i$, the ideal in R generated by $r_1, \ldots, r_n$. Then the ideal $C(y)$ does not depend on the choice of base $(e_i)_{i=1}^n$ for F.

Proof. By Theorem 88 all bases for F have the same cardinality. Let $(e_i')_{i=1}^n$ be another base for F, and let $r_1', \ldots, r_n' \in R$ be such that

$$y = \sum_{i=1}^n r_i' e_i'.$$

We need to prove that $(r_1, \ldots, r_n) = (r_1', \ldots, r_n')$. Let $a_{ij}, b_{ij} \in R$, $1 \leq i, j \leq n$ be such that

$$e_i' = \sum_{j=1}^n a_{ij} e_j, \qquad e_i = \sum_{j=1}^n b_{ij} e_j'.$$

Now

$$\begin{aligned} y &= \sum_{i=1}^n r_i e_i \\ &= \sum_{i=1}^n r_i \left(\sum_{j=1}^n b_{ij} e_j' \right) \\ \sum_{j=1}^n r_j' e_j' &= \sum_{j=1}^n \left(\sum_{i=1}^n r_i b_{ij} \right) e_j'. \end{aligned}$$

This implies that

$$r_j' = \sum_{i=1}^n r_i b_{ij}, \qquad 1 \leq j \leq n.$$

Hence,

$$(r_1', \ldots, r_n') \subseteq (r_1, \ldots, r_n).$$

Similarly,

$$(r_1, \ldots, r_n) \subseteq (r_1', \ldots, r_n').$$

It follows that $(r_1', \ldots, r_n') = (r_1, \ldots, r_n)$, as desired. □

Lemma 127. *Let R be a PID, and let F be a non-zero free R-module with finite base. Let $y \in F$, and let $c_y \in R$ be a generator for the ideal $C(y)$, so that $C(y) = (c_y)$. Then there exists a base $(e_i')_{i=1}^n$ for F such that $y = c_y e_1'$.*

Proof. We will prove the lemma by induction on n. Assume first that $n = 1$. If $y = 0$, then the assertion of the lemma is trivially true. Assume that $y \neq 0$. Let e_1 be a base for F so that $F = Re_1$. Let $r \in R$ be such that $y = re_1$. Then $r \neq 0$ because $y \neq 0$. By the definition of $C(y)$ we have $C(y) = (r)$. Since we also have $C(y) = (c_y)$, and since R is an integral domain, there exists a unit u of R such that $c_y = ur$. Now

$$y = re_1 = ur(u^{-1}e_1) = c_y(u^{-1}e_1).$$

Set $e_1' = u^{-1}e_1$. Then e_1' is a base for F, and $y = c_y e_1'$, which completes the proof of the lemma in the case $n = 1$.

Now suppose that $n > 1$ and the lemma holds for $n - 1$. Again, the assertion of the lemma is trivially true if $y = 0$; assume that $y = 0$. Let $(e_i)_{i=1}^n$ be a base for F. Write

$$y = r_1 e_1 + \cdots + r_n e_n$$

for some $r_1, \ldots, r_n \in R$. By definition, we have

$$C(y) = (r_1, \ldots, r_n) = (c_y).$$

Define

$$F' = Re_2 + \cdots + Re_n,$$
$$z = r_2 e_2 + \cdots + re_n.$$

Then F' is a free R-module of rank $n - 1$ and we have

$$y = r_1 e_1 + z.$$

We apply the induction hypothesis to F' and z. By this, there exists a base $(e_i'')_{i=2}^n$ for F' such that

$$z = c_z e_2''$$

where

$$(c_z) = (r_2, \ldots, r_n).$$

Now

$$(c_y) = (r_1, \ldots, r_n) = (r_1) + (r_2, \ldots, r_n) = (r_1) + (c_z).$$

It follows that there exist $s, t \in R$ such that

$$r_1 = sc_y, \qquad c_z = tc_y.$$

Also, there exist $u, v \in R$ such that

$$c_y = ur_1 + vc_z.$$

Substituting, we obtain:

$$\begin{aligned} c_y &= ur_1 + vc_z \\ &= usc_y + vtc_y \\ c_y &= (us + vt)c_y. \end{aligned}$$

Since $c_y \neq 0$ and R is an integral domain we conclude that

$$1 = us + vt.$$

We now define

$$\begin{aligned} e_1' &= se_1 + te_2'', \\ e_2' &= ve_1 - ue_2'', \\ e_i' &= e_i'', \qquad \text{for } 3 \leq i \leq n. \end{aligned}$$

Then

$$\begin{aligned} c_y e_1' &= c_y(se_1 + te_2'') \\ &= c_y se_1 + c_y te_2'' \\ &= r_1 e_1 + c_z e_2'' \\ &= r_1 e_1 + z \\ &= y. \end{aligned}$$

To complete the proof we need to prove that $(e_i'')_{i=1}^n$ is a base for F. Now

$$\begin{aligned} F &= Re_1 + Re_2 + \cdots + Re_n \\ &= Re_1 + Re_2'' + \cdots + Re_n'' \\ &= Re_1 + Re_2'' + Re_3'' + \cdots + Re_n'' \\ &= Re_1 + Re_2'' + Re_3' + \cdots + Re_n'. \end{aligned}$$

We consider $Re_1 + Re_2''$. Now

$$\begin{aligned} ue_1' + te_2' &= u(se_1 + te_2'') + t(ve_1 - ue_2'') \\ &= use_1 + ute_2'' + tve_1 - tue_2'' \\ &= (us + tv)e_1 \\ &= e_1. \end{aligned}$$

And

$$\begin{aligned} ve_1' - se_2' &= v(se_1 + te_2'') - s(ve_1 - ue_2'') \\ &= vse_1 + vte_2'' - sve_1 + sue_2'' \\ &= (vt + su)e_2'' \\ &= e_2''. \end{aligned}$$

This implies that

$$Re_1 + Re_2'' \subseteq Re_1' + Re_2'.$$

Also, from the definition of e_1' and e_2' we have

$$Re_1' + Re_2' \subseteq Re_1 + Re_2''.$$

Hence,

$$Re_1 + Re_2'' = Re_1' + Re_2'.$$

It follows that

$$F = Re_1' + Re_2' + Re_3' + \cdots + Re_n'.$$

Finally, assume that $r_1', \ldots, r_n' \in R$ are such that

$$r_1'e_1' + \cdots + r_n'e_n' = 0.$$

Then substituting, we obtain:

$$\begin{aligned} 0 &= r_1'e_1' + r_2'e_2' + r_3'e_3' + \cdots + r_n'e_n' \\ &= r_1'(se_1 + te_2'') + r_2'(ve_1 - ue_2'') + r_3'e_3' + \cdots + r_n'e_n' \\ &= (r_1's + r_2'v)e_1 + (r_1't - r_2'u)e_2'' + r_3'e_i'' + \cdots + r_n'e_n''. \end{aligned}$$

Since $e_1, e_2'', e_3'', \ldots, e_n''$ are base for F we must have

$$\begin{aligned} 0 &= r_1's + r_2'v, \\ 0 &= r_1't - r_2'u, \end{aligned}$$

$$0 = r_i', \qquad \text{for } 3 \leq i \leq n.$$

The first two equations can be rewritten in matrix form as:

$$\begin{bmatrix} s & v \\ t & -u \end{bmatrix} \begin{bmatrix} r_1' \\ r_2' \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Since

$$\det\left(\begin{bmatrix} s & v \\ t & -u \end{bmatrix}\right) = -(su + vt) = -1,$$

which is a unit in R, this 2×2 matrix is invertible. This implies that $r_1' = r_2' = 0$. This completes the proof that $(e_1')_{i=1}^n$ is a base for F. □

Lemma 128. *Let R be a PID, and let F be a free R-module with a finite base. Let H be a submodule of F. Let $z \in H$ be such that the ideal $C(z)$ is a maximal element of $\{C(y) : y \in H\}$ (recall that R is Noetherian). Then $C(y) \subseteq C(z)$ for all $y \in H$.*

Proof. Let $y \in H$; we need to prove that $C(y) \subseteq C(z)$. Let $c_z \in R$ be such that $C(z) = Rc_z$. By Lemma 127 there exists a base $(e_i')_{i=1}^n$ for F such that $z = c_z e_1'$. Also, let $r_1, \ldots, r_n \in R$ be such that

$$y = r_1 e_1' + \cdots + r_n e_n'.$$

Now

$$C(y) = (r_1, \ldots, r_n) = (r_1) + \cdots + (r_n).$$

To prove that $C(y) \subseteq C(z)$ it will suffice to prove that $(r_1), \ldots, (r_n) \subseteq C(z)$. We first prove that $(r_1) \subseteq C(z)$. Consider

$$(c_z) + (r_1) = C(z) + (r_1).$$

This ideal is principal; let $t \in R$ be such that

$$(c_z) + (r_1) = (t).$$

Let $u, v \in R$ be such that

$$t = uc_z + vr_1.$$

Then

$$\begin{aligned} uz + vy &= uc_z e_1' + v(r_1 e_1' + \cdots + r_n e_n') \\ &= (uc_z + vr_1)e_1' + vr_2 e_2' + \cdots + vr_n e_n' \\ &= te_1' + vr_2 e_2' + \cdots + vr_n e_n'. \end{aligned}$$

Hence,

$$\begin{aligned} C(uz+vy) &= (t, vr_2, \ldots, vr_n) \\ &\supseteq (t) \\ &= (c_z) + (r_1) \\ &\supseteq (c_z) \\ &= C(z). \end{aligned}$$

By the maximality of $C(z)$ we have $C(uz+vy) = C(z)$ so that all of these inclusions are equalities. Hence,

$$C(z) = (c_z) = (t) = (c_z) + (r_1).$$

This implies that

$$(r_1) \subseteq C(z).$$

Finally, we prove that $(r_2), \ldots, (r_n) \subseteq C(z)$. Let $w \in R$ be such that $r_1 = wc_z$. We have

$$\begin{aligned} (1-w)z + y &= (1-w)c_z e_1' + r_1 e_1' + \cdots + r_n e_n' \\ &= (c_z - wc_z + wc_z)e_1' + r_2 e_2' + \cdots + r_n e_n' \\ &= c_z e_1' + r_2 e_2' + \cdots + r_n e_n'. \end{aligned}$$

Hence,

$$\begin{aligned} C((1-w)z+y) &= (c_z, r_2, \ldots, r_n) \\ &\supseteq (c_z) \\ &= C(z). \end{aligned}$$

By the maximality of $C(z)$, $C((1-2)z+y) = C(z)$, so that the inclusion is an equality:

$$C(z) = (c_z, r_2, \ldots, r_n).$$

This implies that

$$(r_2), \ldots, (r_n) \subseteq C(z),$$

as desired. □

Theorem 129 (Elementary Divisors Theorem)**.** *Let R be a PID, and let F a a non-zero free R-module with a finite base and rank n. Let H be an R-submodule of F. Then there exists a base $(e_i)_{i=1}^n$ for F and elements $a_1, \ldots, a_n \in R$ such that*

$$(a_n) \subseteq (a_{n-1}) \subseteq \cdots \subseteq (a_1)$$

and H is generated by $a_1e_1, \ldots, a_ne_n$.

Proof. We will prove this theorem by induction on n. Assume first that $n = 1$. Let e_1 be a base for F. Consider

$$I = \{r \in R : re_1 \in H\}.$$

Then I is an ideal of R. Since R is a PID, we have $I = (a_1)$ for some $a_1 \in R$. Evidently, $a_1e_1 \in H$. We claim that a_1e_1 generates H. Let $y \in H$. Then for some $r_1 \in R$, we have $y = r_1e_1$. By the definition of I, $r_1 \in I$. Let $t \in R$ be such that $r_1 = ta_1$. Then

$$y = r_1e_1 = t(a_1e_1).$$

Thus, a_1e_1 generates H.
Now assume that the theorem holds for the case of free R-modules of rank $n-1$; we will prove that it holds for free R-modules of rank n. By Lemma 128, there exists $z \in H$ such that

$$C(y) \subseteq C(z) \tag{3}$$

for all $y \in H$. Let $c_z \in R$ be such that $C(z) = (c_z)$. By Lemma 127 there exists a base $(e'_1)_{i=1}^n$ for F such that

$$z = c_ze'_1.$$

Now define

$$F' = Re'_2 + \cdots + Re'_n,$$
$$H' = H \cap F'.$$

Then F' is a free R-module of rank $n-1$, and H' is an R-submodule of F'. By the induction hypothesis, there exists a base $(e_i)_{i=2}^n$ for F' and $a_2, \ldots, a_n \in R$ such that

$$(a_n) \subseteq (a_{n-1}) \subseteq \cdots \subseteq (a_3) \subseteq (a_2)$$

and H' is generated by $a_2e_2, \ldots, a_ne_n$. We also define

$$e_1 = e'_1,$$
$$a_1 = c_z,$$

and we claim that $a_1, \ldots, a_n$ and $(e_i)_{i=1}^n$ have the required properties. To prove that

$$(a_n) \subseteq (a_{n-1}) \subseteq \cdots \subseteq (a_2) \subseteq (a_1)$$

it will suffice to prove that $(a_2) \subseteq (a_1)$. Now

$$\begin{aligned}(a_1) &= (c_z) \\ &= C(z) \\ &\supseteq C(a_2 e_2) \qquad (\text{ by (3)}) \\ &= (a_2) \qquad (\text{by the definition of } C(a_2 e_2)).\end{aligned}$$

Next we prove that $(e_1)_{i=1}^n$ is a base for F. We have

$$\begin{aligned}F &= Re_1' + \cdots + Re_n' \\ &= Re_1' + Re_2' + \cdots + Re_n' \\ &= Re_1' + F' \\ &= Re_1 + Re_2 + \cdots + Re_n.\end{aligned}$$

Thus, $(e_i)_{i=1}^n$ generates F. Assume that $r_1, \ldots, r_n \in R$ are such that

$$0 = r_1 e_1 + \cdots + r_n e_n.$$

Since

$$r_2 e_2 + \cdots + r_n e_n \in F'$$

there exist $r_2', \ldots, r_n' \in R$ such that

$$r_2 e_2 + \cdots + r_n e_n = r_2' e_2' + \cdots + r_n' e_n'.$$

Hence,

$$\begin{aligned}0 &= r_1 e_1 + \cdots + r_n e_n \\ &= r_1 e_1 + r_2' e_2' \cdots + r_n' e_n' \\ &= r_1 e_1' + r_2' e_2' \cdots + r_n' e_n'.\end{aligned}$$

Since $(e_i')_{i=1}^n$ is a base for F, we have

$$r_1 = r_2' = \cdots = r_n' = 0.$$

This implies that

$$r_2 e_2 + \cdots + r_n e_n = 0.$$

Since $(e_i)_{i=2}^n$ is a base for F', $r_2 = \cdots = r_n = 0$. This completes the argument that $(e_i)_{i=1}^n$ is a base for F.

Finally, we prove that H is generated by $a_1e_1, \ldots, a_ne_n$. We first note that

$$a_1e_1 = c_ze_1' = z \in H,$$

and that $a_2e_2, \ldots, a_ne_n \in H' \subseteq H$. Next, let $y \in H$. Let $s_1, \ldots, s_n \in R$ be such that

$$y = s_1e_1 + \cdots + s_ne_n.$$

Then

$$\begin{aligned}(s_1) &\subseteq (s_1, \ldots, s_n) \\ &= C(y) \\ &\subseteq C(z) \\ &= (c_z).\end{aligned}$$

Hence, there exists $t \in R$ such that $s_1 = tc_z$. Now

$$\begin{aligned}y - ta_1e_1 &= s_1e_1 + \cdots + s_ne_n - ta_1e_1 \\ &= (s_1 - ta_1)e_1 + s_2e_2 + \cdots + s_ne_n \\ &= s_2e_2 + \cdots + s_ne_n \\ &\in F' \cap H = H'.\end{aligned}$$

Since H' is generated by $a_2e_2, \ldots, a_ne_n$, we obtain

$$s_2e_2 + \cdots + s_ne_n \in Ra_2e_2 + \cdots Ra_ne_n.$$

We conclude that

$$y \in Ra_1e_1 + Ra_2e_2 + \cdots + Ra_ne_n,$$

so that $a_1e_1, \ldots, a_ne_n$ generate H. □

Corollary 130. *Let R be a PID, and let F be a non-zero free R-module with a finite base. If H is a submodule of F, then H is free, and* $\operatorname{rank}(H) \leq \operatorname{rank}(F)$.

Proof. By Theorem 129, there exists a base $(e_i)_{i=1}^n$ for F and $a_1, \ldots, a_n \in R$ such that

$$(a_n) \subseteq (a_{n-1}) \subseteq \cdots \subseteq (a_1)$$

and H is generated by $a_1e_1, \ldots, a_ne_n$. We note that if $1 \leq j \leq n$ is such that $a_j = 0$, then $a_n = a_{n-1} = \cdots = a_j = 0$. If there exists a $1 \leq j \leq n$ such that $a_j = 0$, then let t be the smallest such that j; if no such j exists let $t = n + 1$. We have $a_i \neq 0$ for $1 \leq i \leq t - 1$. If $t = 1$, then $a_1 = \cdots = a_n = 0$, and $H = 0$ so that there is nothing to prove. Assume that $t > 1$. To complete

the proof it will suffice to prove that $(a_i e_i)_{i=1}^{t-1}$ is a base for H. Assume that $r_1, \ldots, r_{t-1}$ are such that

$$\sum_{i=1}^{t-1} r_i a_i e_i = 0.$$

Since $(e_i)_{i=1}^n$ is a base for F we have $r_1 a_1 = \cdots = r_{t-1} a_{t-1} = 0$. Also, since $a_1 \neq 0, \ldots, a_{t-1} \neq 0$, we get $r_1 = \cdots = r_{t-1} = 0$. Finally, since $\{a_1 e_1, \cdots, a_{t-1} e_{t-1}\} = \{a_1 e_1, \ldots, a_n e_n\}$ generates H, we conclude that $(a_i e_i)_{i=1}^{t-1}$ is a base for H. □

Lemma 131. *Let R be a commutative ring, and let $M_1, \ldots, M_n$ be R-modules. For $1 \leq i \leq n$, let N_i be a submodule of M_i. Then the map*

$$f : M_1 \oplus \cdots \oplus M_n \longrightarrow M_1/N_1 \oplus \cdots \oplus M_n/N_n$$

defined by

$$f(m_1, \ldots, m_n) = (m_1 + N_1, \ldots, m_n + N_n)$$

for $(m_1, \ldots, m_n) \in M_1 \oplus \cdots \oplus M_n$ is a surjective homomorphism with kernel $N_1 \oplus \cdots \oplus N_n$, so that

$$(M_1 \oplus \cdots \oplus M_n)/(N_1 \oplus \cdots \oplus N_n) \cong M_1/N_1 \oplus \cdots \oplus M_n/N_n.$$

Proof. We leave the proof to the reader. □

Theorem 132 (Structure theorem for finitely generated modules over a PID)**.** *Let R be a PID, and let M be a non-zero finitely generated R-module. There exist $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in R$ such that*

$$(a_n) \subseteq (a_{n-1}) \subseteq \cdots \subseteq (a_1) \subsetneqq R$$

and

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_n).$$

Moreover, if $m \in \mathbb{N}$ and $b_1, \ldots, b_m \in R$ are such that

$$(b_m) \subseteq (b_{m-1}) \subseteq \cdots \subseteq (b_1) \subsetneqq R$$

and

$$M \cong R/(b_1) \oplus \cdots \oplus R/(b_m),$$

then $m = n$ and $(a_i) = (b_i)$ for $1 \leq i \leq n$.

Proof. Let M be generated by $m_1, \ldots, m_n$. Let F be the free R-module on the n symbols $(e_i')_{i=1}^n$. Define $f : F \to M$ by

$$f(\sum_{i=1}^n r_i e_i) = \sum_{i=1}^n r_i m_i$$

for $r_1, \ldots, r_n \in R$. Then f is surjective R-homomorphism. Let $H = \ker(f)$. By the first isomorphism theorem,

$$F/H \cong M$$

as R-modules. By the Elementary Divisors Theorem, Theorem 129, there exist a base $(e_i)_{i=1}^n$ for F and $a_1, \ldots, a_n \in R$ such that

$$(a_n) \subseteq (a_{n-1}) \subseteq \cdots \subseteq (a_1)$$

and H is spanned by $(a_i e_i)_{i=1}^n$. Now

$$F \cong Re_1 \oplus \cdots \oplus Re_n,$$
$$H \cong Ra_1e_1 \oplus \cdots \oplus Ra_ne_n.$$

By Lemma 131, we obtain

$$F/H \cong Re_1/Ra_1e_1 \oplus \cdots \oplus Re_n/Ra_ne_n.$$

Let $i \in \{1, \ldots, n\}$. Define

$$g : R \longrightarrow Re_i/Ra_ie_i$$

by

$$g(r) = re_i + Ra_ie_i$$

for $r \in R$. Then g is a surjective R-homomorphism. Moreover, $\ker(g) = (a_i)$, so that

$$R/(a_i) \cong Re_i/Ra_ie_i$$

as R-modules. We conclude that

$$F/H \cong R/(a_1) \oplus \cdots \oplus R/(a_n).$$

Now if $(a_1) \subsetneqq R$, then we have proven the first assertion of the theorem. Assume $R = (a_1)$. Let r be the largest integer such that $1 \leq r \leq n$ and $(a_r) = R$. Then $r \leq n-1$; otherwise, $M = 0$, a contradiction. The elements $a_{t+1}, \ldots, a_n$ then satisfy the first assertion. Finally, we omit the proof of the uniqueness assertion. □

Let R be a Euclidean integral domain, let $m, n \in \mathbb{N}$, and let $M \in \mathrm{M}_{m\times n}(R)$ so that M is an $m \times n$ matrix with entries from R. The following are called ***elementary row operations*** on M:

(i) interchanging two rows of M;
(ii) multiplying a row of M by a unit in R;
(iii) for $r \in R$ and $1 \leq i, j \leq n$ with $i \neq j$, adding r times the j-th row to the i-th row.

Elementary column operations are similarly defined.

Theorem 133 (Smith normal form)**.** *Let R be an Euclidean integral domain, let $m, n \in \mathbb{N}$, and let $M \in \mathrm{M}_{m\times n}(R)$ be non-zero. Then there exist a sequence of elementary row and column operations on M such that M can be brought into the form*

$$\begin{bmatrix} L_r & 0 \\ 0 & 0 \end{bmatrix}$$

where L_r is an $r \times r$ diagonal matrix

$$L = \begin{bmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{bmatrix}$$

such that $d_1, \ldots, d_r \in R$ are non-zero and $d_1 \mid d_2 \mid \cdots \mid d_r$. The ideals $(d_1), \ldots, (d_r)$ are uniquely determined by M.

Proof. We omit the proof. □

Example. Let $R = \mathbb{Z}$, let F be a free $\mathbb{Z}$-module of rank 3 with base $(v_i)_{i=1}^3$, and let H be the submodule of F generated by the elements

$$r_1 = 3v_1 + 9v_2 + 9v_3, \qquad r_2 = 9v_1 - 3v_2 + 9v_3.$$

Determine the structure of the finitely generated $\mathbb{Z}$ module F/H.

Proof. To solve this problem we need to find a basis $(e_i)_{i=1}^3$ as in the Elementary Divisors Theorem, Theorem 129. To do this we represent the data as the matrix

$$M = \begin{bmatrix} 3 & 9 & 9 \\ 9 & -3 & 9 \end{bmatrix}$$

and the perform elementary row and column operations on M until we arrive at a Smith normal form. Elementary row operations correspond to changing the generators for H; elementary column operations correspond to changing the base for F. After each operation the data still represents F/H. We have

$$\begin{bmatrix} 3 & 9 & 9 \\ 9 & -3 & 9 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 0 & 9 \\ 9 & -30 & 9 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 0 & 0 \\ 9 & -30 & -18 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 0 & 0 \\ 0 & -30 & -18 \end{bmatrix} \longrightarrow$$
$$\begin{bmatrix} 3 & 0 & 0 \\ 0 & 18 & 30 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 0 & 0 \\ 0 & 18 & 12 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 0 & 0 \\ 0 & 6 & 12 \end{bmatrix} \longrightarrow \begin{bmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \end{bmatrix}.$$

We conclude that F has a base $(e_i)_{i=1}^3$ such that H is generated by $3e_1, 6e_2$. Therefore,

$$F/H \cong (\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z})/(3\mathbb{Z} \oplus 6\mathbb{Z} \oplus 0\mathbb{Z}) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}.$$

This solves the problem. □

Example. Let $R = \mathbb{Q}[X]$, and let F be a free R-module of rank 3 with base $(v_i)_{i=1}^3$, and let H be the submodule of F generated by

$$(X+1)v_1 + (X^2-1)v_2 + Xv_3, \qquad (X+2)v_1 + Xv_2 + X^2v_3.$$

Determine the structure of the finitely generated $\mathbb{Q}[X]$ module F/H.

Proof. We proceed as in the previous example, using elementary row and column operations:

$$\begin{bmatrix} X+1 & X^2-1 & X \\ X+2 & X & X^2 \end{bmatrix} = \begin{bmatrix} X+1 & (X-1)(X+1) & X \\ X+2 & X & X^2 \end{bmatrix} \longrightarrow$$
$$\begin{bmatrix} X+1 & 0 & X \\ X+2 & X-(X-1)(X+2) & X^2 \end{bmatrix} = \begin{bmatrix} X+1 & 0 & X \\ X+2 & 2-X^2 & X^2 \end{bmatrix} \longrightarrow$$
$$\begin{bmatrix} X+1 & 0 & -1 \\ X+2 & 2-X^2 & X^2-(X+2) \end{bmatrix} = \begin{bmatrix} X+1 & 0 & -1 \\ X+2 & 2-X^2 & X^2-X-2 \end{bmatrix} \longrightarrow$$
$$\begin{bmatrix} 0 & 0 & -1 \\ X+2+(X+1)(X^2-X-2) & 2-X^2 & X^2-X-2 \end{bmatrix} = \begin{bmatrix} 0 & 0 & -1 \\ X^3-2X & 2-X^2 & X^2-X-2 \end{bmatrix}$$
$$\longrightarrow \begin{bmatrix} 0 & 0 & 1 \\ -X(2-X^2) & 2-X^2 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 0 & 0 & 1 \\ 0 & 2-X^2 & 0 \end{bmatrix} \longrightarrow \begin{bmatrix} 1 & 0 & 0 \\ 0 & X^2-2 & 0 \end{bmatrix}.$$

We conclude that F has a basis $(e_i)_{i=1}^3$ such that H is generated by $e_1, (X^2-2)e_2$. Therefore,

$$\begin{aligned} F/H &\cong (\mathbb{Q}[X] \oplus \mathbb{Q}[X] \oplus \mathbb{Q}[X])/(1 \cdot \mathbb{Q}[X] \oplus (X^2-2) \cdot \mathbb{Q}[X] \oplus 0 \cdot \mathbb{Q}[X]) \\ &\cong \mathbb{Q}[X]/(1) \oplus \mathbb{Q}[X]/(X^2-2) \oplus \mathbb{Q}[X] \\ &\cong \mathbb{Q}[X]/(X^2-2) \oplus \mathbb{Q}[X]. \end{aligned}$$

This completes the calculation. □

Lemma 134. *Let R be an integral domain, and let M be an R-module. Define*

$$M_t = \{m \in M : \text{there exists } r \in R,\ r \neq 0, \text{ such that } rm = 0\}.$$

The M_t is a submodule of M called the **torsion submodule** *of M and we refer to the elements of M_t as* **torsion elements**.

Proof. Let $m_1, m_2 \in M_t$ and $s_1, s_2 \in R$; we need to prove that $s_1m_1 + s_2m_2 \in M_t$. Let $r_1, r_2 \in R$ be such that $r_1 \neq 0$, $r_2 \neq 0$, and $r_1m_1 = r_2m_2 = 0$. Then $r_1r_2 \neq 0$ because R is an integral domain, and:

$$r_1r_2(s_1m_1 + s_2m_2) = r_2s_1(r_1m_1) + r_1s_2(r_2m_2)$$

$$= r_2 s_1 \cdot 0 + r_1 s_2 \cdot 0$$
$$= 0.$$

This implies that $s_1 m_1 + s_2 m_2 \in M_t$. □

Proposition 135. *Let R be a PID, and let M be a non-zero finitely generated R-module. By Theorem 132 there exist $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in R$ such that*

$$(a_n) \subseteq (a_{n-1}0 \subseteq \cdots \subseteq (a_1) \subsetneqq R$$

and

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_n).$$

If $a_1 = \cdots = a_n = 0$, then $M_t = 0$ and M is a free R-module. If $a_i \neq 0$ for some $1 \leq i \leq n$, and m is the largest such i, then

$$M_t \cong R/(a_m) \oplus \cdots \oplus R/(a_1).$$

Proof. Assume first that $a_1 = \cdots = a_n = 0$. Then $M \cong R \oplus \cdots \oplus R$ is a free R-module and consequently $M_t = 0$. Assume that $a_i \neq 0$ for some $1 \leq i \leq n$ and let m be the largest such i. Then

$$M \cong M'$$

where

$$M' R/(a_1) \oplus \cdots \oplus R/(a_n) \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus \underbrace{R \oplus \cdots \oplus R}_{m-n}.$$

Evidently, the elements of the submodule

$$R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus \underbrace{0 \oplus \cdots \oplus 0}_{m-n}$$

are all torsion elements of M' because $a_1 \cdots a_m x = 0$ for any element x in this submodule. Conversely, if $x \in M'_t$, and

$$x = (r_1 + (a_1), \ldots, r_m + (a_m), r_{m+1}, \ldots, r_n)$$

then we must have $r_{m+1} = \cdots = r_n = 0$, so that x is in the above submodule of M'_t. It follows that

$$M'_t = R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus \underbrace{0 \oplus \cdots \oplus 0}_{m-n}$$

which completes the proof. □