MATH 420/820 - Commutative Algebra

Martin Frankland

March 11, 2024

Abstract

These are the evolving lecture notes for the course MATH 420/820 - Commutative Algebra in the Winter 2024 semester. We are following Atiyah and Macdonald as main reference. The notes provide more details and examples.

Contents

1 Ideals and quotient rings

1.1 Ring homomorphisms

Definition 1.1.1. Let R and S be rings. A **ring homomorphism** (or *ring map*) from R to S is a function $f\colon R \to S$ satisfying:

$$f(x+y) = f(x) + f(y)$$
$$f(xy) = f(x)f(y)$$

for all $x, y \in R$. The ring homomorphism f is **unital** if moreover it satisfies

$$f(1_R) = 1_S.$$

In this course, ring homomorphisms will be assumed unital unless otherwise noted.

Exercise 1.1.2. Given ring maps $f\colon R \to S$ and $g\colon S \to T$, check that the composition

$$g \circ f\colon R \to T$$

is also a ring map.

Example 1.1.3. Let R be any ring.

1. The identity map $\mathrm{id}\colon R \to R$ is a ring homomorphism.
2. There is a unique ring map $R \to 0$ to the zero ring 0, namely the constant map with value 0. This says that the zero ring 0 is the *terminal* ring.
3. There is a unique ring map $\mathbb{Z} \to R$, given by
$$n \mapsto n \cdot 1_R.$$
This says that $\mathbb{Z}$ is the *initial* (unital) ring.

Example 1.1.4. For any ring R, ring maps $\varphi\colon \mathbb{Z}[x] \to R$ correspond bijectively to elements of R, via evaluation at x:

$$\{\text{ring maps } \varphi\colon \mathbb{Z}[x] \to R\} \xrightarrow{\cong} R$$
$$\varphi \mapsto \varphi(x).$$

Given an element $a \in R$, the corresponding ring map

$$\varphi_a\colon \mathbb{Z}[x] \to R$$

is given by evaluating at $x = a$:

$$\varphi_a(p(x)) = p(a),$$

or more explicitly:

$$\varphi_a\left(\sum_{i=0}^{d} c_i x^i\right) = \sum_{i=0}^{d} c_i a^i.$$

This says that $\mathbb{Z}[x]$ is the *free* ring on one generator, as well as the free commutative ring on one generator.

Example 1.1.5. For a *commutative* ring R, ring maps $\varphi\colon \mathbb{Z}[x,y] \to R$ correspond bijectively to pairs of elements of R, via evaluation at x and y:

$$\begin{aligned}\{\text{ring maps } \varphi\colon \mathbb{Z}[x,y] \to R\} &\xrightarrow{\cong} R^2 \\ \varphi &\mapsto (\varphi(x), \varphi(y))\,.\end{aligned}$$

Given a pair of elements $(a,b) \in R^2$, the corresponding ring map

$$\varphi_{a,b}\colon \mathbb{Z}[x,y] \to R$$

is given by evaluating at $x = a$ and $y = b$:

$$\varphi_{a,b}(p(x,y)) = p(a,b).$$

This says that $\mathbb{Z}[x,y]$ is the free commutative ring on two generators.

Remark 1.1.6. For a not necessarily commutative ring R, ring maps $\varphi\colon \mathbb{Z}[x,y] \to R$ correspond bijectively to pairs of *commuting* elements of R, via evaluation at x and y.

The free ring on two generators is the ring of polynomials in two non-commuting variables $\mathbb{Z}\langle X, Y\rangle$.

Definition 1.1.7. A ring homomorphism $f\colon R \to S$ is an **isomorphism** if there exists a ring homomorphism $g\colon S \to R$ satisfying $g \circ f = \mathrm{id}_R$ and $f \circ g = \mathrm{id}_S$.

Proposition 1.1.8. *A ring homomorphism $f\colon R \to S$ is an isomorphism if and only if f is bijective.*

1.2 Subrings and ideals

Definition 1.2.1. A **subring** of a ring R is a subset $A \subseteq R$ satisfying:

- $0 \in A$
- $x, y \in A \implies x + y \in A$ and $-x \in A$
- $x, y \in A \implies xy \in A$.

The subring A is **unital** if moreover it satisfies $1_R \in A$.

As for rings, subrings will be assumed unital unless otherwise noted.

Remark 1.2.2. Given a subring $A \subseteq R$, the inclusion map $\mathrm{inc}\colon A \hookrightarrow R$ is a ring homomorphism.

Example 1.2.3.

1. The integers are a subring of the rational numbers: $\mathbb{Z} \subset \mathbb{Q}$.
2. The integers are also a subring of the Gaussian integers: $\mathbb{Z} \subset \mathbb{Z}[i]$.
3. The rational numbers are a subring of the real numbers: $\mathbb{Q} \subset \mathbb{R}$.
4. Given a commutative ring k, consider the polynomial ring $k[x]$. The subset of polynomials having only even degree terms
$$k[x^2] = \left\{ \sum_{i=0}^{n} c_{2i} x^{2i} \mid n \geq 0, c_{2i} \in k \right\}$$
is a subring of $k[x]$.
5. The polynomials form a subring of the power series: $k[x] \subset k[\![x]\!]$.
6. The polynomials also form a subring of the Laurent polynomials: $k[x] \subset k[x, x^{-1}]$.

Definition 1.2.4. Let R be a commutative ring. An **ideal** of R is a subset $I \subseteq R$ satisfying:

- $0 \in I$
- $x, y \in I \implies x + y \in I$
- $r \in R$ and $x \in I \implies rx \in I$.

Example 1.2.5.

1. Given an integer $n \in Z$, the multiples of n form an ideal $n\mathbb{Z} \subseteq \mathbb{Z}$, also denoted $(n) = n\mathbb{Z}$.
2. The polynomials that are multiples of x (i.e. those with constant term zero) form an ideal of the polynomial ring $k[x]$:
$$x\,k[x] = \left\{ \sum_{i=1}^{d} c_i x^i \mid d \geq 0, c_i \in k \right\}$$
also denoted $(x) = x\,k[x]$.

3. More generally, given a commutative ring R and an element $a \in R$, the ideal generated by a consists of all multiples of a:

$$(a) = Ra = \{ra \mid r \in R\} \subseteq R.$$

An ideal of the form (a) is called a **principal ideal**.

4. Yet more generally, the ideal generated by elements $a_1, \ldots, a_n \in R$ consists of all R-linear combinations of the a_i:

$$(a_1, \ldots, a_n) = Ra_1 + \cdots + Ra_n = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R \right\} \subseteq R.$$

It is the smallest ideal of R containing $a_1, \ldots, a_n$.

Remark 1.2.6. If an ideal $I \subseteq R$ contains an invertible element u, we have

$$\begin{aligned} u \in I &\implies u^{-1}u = 1 \in I \\ &\implies r \cdot 1 \in I \quad \text{for all } r \in R \\ &\implies I = R. \end{aligned}$$

Hence a proper ideal $I \subsetneq R$ cannot be a unital subring of R, though it is a non-unital subring.

Definition 1.2.7. A **principal ideal domain** (PID for short) is an integral domain in which every ideal is principal.

Example 1.2.8. 1. The integers $\mathbb{Z}$ form a PID. Any non-zero ideal $I \subseteq \mathbb{Z}$ is generated by the greatest common divisor of its non-zero elements. For instance:

$$\begin{aligned} (a, b) &= (\gcd(a, b)) \\ (6, 10) &= (2) \\ (10, 15) &= (5) \\ (10, 13) &= (1) = \mathbb{Z}. \end{aligned}$$

2. For any field k, the polynomial ring $k[x]$ is a PID. For instance:

$$\begin{aligned} (x^2 - 1, x^2 - x) &= (x - 1) \subset k[x] \\ (x^2 - 1, x + 2) &= (1) = k[x]. \end{aligned}$$

3. The polynomial ring $k[x, y]$ is **not** a PID, since the ideal $(x, y) \subset k[x, y]$ is not principal.

4. The polynomial ring $\mathbb{Z}[x]$ is **not** a PID, since the ideal $(7, x) \subset \mathbb{Z}[x]$ is not principal.

1.3 Quotient rings

Definition 1.3.1. Given a commutative ring R and an ideal $I \subseteq R$, the **quotient ring** R/I is the set of cosets of I

$$R/I = \{r + I \mid r \in R\}.$$

We also denote the equivalence class of r by $r + I = [r] = \overline{r} = q(r)$. Addition and multiplication in R/I are induced by those in R via the formulas

$$[a] + [b] = [a + b]$$
$$[a][b] = [ab],$$

which are well-defined, i.e., independent of the choices of representatives in R.

If the ring R was unital to begin with, then so is the quotient ring R/I, with unit element

$$1_{R/I} = [1_R].$$

Warning 1.3.2. We sometimes denote the equivalence class of $r \in R$ in a quotient ring R/I also by r rather than $\overline{r}$, $[r]$, or $r + I$, if the context makes clear that we are working in the quotient ring.

Remark 1.3.3. Given an ideal $I \subseteq R$, the quotient map $q\colon R \twoheadrightarrow R/I$ is a ring homomorphism.

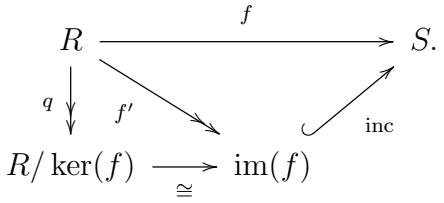
Lemma 1.3.4. *Let R be a commutative ring.*

1. *For any ring map $f\colon R \to S$, the kernel $\ker(f) \subseteq R$ is an ideal of R.*
2. *Every ideal $I \subseteq R$ arises as the kernel of some ring map.*

Proof. 1. Exercise.

2. The ideal $I \subseteq R$ is the kernel of the quotient map $q\colon R \twoheadrightarrow R/I$. □

Remark 1.3.5. Every ring map $f\colon R \to S$ factors as a quotient map followed by an inclusion:



Example 1.3.6. 1. The integers modulo n are the quotient ring

$$\mathbb{Z}/n \coloneqq \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/(n).$$

2. Given a commutative ring k, the quotient ring $k[x]/(x)$ is described by the isomorphism that evaluates polynomials at $x = 0$:

$$\begin{aligned} k[x]/(x) &\xrightarrow{\cong} k \\ [p(x)] &\mapsto p(0), \end{aligned}$$

in other words, extracting the constant term:

$$\left[\sum_{i=0}^{d} c_i x^i\right] \mapsto c_0.$$

3. More generally, for any $a \in k$, evaluation at $x = a$ yields an isomorphism of rings

$$\begin{aligned} k[x]/(x-a) &\xrightarrow{\cong} k \\ [p(x)] &\mapsto p(a). \end{aligned}$$

4. For any $b \in k$, evaluation at $y = b$ yields an isomorphism of rings

$$\begin{aligned} k[x,y]/(y-b) &\xrightarrow{\cong} k[x] \\ [p(x,y)] &\mapsto p(x,b). \end{aligned}$$

5. The quotient ring

$$k[\epsilon] \coloneqq k[x]/(x^2) \cong \{a + b\epsilon \mid a, b \in k,\ \epsilon^2 = 0\}$$

is called the ring of **dual numbers**. Here ϵ denotes the equivalence class $[x]$ of x in the quotient ring $k[x]/(x^2)$.

Lemma 1.3.7. *Let $f\colon R \to S$ be a ring map.*

1. *For any ideal $J \subseteq S$, the preimage $f^{-1}(J) \subseteq R$ is an ideal of R.*
2. *For any ideal $I \subseteq R$, the image $f(I) \subseteq S$ is a non-unital subring of S.*
3. *If f is surjective, then for any ideal $I \subseteq R$, the image $f(I) \subseteq S$ is an ideal of S.*

Remark 1.3.8. The image $f(I) \subseteq S$ need **not** be an ideal in general. Consider for instance the image of the inclusion map $\mathrm{inc}\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$, which is not an ideal of $\mathbb{Q}$. More generally, any (proper unital) subring $A \subsetneq R$ is not an ideal of R, as observed in Remark 1.2.6.

Exercise 1.3.9. (a) Let $f\colon R \to S$ be a non-surjective ring map. Show that there is an ideal $I \subseteq R$ whose image $f(I)$ is not an ideal of S.

(b) Find an example of non-surjective ring map $f\colon R \to S$ such that for every *proper* ideal $I \subsetneq R$, the image $f(I)$ is an ideal of S.

Proposition 1.3.10. *Let R be a commutative ring and $I \subseteq R$ an ideal. The ideals of R/I correspond bijectively to the ideals of R containing I, via the correspondence:*

$$\{\textit{ideals of } R/I\} \xrightarrow{\cong} \{\textit{ideals of } R \textit{ containing } I\}$$

$$J \subseteq R/I \longmapsto q^{-1}(J)$$

$$q(I') \longmapsfrom I' \subseteq R.$$

Here $q\colon R \twoheadrightarrow R/I$ denotes the quotient map.

2 Zero-divisors, nilpotent elements, units

2.1 Zero-divisors

Definition 2.1.1. Let R be a commutative ring. An element $x \in R$ is a **zero-divisor** if there exists $y \neq 0$ in R satisfying $xy = 0$.

Technically 0 is considered a zero-divisor, though we will often be interested in nontrivial zero-divisors $x \neq 0$.

Example 2.1.2. In the ring $\mathbb{Z}/6$, the elements 2 and 3 are zero-divisors since they satisfy $2 \cdot 3 = 0$, but $2 \neq 0$ and $3 \neq 0$.

Definition 2.1.3. An **integral domain** is a commutative ring with $1 \neq 0$ and containing no nontrivial zero-divisors.

Having no nontrivial zero-divisors can be rephrased as the implication

$$xy = 0 \implies x = 0 \quad \text{or} \quad y = 0.$$

By contraposition, this is in turn equivalent to:

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

Example 2.1.4.

1. The ring $\mathbb{Z}$ is an integral domain.
2. The ring $\mathbb{Z}/5$ is in integral domain (in fact a field). The ring $\mathbb{Z}/6$ is not an integral domain. More generally, $\mathbb{Z}/n$ is an integral domain if and only if n is prime.

Proposition 2.1.5. *If R is an integral domain, then so is the polynomial ring $R[x]$.*

Proof. Let $p, q \in R[x]$ be non-zero polynomials of degrees m and n respectively, that is:

$$p = \sum_{i=0}^{m} a_i x^i \quad \text{and} \quad q = \sum_{j=0}^{n} b_j x^j$$

with $a_m \neq 0$ and $b_n \neq 0$. Their product is

$$pq = a_m b_n x^{m+n} + \text{lower degree terms}.$$

The leading coefficient satisfies $a_m b_n \neq 0$ since R is an integral domain, which ensures $pq \neq 0$. □

2.2 Nilpotent elements

Definition 2.2.1. Let R be a ring. An element $x \in R$ is **nilpotent** if $x^n = 0$ holds for some $n \geq 1$.

Lemma 2.2.2. *Any nilpotent element is a zero-divisor.*

Proof. Let $x \in R$ be nilpotent and let n be the smallest exponent such that $x^n = 0$ holds. Then we have

$$x(x^{n-1}) = x^n = 0$$

but $x^{n-1} \neq 0$. □

Note that the convention $x^0 = 1$ covers the case $x = 0$. Alternately, treat the case $x = 0$ separately by recalling that 0 is always a zero-divisor.

The converse of Lemma 2.2.2 does not hold, as we will see below.

Example 2.2.3.

1. In the ring $\mathbb{Z}/4$, the element 2 is nilpotent since it satisfies $2^2 = 4 = 0$.
2. In the ring $\mathbb{Z}/6$, the element 2 is **not** nilpotent, since its powers are all non-zero:
$$2^1 = 2 \neq 0$$
$$2^2 = 4 \neq 0$$
$$2^3 = 8 = 2.$$
3. For any (nontrivial) commutative ring k, consider the quotient ring $R = k[x, y]/(xy)$. In R, x and y are zero-divisors since they satisfy
$$xy = 0 \quad \text{but} \quad x \neq 0 \text{ and } y \neq 0.$$
However x and y are not nilpotent: $x^n \neq 0$ holds for all $n \geq 1$, and likewise for y.

Lemma 2.2.4. *Let R be a commutative ring and $a, b \in R$ nilpotent elements.*

1. *The sum $a + b$ is nilpotent.*
2. *The product ra is nilpotent for any $r \in R$.*

In other words, the nilpotent elements form an ideal of R.

Proof. 1. Assume $a^m = 0$ and $b^n = 0$. Since R is commutative, the binomial expansion yields

$$(a+b)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} a^i b^{m+n-1-i}.$$

The terms with $i \geq m$ have $a^i = 0$ and thus vanish. The terms with $i < m$ have

$$m + n - 1 - i \geq n \implies b^{m+n-1-i} = 0.$$

Hence the entire sum vanishes: $(a + b)^{m+n-1} = 0$.

2. Since R is commutative, we have $(ra)^n = r^n a^n = 0$. □

Remark 2.2.5. The statement does **not** hold for a non-commutative ring R. The proof does show the following.

1. If $a, b \in R$ are *commuting* nilpotent elements, then $a + b$ is nilpotent.
2. If a nilpotent element $a \in R$ *commutes* with $r \in R$, then ra is nilpotent.

Example 2.2.6. Let k be a commutative ring and consider the matrix ring $R = \mathrm{Mat}_2(k)$. Take the matrices

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix},$$

both of which are nilpotent: $A^2 = B^2 = 0$. Their sum is the invertible matrix

$$A + B = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

which in particular is not nilpotent. Their product is

$$AB = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix},$$

which is not nilpotent.

Example 2.2.7. Let k be a commutative ring and consider the ring of polynomials in two non-commuting variables $k\langle X, Y\rangle$. Consider the quotient

$$R = k\langle X, Y\rangle/(X^2, Y^2)$$

by the two-sided ideal generated by X^2 and Y^2. In R, the elements X and Y are both nilpotent: $X^2 = Y^2 = 0$. However, their sum $X + Y$ is not nilpotent. Their product XY is also not nilpotent.

Now back to commutative rings.

Definition 2.2.8. Let R be a commutative ring.

1. The ideal of nilpotent elements of R is called the **nilradical** of R, denoted
$$\mathrm{nil}(R) = \{a \in R \mid a^n = 0 \text{ for some } n \geq 1\}.$$
2. The ring R is **reduced** if it has no nontrivial nilpotents: $\mathrm{nil}(R) = 0$.

By Lemma 2.2.2, every integral domain is reduced, though the converse does not hold.

Example 2.2.9.
1. The ring $\mathbb{Z}/4$ has nilradical
$$\mathrm{nil}(\mathbb{Z}/4) = (2) = \{0, 2\}.$$
2. The ring $\mathbb{Z}/6$ has nilradical
$$\mathrm{nil}(\mathbb{Z}/6) = 0.$$
Hence $\mathbb{Z}/6$ is reduced, though it is not an integral domain.

Exercise 2.2.10. (a) Compute the nilradical $\mathrm{nil}(\mathbb{Z}/72)$.

(b) Recall that $\mathbb{Z}/n$ is an integral domain if and only if n is prime. When is $\mathbb{Z}/n$ reduced?

2.3 Units

Definition 2.3.1. Let R be a commutative ring.

1. An element $a \in R$ is a **unit** if it is invertible. Explicitly: there is an element $b \in R$ satisfying
$$ab = 1.$$
If such a b exists, it is unique, and called the **inverse** of a, denoted a^{-1}.

2. The set of all units in R is called the **group of units** (or *multiplicative group*) of R, denoted
$$R^\times = \{a \in R \mid a \text{ is invertible}\}.$$

Exercise 2.3.2. Show that an element $a \in R$ is a unit if and only if the ideal generated by a is the whole ring: $(a) = (1) = R$.

Let us justify that units form a group under multiplication.

Lemma 2.3.3. *Let R be a commutative ring.*

1. *If $a, b \in R$ are units, then so is their product ab.*
2. *If x is a non-unit, then so is rx for any $r \in R$.*

Proof. 1. The inverse of ab is $b^{-1}a^{-1}$:
$$ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1.$$

2. By contraposition, the statement is equivalent to saying that if a product ab is invertible, then both factors must be invertible. This holds, since the inverse of a is $b(ab)^{-1}$:
$$a\left(b(ab)^{-1}\right) = (ab)(ab)^{-1} = 1.$$ □

Example 2.3.4. 1. The only invertible integers are 1 and -1:
$$\mathbb{Z}^\times = \{\pm 1\}.$$

2. An element $a \in \mathbb{Z}/n$ is invertible if and only if it is coprime to n:
$$(\mathbb{Z}/n)^\times = \{a \in \mathbb{Z}/n \mid \gcd(a, n) = 1\}.$$

Example 2.3.5. Let R be an integral domain. A polynomial $p = \sum_{i=0}^{d} c_i x^i \in R[x]$ is invertible if and only if it is a constant polynomial $p = c_0$ and the constant term c_0 is invertible in R:
$$R[x]^\times \cong R^\times.$$

Example 2.3.6. Recall that Laurent polynomials are like polynomials except that they may have terms of negative degrees. For instance:

$$3x^{-8} + 7x^{-1} + 5x^2 \in \mathbb{Z}[x, x^{-1}].$$

The ring of Laurent polynomials with coefficients in R is

$$R[x, x^{-1}] = \left\{ \sum_{i \in \mathbb{Z}} c_i x^i \mid c_i \in R, c_i \neq 0 \text{ for finitely many } i \right\}.$$

If R is an integral domain, then a Laurent polynomial is invertible if and only if it is a unit in R times a power of x:

$$R[x, x^{-1}]^\times = \{ux^d \mid d \in \mathbb{Z}, u \in R^\times\}.$$

In that case, its inverse is

$$(ux^d)^{-1} = u^{-1}x^{-d}.$$

Proposition 2.3.7. *Let R be a commutative ring. A power series $f \in R[\![x]\!]$ is invertible if and only if its constant term c_0 is invertible in R:*

$$R[\![x]\!]^\times = \left\{ \sum_{i=0}^{\infty} c_i x^i \in R[\![x]\!] \mid c_0 \in R^\times \right\}.$$

Proof. See Homework 2 Problem 2, which is [AM69, §1 Exercise 5(i)]. □

Example 2.3.8. In the power series ring $\mathbb{Z}[\![x]\!]$, the inverse of $1 + 3x$ can be computed using a geometric series:

$$\begin{aligned}
(1+3x)^{-1} &= \frac{1}{1+3x} \\
&= \frac{1}{1-(-3x)} \\
&= \sum_{i=0}^{\infty} (-3x)^i \\
&= \sum_{i=0}^{\infty} (-3)^i x^i \\
&= 1 - 3x + 9x^2 - 27x^3 + \cdots
\end{aligned}$$

Example 2.3.9. In the polynomial ring $\mathbb{Z}/4[x]$, the polynomial $1 + 2x$ is a unit, in fact, is its own inverse:

$$(1+2x)(1+2x) = 1 + 4x + 4x^2 = 1.$$

Lemma 2.3.10. *Let R be a commutative ring. If $u \in R^\times$ is a unit and $x \in R$ is nilpotent, then $u + x$ is a unit.*

Slogan: "unit + nilpotent = unit".

Proof. This is [AM69, §1 Exercise 1]. If you want to solve it on your own, skip this spoiler. Since x is nilpotent, $x^n = 0$ holds for some $n \geq 1$. The difference

$$u^n - x^n = u^n - 0 = u^n$$

is a unit, by Lemma 2.3.3. But that difference factors as

$$u^n - x^n = (u - x)(u^{n-1} + u^{n-2}x + \cdots + x^{n-1}).$$

Again by Lemma 2.3.3, the factor $u - x$ must be a unit. □

Alternate proof. We first treat the case $u = 1$. We would like to use the geometric series

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots = \sum_{i=0}^{\infty} x^i.$$

Since $x^n = 0$ holds, the formula for geometric sums yields the equation in R

$$(1 - x)^{-1} = 1 + x + x^2 + \cdots + x^{n-1}$$

so that $1 - x$ is invertible. The general case with a unit $u \in R^\times$ reduces to the previous case via

$$u - x = u(1 - u^{-1}x)$$

since $u^{-1}x$ is nilpotent. □

The next proposition generalizes Example 2.3.5 and explains what was going on in Example 2.3.9.

Proposition 2.3.11. *Let R be a commutative ring. A polynomial $p = \sum_{i=0}^{d} c_i x^i \in R[x]$ is invertible if and only if its constant term c_0 is invertible in R and the other coefficients $c_1, \ldots, c_d$ are nilpotent.*

Proof. [AM69, §1 Exercise 2]. □

Exercise 2.3.12. Let R be a commutative ring.

1. Show that two elements $a, b \in R$ generate the same principal ideal $(a) = (b)$ if and only if they divide each other: $a \mid b$ and $b \mid a$. Two such elements are said to be **associate**.
2. If two elements $a, b \in R$ are related by $a = ub$ for some unit $u \in R^\times$, show that they are associate.
3. Show that the converse holds if R is an integral domain.

2.4 Fields

Definition 2.4.1. A **field** is a commutative ring k in which $1 \neq 0$ and every non-zero element is invertible:

$$k^\times = k \setminus \{0\}.$$

Proposition 2.4.2. *The following conditions on a commutative ring $R \neq 0$ are equivalent.*

1. *R is a field.*
2. *The only ideals of R are 0 and $(1) = R$.*
3. *Every ring map $R \to S$ into a non-zero ring S is injective.*

Example 2.4.3.
1. The ring $\mathbb{Z}/n$ is a field if and only if n is prime. We denote the field with p elements $\mathbb{F}_p = \mathbb{Z}/p$.
2. The rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, and the complex numbers $\mathbb{C}$ are fields.

Example 2.4.4. The Gaussian rationals

$$\mathbb{Q}[i] = \{a + bi \in \mathbb{C} \mid a, b \in \mathbb{Q}\}$$

form a field. It can be obtained both as the fraction field of the Gaussian integers:

$$\mathbb{Q}[i] = \mathrm{Frac}(\mathbb{Z}[i])$$

and as the field extension of $\mathbb{Q}$ obtained by adjoining a square root of -1:

$$\mathbb{Q}[i] = \mathbb{Q}(i).$$

Remark 2.4.5. Given $\alpha \in \mathbb{C}$, denote by $\mathbb{Q}[\alpha]$ the smallest subring of $\mathbb{C}$ containing $\mathbb{Q}$ and α. It consists of all polynomial expressions in α with rational coefficients:

$$\mathbb{Q}[\alpha] = \left\{ \sum_{i=0}^{d} c_i \alpha^i \mid d \geq 0, c_i \in \mathbb{Q} \right\}.$$

Denote by $\mathbb{Q}(\alpha)$ the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and α. It consists of all rational expressions in α with rational coefficients:

$$\mathbb{Q}(\alpha) = \left\{ \frac{p}{q} \mid p, q \in \mathbb{Q}[\alpha], q \neq 0 \right\}.$$

We have equivalent conditions:

1. The inclusion of rings $\mathbb{Q}[\alpha] \subseteq \mathbb{Q}(\alpha)$ is an equality.
2. The number α is algebraic, i.e., a root of some polynomial in $\mathbb{Q}[x]$.
3. The ring $\mathbb{Q}[\alpha]$ is finite-dimensional as a $\mathbb{Q}$-vector space.

See [DF04, §13.1] for more details.

Example 2.4.6. For a field k, the field of rational functions with coefficients in k is

$$k(x) = \left\{ \frac{p}{q} \mid p, q \in k[x], q \neq 0 \right\}.$$

It is the fraction field of the polynomial ring with coefficients in k:

$$k(x) = \mathrm{Frac}(k[x]).$$

Remark 2.4.7. More generally, we could start with an integral domain R and consider the polynomial ring $R[x]$, which is also an integral domain, by Proposition 2.1.5. Its fraction field consists of the rational functions with coefficients in R:

$$\mathrm{Frac}(R[x]) = \left\{ \frac{p}{q} \mid p, q \in R[x], q \neq 0 \right\}.$$

However, this construction has the same effect as first inverting all the non-zero constant polynomials, then taking rational functions:

$$\mathrm{Frac}(R[x]) \cong \mathrm{Frac}(R)(x).$$

Example 2.4.8. With $R = \mathbb{Z}$, we have

$$\mathrm{Frac}(\mathbb{Z}[x]) \cong \mathbb{Q}(x) \cong \mathrm{Frac}(\mathbb{Q}[x]).$$

By clearing denominators of the coefficients, a rational function in $\mathbb{Q}(x)$ can always be written as a fraction of polynomials with integer coefficients, for instance:

$$\frac{3/4 + x^7}{1 + (5/3)x} = \frac{9/4 + 3x^7}{3 + 5x} = \frac{9 + 12x^7}{12 + 20x}.$$

3 Prime ideals and maximal ideals

3.1 Definitions and properties

Definition 3.1.1. Let R be a commutative ring. A proper ideal $I \subsetneq R$ is called:

- **prime** if the following implication holds:

$$xy \in I \implies x \in I \text{ or } y \in I.$$

  Equivalently:

$$x \notin I \text{ and } y \notin I \implies xy \notin I.$$

- **maximal** if the only ideal larger than I is the whole ring R:

$$I \subsetneq J \implies J = R.$$

Remark 3.1.2. Recall that an element $p \in R$ is called *prime* if the following implication holds:

$$p \mid xy \implies p \mid x \text{ or } p \mid y.$$

Reformulating in terms of the ideal (p) generated by p, the implication becomes:

$$xy \in (p) \implies x \in (p) \text{ or } y \in (p).$$

In other words, the element p is prime if and only if the ideal (p) is prime.

Proposition 3.1.3. *1. An ideal $P \subset R$ is prime if and only if the quotient ring R/P is an integral domain.*

2. An ideal $\mathfrak{m} \subset R$ is maximal if and only if the quotient ring $R/\mathfrak{m}$ is a field.

Corollary 3.1.4. *1. The ideal $(0) \subset R$ is prime if and only if R is an integral domain.*

2. The ideal $(0) \subset R$ is maximal if and only if R is a field.

We can see those characterizations directly. The ideal (0) being prime means:

$$xy \in (0) \implies x \in (0) \text{ or } y \in (0),$$

that is, R is an integral domain. The ideal (0) being maximal means:

$$x \notin (0) \implies (x) = R,$$

that is, every non-zero element $x \neq 0$ is a unit.

Corollary 3.1.5. *Every maximal ideal is prime.*

Proposition 3.1.6. *Let R be a commutative ring and $I \subseteq R$ an ideal, and let $q\colon R \twoheadrightarrow R/I$ denote the quotient map. Via the bijective correspondence from Proposition 1.3.10*

$$\{\textit{ideals of } R/I\} \xrightarrow{\cong} \{\textit{ideals of } R \textit{ containing } I\}$$

$$J \subseteq R/I \longmapsto q^{-1}(J)$$

prime ideals correspond to prime ideals, and maximal ideals correspond to maximal ideals.

Proof. For an ideal $J \subseteq R/I$, the third isomorphism theorem yields

$$(R/I)/J \cong R/q^{-1}(J).$$

From this and Proposition 3.1.3, we obtain a chain of equivalent conditions:

The ideal $J \subseteq R/I$ is prime.

$\iff$ The quotient ring $(R/I)/J$ is an integral domain.

$\iff$ The quotient ring $R/q^{-1}(J)$ is an integral domain.

$\iff$ The ideal $q^{-1}(J) \subseteq R$ is prime.

The same argument works for maximal ideals, replacing "integral domain" with "field". □

Proposition 3.1.7. *Let $\varphi\colon R \to S$ be a ring map. If $Q \subseteq S$ is a prime ideal, then the preimage $\varphi^{-1}(Q) \subseteq R$ is a prime ideal.*

Proof. For any $x, y \in R$, assume that the product satisfies $xy \in \varphi^{-1}(Q)$. We obtain the implication:

$$\begin{aligned} xy \in \varphi^{-1}(Q) &\iff \varphi(xy) \in Q \\ &\iff \varphi(x)\varphi(y) \in Q \\ &\implies \varphi(x) \in Q \text{ or } \varphi(y) \in Q \qquad \text{since } Q \text{ is prime} \\ &\iff x \in \varphi^{-1}(Q) \text{ or } y \in \varphi^{-1}(Q), \end{aligned}$$

which shows that $\varphi^{-1}(Q)$ is prime. □

Warning 3.1.8. Given a maximal ideal $\mathfrak{n} \subset S$, the preimage $\varphi^{-1}(\mathfrak{n}) \subseteq R$ need **not** be maximal. Take for example the inclusion map $\mathrm{inc}\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$. The ideal $(0) \subset \mathbb{Q}$ is maximal, since $\mathbb{Q}$ is a field, yet its preimage

$$\mathrm{inc}^{-1}(0) = (0) \subset \mathbb{Z}$$

is not maximal.

Nonetheless, by Corollary 3.1.5 and Proposition 3.1.7, the preimage $\varphi^{-1}(\mathfrak{n}) \subseteq R$ is guaranteed to be prime.

3.2 Examples

Example 3.2.1. In $\mathbb{Z}$, every ideal is of the form $(n) \subseteq \mathbb{Z}$ for some $n \in \mathbb{Z}$. For $n \neq 0$, we have equivalent conditions:

The ideal (n) is prime.

$\iff$ The number n is prime.

$\iff$ The ideal (n) is maximal.

Indeed, if n is a composite number $n = ab$, then any divisor will generate a larger ideal $(a) \subseteq (n)$, for instance:

$$(6) \subsetneq (2).$$

Example 3.2.2. Let $n \geq 2$ and consider the quotient ring $\mathbb{Z}/n$. By the correspondence in Proposition 1.3.10, every ideal in $\mathbb{Z}/n$ is of the form $(\overline{k})$ for some divisor $k \mid n$. The ideal $(\overline{k}) \subseteq \mathbb{Z}/n$ is prime if and only if k is prime, in which case $(\overline{k})$ is also maximal.

Example 3.2.3. For a field k, recall that the polynomial ring $k[x]$ is a principal ideal domain (PID). For a polynomial $f \neq 0$, we have equivalent conditions:

The ideal (f) is prime.

$\iff$ The polynomial f is prime.

$\iff$ The polynomial f is irreducible, i.e., cannot be written as a product $f = ab$ of non-units.

$\iff$ The ideal (f) is maximal.

Example 3.2.4. For a field k, consider the truncated polynomial ring $k[x]/(x^n)$ for some $n \geq 1$. Every ideal $I \subseteq k[x]/(x^n)$ is of the form

$$I = (x^i)$$

for some exponent $0 \leq i \leq n$. This includes the extreme cases $(x^0) = (1) = k[x]/(x^n)$ and $(x^n) = (0)$. Hence the only prime ideal is (x), which is also the only maximal ideal.

Example 3.2.5. For a field k, the polynomial ring $k[x, y]$ is a unique factorization domain (UFD) but not a PID. The ideal (x) is prime, since the polynomial x is irreducible. However (x) is not maximal, since there are larger proper ideals, for instance $(x) \subsetneq (x, y)$.

More generally, for any $a, b \in k$, the ideal $(x - a) \subset k[x, y]$ is prime, but not maximal, as exhibited by the inclusions

$$(x - a) \subsetneq (x - a, y - b) \subsetneq k[x, y].$$

The following statement generalizes Examples 3.2.1 and 3.2.3.

Proposition 3.2.6. *In a principal ideal domain, a non-zero ideal $I \neq (0)$ is prime if and only if it is maximal.*

The following statement generalizes Examples 3.2.2 and 3.2.4.

Corollary 3.2.7. *Let R be a principal domain domain and $I \subset R$ an ideal. Every ideal in the quotient ring $J \subseteq R/I$ is principal. A non-zero ideal $J \subseteq R/I$ is prime if and only if it is maximal.*

Proof. This follows from Propositions 1.3.10 and 3.1.6. □

Proposition 3.2.8. *Let k be a field and consider the power series ring $k[\![x]\!]$. Every non-zero ideal in $k[\![x]\!]$ is of the form (x^n) for some $n \geq 0$.*

In particular, the only maximal ideal is (x), and the prime ideals are (0) and (x).

Proof. For a power series $f = \sum_{i=0}^{\infty} c_i x^i$ with $f \neq 0$, define the *order* of f as the lowest degree appearing in f:

$$\nu(f) := \min\{i \in \mathbb{N} \mid c_i \neq 0\}.$$

For instance:

$$\nu(7x^2 + 5x^9) = 2.$$

Let $I \subseteq k[\![x]\!]$ be a non-zero ideal. Take the lowest degree appearing in *any* of the power series in I:

$$n := \min\{\nu(f) \mid f \in I\}.$$

We claim $I = (x^n)$. Let us prove both inclusions separately.

($\subseteq$) For every $f \in I$, the order of f is at least n:

$$m = \nu(f) \geq n$$

so that we can factor out x^n:

$$\begin{aligned} f &= c_m x^m + c_{m+1} x^{m+1} + \cdots \\ &= x^n \left(c_m x^{m-n} + c_{m+1} x^{m-n+1} + \cdots \right) \\ &\in (x^n). \end{aligned}$$

($\supseteq$) The lowest order n is realized by some power series $g = \sum_{i=n}^{\infty} d_i x^i \in I$, with $d_n \neq 0$. Factoring out x^n yields

$$\begin{aligned} g &= d_n x^n + d_{n+1} x^{m+1} + \cdots \\ &= x^n \left(d_n + d_{n+1} x + \cdots \right) \\ &= x^n h. \end{aligned}$$

The power series $h = d_n + d_{n+1}x + \cdots$ is invertible, since its constant term $d_n \neq 0$ is invertible in k; see Homework 2 Problem 2. Therefore we obtain

$$\begin{aligned} & g \in I \\ \implies & gh^{-1} \in I \\ \implies & x^n \in I, \end{aligned}$$

which proves the inclusion $(x^n) \subseteq I$. □

Remark 3.2.9. The power series ring $k[\![x]\!]$ is an example of *discrete valuation ring* (DVR), with the order function ν being the valuation. A similar argument shows more generally that a DVR is a PID, where in fact every ideal is a power of the maximal ideal.

3.3 Existence

Theorem 3.3.1. *Every nontrivial commutative ring $R \neq 0$ has a maximal ideal.*

Remark 3.3.2. The proof relies on Zorn's lemma, which is equivalent to the axiom of choice. In fact, the statement of Theorem 3.3.1 is also *equivalent* to the axiom of choice.

Corollary 3.3.3. *Every proper ideal $I \subsetneq R$ is contained in some maximal ideal.*

Proof. Since $I \subsetneq R$ is a proper ideal, the quotient ring $R/I \neq 0$ is nontrivial. By Theorem 3.3.1, R/I has a maximal ideal $\mathfrak{m} \subseteq R/I$. By Proposition 3.1.6, the preimage $q^{-1}(\mathfrak{m}) \subseteq R$ is a maximal ideal containing I. □

Corollary 3.3.4. *Every non-unit of R is contained in some maximal ideal.*

Proof. A non-unit $x \in R$ generates a proper ideal $(x) \subsetneq R$. By Corollary 3.3.3, (x) is contained in some maximal ideal $\mathfrak{m}$. □

4 Zorn's lemma

4.1 Preliminaries on posets

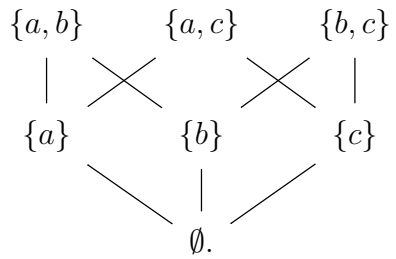
Definition 4.1.1. Let $(P, \leq)$ be a partially ordered set (or *poset* for short).

1. A **chain** in P is a totally ordered subset $C \subseteq P$.
2. Given a subset $A \subseteq P$, an **upper bound** for A is an element $b \in P$ such that
$$a \leq b$$
holds for all $a \in A$.
Note that the upper bound b itself need not lie in A.
3. An element $m \in P$ is **maximal** if there is no larger element:
$$m \leq n \implies n = m.$$
Note that m need not be larger than every element of P, since m might be incomparable with many elements.

Example 4.1.2. Consider the set $S = \{a, b, c\}$ and its power set $\mathcal{P}(S)$, viewed as a poset ordered by inclusion. Take the poset of proper subsets of S:

$$\begin{aligned} P &= \mathcal{P}(S) \setminus \{S\} \\ &= \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}\}, \end{aligned}$$

as illustrated in the following Hasse diagram:



In the poset P, the subsets

$$C = \{\emptyset, \{a\}\}$$
$$D = \{\emptyset, \{a\}, \{a, b\}\}$$

are chains, whereas the subset

$$\{\emptyset, \{a\}, \{b, c\}\}$$

is *not* a chain.

For the chain C, the element $\{a\}$ is an upper bound, as are $\{a, b\}$ and $\{a, c\}$. In fact, $\{a\}$ is the least upper bound (a.k.a. supremum) for C.

The maximal elements in the poset P are those of the form $S \setminus \{s\}$, namely $\{a, b\}$, $\{a, c\}$, and $\{b, c\}$. Note that $\{a, b\}$ is maximal but is not greater than $\{c\}$, since the two are incomparable.

Example 4.1.3. In the totally ordered set $\mathbb{R}$, consider the interval $A = [5, 8)$. The element 8 is an upper bound for A, as are 9, 9.1, and 43. In fact, 8 is the least upper bound for A.

Example 4.1.4. In the totally ordered set $\mathbb{Q}$, consider the subset

$$A = \{x \in \mathbb{Q} \mid x^2 < 2\}.$$

The element 1.5 is an upper bound for A. However, A does not have a least upper bound in $\mathbb{Q}$.

4.2 The statement

Theorem 4.2.1 (Zorn's lemma)**.** *Let $(P, \leq)$ be a non-empty poset in which every chain admits an upper bound. Then P has a maximal element.*

Remark 4.2.2. The statement of Zorn's lemma is equivalent to the axiom of choice.

5 Local rings, nilradical, Jacobson radical

5.1 Local rings

Definition 5.1.1. A commutative ring R is **local** if it has a unique maximal ideal.

We sometimes denote a local ring $(R, \mathfrak{m})$ where $\mathfrak{m} \subset R$ is the maximal ideal. The **residue field** of R is the quotient ring $k = R/\mathfrak{m}$.

Proposition 5.1.2. *For a commutative ring R, the following are equivalent.*

1. *R is local.*
2. *The non-units of R form an ideal (and thus the unique maximal ideal).*
3. *The non-units of R are closed under addition.*
4. *There is a maximal ideal $\mathfrak{m} \subset R$ such that every element of $1 + \mathfrak{m}$ is a unit.*

Let us prove more directions than needed, because the arguments are interesting.

Proof. (2 $\iff$ 3) The non-units are always closed under multiplication by arbitrary elements:

$$x \text{ is a non-unit } \implies rx \text{ is a non-unit for all } r \in R.$$

Hence the non-units form an ideal if and only if they satisfy the other condition in the definition of ideal, namely being closed under addition.

(1 $\implies$ 2) Assume that R local, with unique maximal ideal $\mathfrak{m}$. Every non-unit $x \in R$ is contained in some maximal ideal, hence $x \in \mathfrak{m}$ since that is the only maximal ideal. This proves the inclusion

$$\{\text{non-units}\} \subseteq \mathfrak{m}.$$

Since $\mathfrak{m}$ is a proper ideal, the reverse inclusion also holds:

$$\mathfrak{m} = \{\text{non-units}\}.$$

(2 $\implies$ 1) Assume that the non-units of R form an ideal. Then the ideal of non-units is maximal, since any larger ideal J must contain a unit, hence $J = (1) = R$.

Moreover, every proper ideal $I \subset R$ consists of non-units:

$$I \subseteq \{\text{non-units}\}.$$

In particular, any maximal ideal $\mathfrak{m} \subset R$ must satisfy

$$\mathfrak{m} = \{\text{non-units}\}$$

by the maximality condition.

($2 \implies 4$) Assume that the non-units of R form an ideal, hence a maximal ideal $\mathfrak{m} = R \setminus R^\times$. For every $x \in \mathfrak{m}$, the element $1 + x$ must be a unit, otherwise

$$1 = (1 + x) - x$$

would be a sum of non-units, hence a non-unit.

($4 \implies 2$) Let $\mathfrak{m} \subset R$ be a maximal ideal such that every element of $1 + \mathfrak{m}$ is a unit. We want to show that $\mathfrak{m}$ consists of all the non-units, i.e., that every element $x \in R \setminus \mathfrak{m}$ is a unit. By maximality of $\mathfrak{m}$, adjoining x to $\mathfrak{m}$ yields the whole ring:

$$\begin{aligned} & (x) + \mathfrak{m} = (1) = R \\ \implies & rx + m = 1 \quad \text{for some } r \in R, m \in \mathfrak{m} \\ \implies & rx = 1 - m \ \text{ is a unit, by the assumption} \\ \implies & x \ \text{ is a unit.} \end{aligned}$$

□

Example 5.1.3. Any field k is a local ring, with unique maximal ideal $(0) \subset k$.

Example 5.1.4.

1. The ring $\mathbb{Z}$ is not local, since it has distinct maximal ideals $(2) \neq (3)$. Recall that the maximal ideals of $\mathbb{Z}$ are those of the form (p) for a prime number $p \in \mathbb{Z}$.

   We also see that non-units in $\mathbb{Z}$ fail to be closed under addition, for instance

   $$3 - 2 = 1 \in \mathbb{Z}^\times.$$

2. The ring $\mathbb{Z}/6$ is not local, since it has distinct maximal ideals $(2) \neq (3)$.

3. The ring $\mathbb{Z}/4$ is local, with unique maximal ideal $(2) \subset \mathbb{Z}/4$.

Example 5.1.5. The ***p*-local integers** are the rational numbers where we may divide by any prime *except* p:

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}.$$

The units of $\mathbb{Z}_{(p)}$ are the fractions that can be written without a factor of p in the numerator:

$$\mathbb{Z}_{(p)}^\times = \left\{ \frac{a}{b} \in \mathbb{Z}_{(p)} \mid p \nmid a \right\}.$$

Taking complements, the non-units of $\mathbb{Z}_{(p)}$ are the multiples of p:

$$\mathbb{Z} \setminus \mathbb{Z}_{(p)}^\times = (p).$$

Therefore $\mathbb{Z}_{(p)}$ is local, with unique maximal ideal (p) and residue field $\mathbb{Z}_{(p)}/(p) \cong \mathbb{F}_p$.

Example 5.1.6. For a field k, the polynomial ring $k[x]$ is not local, since it has distinct maximal ideals $(x) \neq (x - 1)$.

Note that non-units in $k[x]$ fail to be closed under addition, for instance

$$x - (x - 1) = 1 \in k[x]^\times.$$

Example 5.1.7. For a field k, consider the truncated polynomial ring $k[x]/(x^n)$ for some $n \geq 1$. In Example 3.2.4, we saw that the only prime ideal in $k[x]/(x^n)$ is (x). Therefore $k[x]/(x^n)$ is local, with unique maximal ideal (x) and residue field

$$(k[x]/(x^n))\,/(x) \cong k[x]/(x) \cong k.$$

Example 5.1.8. For a field k, consider the power series ring $k[\![x]\!]$. In Proposition 3.2.8, we saw that the only prime ideals of $k[\![x]\!]$ are (0) and (x). Therefore $k[\![x]\!]$ is local, with unique maximal ideal (x) and residue field $k[\![x]\!]/(x) \cong k$.

5.2 Nilradical

Recall that the *nilradical* of a commutative ring R is the ideal of nilpotent elements:

$$\operatorname{nil}(R) = \{x \in R \mid x^n = 0 \text{ for some } n \geq 1\}.$$

Proposition 5.2.1. *The quotient ring $R/\operatorname{nil}(R)$ is reduced, i.e., has no nilpotents.*

Proof. For $x \in R$, denote by $\overline{x}$ its equivalence class in the quotient ring $R/\operatorname{nil}(R)$. Let $\overline{x} \in R/\operatorname{nil}(R)$ be nilpotent, so that

$$\overline{x}^n = 0 \in R/\operatorname{nil}(R)$$

holds for some $n \geq 1$. The representative $x^n \in R$ lies in the ideal $\operatorname{nil}(R)$, i.e., is nilpotent, so that

$$(x^n)^k = 0 = x^{nk}$$

holds for some $k \geq 1$. The equation exhibits x as being nilpotent:

$$\begin{aligned} & x \in \operatorname{nil}(R) \\ \iff & \overline{x} = 0 \in R/\operatorname{nil}(R). \end{aligned}$$

□

Exercise 5.2.2. In a commutative ring R, show that an arbitrary intersection of ideals $\bigcap_\alpha I_\alpha$ is an ideal.

Proposition 5.2.3. *For any commutative ring R, the nilradical is the intersection of all prime ideals:*

$$\operatorname{nil}(R) = \bigcap_{\substack{P \subset R \\ P \text{ prime}}} P.$$

Proof. ($\subseteq$) Let $a \in \operatorname{nil}(R)$ be a nilpotent element, so that $a^n = 0$ holds for some $n \geq 1$. Let $P \subset R$ be a prime ideal. The condition

$$a^n = 0 \in P$$

implies $a \in P$ since P was arbitrary, we obtain

$$a \in \bigcap_{\substack{P \subset R \\ P \text{ prime}}} P.$$

($\supseteq$) Let $a \in R \setminus \operatorname{nil}(R)$ be a non-nilpotent element. We want to find some prime ideal $P \subset R$ satisfying $a \notin P$. While the proof in [AM69, Proposition 1.8] is perfectly fine, here is a streamlined argument explained by Martin Brandenburg in [Bra17].

Since $a \in R$ is not nilpotent, the localization $R[\frac{1}{a}]$ is not the zero ring. Hence it has a maximal ideal $\mathfrak{m} \subset R[\frac{1}{a}]$. Since $\frac{a}{1}$ is a unit in $R[\frac{1}{a}]$, it cannot be in a proper ideal, in particular:

$$\begin{aligned} & \frac{a}{1} \notin \mathfrak{m} \\ \iff & a \notin \varphi^{-1}(\mathfrak{m}), \end{aligned}$$

where $\varphi\colon R \to R[\frac{1}{a}]$ denotes the localization map, given by $\varphi(x) = \frac{x}{1}$. Since $\mathfrak{m}$ is a maximal ideal, it is prime, and so is its preimage $P := \varphi^{-1}(\mathfrak{m}) \subset R$. Therefore P is a prime ideal not containing a. □

5.3 Jacobson radical

Definition 5.3.1. The **Jacobson radical** of a commutative ring R is the intersection of all maximal ideals:

$$\mathrm{Jac}(R) := \bigcap_{\substack{\mathfrak{m} \subset R \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m}.$$

Remark 5.3.2. Since every maximal ideal is prime, we always have the inclusion

$$\mathrm{nil}(R) \subseteq \mathrm{Jac}(R).$$

Proposition 5.3.3. *In any commutative ring R, the Jacobson radical is*

$$\mathrm{Jac}(R) = \{x \in R \mid 1 + rx \text{ is a unit for all } r \in R\}.$$

Proof. See [AM69, Proposition 1.9]. □

Example 5.3.4. In a local commutative ring R, the Jacobson radical is the unique maximal ideal $\mathrm{Jac}(R) = \mathfrak{m}$.

Example 5.3.5.

1. The ring $\mathbb{Z}$ has Jacobson radical

$$\begin{aligned}\mathrm{Jac}(\mathbb{Z}) &= \bigcap_{p \text{ prime}} (p) \\ &= \{n \in \mathbb{Z} \mid p \mid n \text{ for all prime number } p\} \\ &= (0).\end{aligned}$$

2. The ring $\mathbb{Z}/6$ has Jacobson radical

$$\mathrm{Jac}(\mathbb{Z}/6) = (2) \cap (3) = (6) = (0).$$

3. $\mathrm{Jac}(\mathbb{Z}/4) = (2)$. This is a special case of Example 5.3.4, since the ring $\mathbb{Z}/4$ is local with unique maximal ideal (2).

4. $\mathrm{Jac}(\mathbb{Z}/18) = (6) = \mathrm{nil}(\mathbb{Z}/18)$. Compare with Homework 3 Problem 1.

Example 5.3.6. The p-local integers have as Jacobson radical

$$\mathrm{Jac}(\mathbb{Z}_{(p)}) = (p).$$

This is also a special case of Example 5.3.4, since the ring $\mathbb{Z}_{(p)}$ is local with unique maximal ideal (p).

However $\mathbb{Z}_{(p)}$ is an integral domain, in particular has no nilpotents:

$$\mathrm{nil}(\mathbb{Z}_{(p)}) = (0) \subsetneq (p) = \mathrm{Jac}(\mathbb{Z}_{(p)}).$$

Example 5.3.7. Let R be an integral domain and consider the polynomial ring $R[x]$. Its Jacobson radical is $\mathrm{Jac}(R[x]) = (0)$. Indeed, for any $f \in \mathrm{Jac}(R[x])$, the polynomial

$$1 + xf$$

must be a unit, hence a constant polynomial since R is an integral domain. This forces $f = 0$.

Example 5.3.8. For a field k, the truncated polynomial ring $k[x]/(x^n)$ is local with unique maximal ideal (x), by Example 5.1.7. By Example 5.3.4, the Jacobson radical is the maximal ideal

$$\mathrm{Jac}\left(k[x]/(x^n)\right) = (x).$$

In this case the nilradical and Jacobson radical agree:

$$\mathrm{nil}\left(k[x]/(x^n)\right) = (x).$$

Example 5.3.9. For a field k, the power series ring $k[\![x]\!]$ is local with unique maximal ideal (x), by Example 5.1.8. By Example 5.3.4, the Jacobson radical is the maximal ideal

$$\mathrm{Jac}(k[\![x]\!]) = (x).$$

However $k[\![x]\!]$ is an integral domain, in particular has no nilpotents:

$$\mathrm{nil}(k[\![x]\!]) = (0) \subsetneq (x) = \mathrm{Jac}(k[\![x]\!]).$$

The previous example can be generalized as follows.

Proposition 5.3.10. *Let R be a commutative ring. In the power series ring $R[\![x]\!]$, a power series $f = \sum_{i=0}^{\infty} c_i x^i$ is in the Jacobson radical of $R[\![x]\!]$ if and only if its constant term c_0 is in the Jacobson radical of R:*

$$f \in \mathrm{Jac}(R[\![x]\!]) \iff c_0 \in \mathrm{Jac}(R).$$

Proof. See Homework 3 Problem 3, which is [AM69, §1 Exercise 5(iii)]. □

6 Operations on ideals

6.1 Sum of ideals

Lemma 6.1.1. *Let R be a commutative ring and $X \subseteq R$ a subset.*

1. *There exists a smallest ideal of R containing X, called the **ideal generated by X**, denoted (X) or RX.*
2. *Said ideal is given by the R-linear combinations of elements of X:*

$$(X) = \left\{ \sum_{i=1}^{n} r_i x_i \mid n \geq 0,\, r_i \in R,\, x_i \in X \right\}.$$

Proof. 1. Since an arbitrary intersection of ideals is an ideal (Exercise 5.2.2), the subset

$$(X) = \bigcap_{\substack{\text{ideals } I \subseteq R \\ X \subseteq I}} I$$

is an ideal, which moreover contains X. It is the smallest such ideal by construction: any ideal $J \subseteq R$ containing X satisfies $(X) \subseteq J$.

2. Let us prove both inclusions separately.

($\supseteq$) Given $r_1, \dots r_n \in R$ and $x_1, \dots, x_n \in X$, each term $r_i x_i$ must lie in (X), since (X) is an ideal. Likewise, their sum $\sum_{i=1}^{n} r_i x_i$ must lie in (X).

($\subseteq$) Denote the right-hand side by L (for *linear* combinations). Since L contains X, it suffices to show that L is an ideal to conclude $(X) \subseteq L$. The set L contains 0 (as the linear combination of $n = 0$ terms), is closed under sums:

$$(\sum_{i=1}^{n} r_i x_i) + (\sum_{j=1}^{m} r'_i x'_i) \in L$$

and closed under multiplication by any element $r \in R$:

$$r(\sum_{i=1}^{n} r_i x_i) = \sum_{i=1}^{n} (r r_i) x_i \in L. \qquad \square$$

Definition 6.1.2. Let R be a commutative ring and $I, J \subseteq R$ ideals. The **sum** of I and J is the ideal

$$I + J = \{x + y \in R \mid x \in I,\, x \in J\}.$$

More generally, given a family of ideals $I_\alpha \subseteq R$ indexed by $\alpha \in \Lambda$, their **sum** is the ideal

$$\sum_{\alpha \in \Lambda} I_\alpha = \left\{ \sum_{i=1}^{n} x_{\alpha_i} \mid n \geq 0,\, \alpha_i \in \Lambda,\, x_{\alpha_i} \in I_{\alpha_i} \right\}.$$

Exercise 6.1.3. 1. Check that $I + J$, and more generally $\sum_{\alpha\in\Lambda} I_\alpha$, is indeed an ideal of R.

2. Show that $I + J$ is the ideal generated by the union of I and J:

$$I + J = (I \cup J)$$

(Homework 4 Problem 1).

3. More generally, the sum $\sum_{\alpha\in\Lambda} I_\alpha$ is the ideal generated by the union of the I_α:

$$\sum_{\alpha\in\Lambda} I_\alpha = \left(\bigcup_\alpha I_\alpha\right).$$

Remark 6.1.4. The union $I \cup J \subseteq R$ is not an ideal, in fact not even a subgroup, unless one of I or J contains the other. Indeed, assume that $I \cup J$ is a subgroup and $I \not\subseteq J$, so that there is an element $i \in I \setminus J$. We want to show the containment $J \subseteq I$. Let $j \in J$. By assumption, the sum $i + j$ also lies in the union: $i + j \in I \cup J$. But $i + j$ cannot lie in J, in light of

$$i = (i + j) - j \notin J.$$

Hence we have $i + j \in i$, from which we obtain

$$j = (i + j) - i \in I$$

and thus $J \subseteq I$.

6.2 Product of ideals

Definition 6.2.1. Let R be a commutative ring and $I, J \subseteq R$ ideals. The **product** of I and J is the ideal

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \in R \mid n \geq 1,\ x_i \in I,\ y_i \in J \right\}.$$

Remark 6.2.2. The collection of products of elements of I and J

$$\{xy \in R \mid x \in I,\ y \in J\}$$

is not closed under addition in general, which is why we needed to take sums in Definition 6.2.1.

However, when I and J are both principal, with $I = (a)$ and $J = (b)$, then the set of products of elements of I and J is already closed under addition, hence an ideal:

$$\begin{aligned} \{xy \in R \mid x \in I,\ y \in J\} &= \{(ra)(sb) \in R \mid r, s \in R\} \\ &= \{r'ab \in R \mid r' \in R\} \\ &= (ab). \end{aligned}$$

Example 6.2.3. Consider the ring of polynomials with rational coefficients $\mathbb{Q}[x]$ and the ideals $I = J = (x, y)$. Both $x \cdot x = x^2$ and $y \cdot y = y^2$ are products of elements of I and J, but their sum $x^2 + y^2$ is not, since $x^2 + y^2$ is irreducible in $\mathbb{Q}[x]$. Nonetheless, we have

$$x^2 + y^2 \in IJ$$

since sums were allowed in Definition 6.2.1.

The product of ideals $I_1, \ldots, I_n \subseteq R$ is the ideal

$$I_1 \cdots I_n = \left\{ \sum_{i=1}^{n} x_{1,i} \cdots x_{n,i} \mid n \geq 1,\ x_{k,i} \in I_k \right\}.$$

In particular, the powers of an ideal I are ideals I^n which form a decreasing sequence

$$\cdots \subseteq I^3 \subseteq I^2 \subseteq I \subseteq I^0 = (1) = R.$$

Lemma 6.2.4. *The product of ideals distributes over the sum: for any ideals $I, J, K \subseteq R$, we have*

$$\begin{aligned} I(J + K) &= IJ + IK \\ (I + J)K &= IK + JK. \end{aligned}$$

Example 6.2.5. The product of principal ideals $I = (a)$ and $J = (b)$ is the principal ideal

$$IJ = (a)(b) = (ab).$$

More generally, if I has m generators $I = (a_1, \ldots, a_m)$ and J has n generators $J = (b_1, \ldots, b_n)$, then the product can be generated by the mn products of generators:

$$IJ = (a_1b_1, a_1b_2, \ldots, a_mb_n)$$

(Homework 4 Problem 1).

Example 6.2.6. In $\mathbb{Z}$, take the ideals $I = (6)$ and $J = (10)$. Their sum is

$$(6) + (10) = (6, 10) = (2).$$

Their product is

$$(6)(10) = (6 \cdot 10) = (60)$$

by Example 6.2.5. Their intersection is

$$\begin{aligned}(6) \cap (10) &= \{n \in \mathbb{Z} \mid 6 \mid n \text{ and } 10 \mid n\} \\ &= \{n \in \mathbb{Z} \mid 30 \mid n\} \\ &= (30).\end{aligned}$$

Example 6.2.7. For k a field, consider the polynomial ring $k[x]$ and take the ideals $I = (x^2 - x)$ and $J = (x^2 - 1)$. Using the factorizations

$$\begin{aligned}x^2 - x &= x(x-1) \\ x^2 - 1 &= (x+1)(x-1),\end{aligned}$$

the sum of I and J is

$$(x^2 - x) + (x^2 - 1) = (x - 1).$$

Their product is

$$(x^2 - x)(x^2 - 1) = \big((x^2 - x)(x^2 - 1)\big) = \big(x(x+1)(x-1)^2\big)$$

by Example 6.2.5. Their intersection is

$$(x^2 - x) \cap (x^2 - 1) = \left(x(x+1)(x-1)\right).$$

The next statement generalizes Examples 6.2.6 and 6.2.7.

Proposition 6.2.8. *Let R be a unique factorization domain (UFD) and $a, b \in R$ non-zero elements.*

1. *The intersection of principal ideals is*

$$(a) \cap (b) = (\operatorname{lcm}(a, b)).$$

2. *The sum of principal ideals satisfies*

$$(a) + (b) \subseteq (\gcd(a, b)).$$

3. If moreover R is a principal ideal domain (PID), then equality holds:

$$(a) + (b) = (\gcd(a, b)).$$

Proof. 1. Since any two non-zero elements in a UFD admit a lowest common multiple, we obtain:

$$\begin{aligned}(a) \cap (b) &= \{x \in R \mid a \mid x \text{ and } b \mid x\} \\ &= \{x \in R \mid \operatorname{lcm}(a, b) \mid x\} \\ &= (\operatorname{lcm}(a, b)).\end{aligned}$$

2. Writing $d = \gcd(a, b)$, the divisibility conditions yield

$$\begin{aligned}& d \mid a \text{ and } d \mid b \\ \implies & (a) \subseteq (d) \text{ and } (b) \subseteq (d) \\ \implies & (a) + (b) \subseteq (d) \qquad \text{by Exercise 6.1.3.}\end{aligned}$$

3. This is Bézout's identity. In more detail: Since R is a PID, we have

$$(a) + (b) = (e)$$

for some element $e \in R$. We deduce the divisibility

$$\begin{aligned}& \begin{cases} a \in (a) \subseteq (e) \implies e \mid a \\ b \in (b) \subseteq (e) \implies e \mid b \end{cases} \\ \implies & e \mid \gcd(a, b) = d \\ \implies & (d) \subseteq (e) = (a) + (b).\end{aligned}$$

□

Remark 6.2.9. Item (3) need not be true if R is not a PID. For example, consider a field k and the polynomial ring $k[x, y]$, which is a UFD. Take the principal ideals $I = (x)$ and $J = (y)$. Their sum is

$$\begin{aligned}(x) + (y) &= (x, y) \\ &= \left\{ p = \sum_{i,j \geq 0} c_{ij} x^i y^j \in k[x, y] \mid c_{00} = 0 \right\} \\ &= \{\text{polynomials } p(x, y) \text{ with constant term } p(0, 0) = 0\}.\end{aligned}$$

However, the greatest common divisor is $\gcd(x, y) = 1$, which yields a strict inclusion

$$(x) + (y) = (x, y) \subsetneq (\gcd(x, y)) = (1) = k[x, y].$$

Let us look at some non-principal ideals.

Example 6.2.10. Consider a field $\Bbbk$ and the polynomial ring in three variables $\Bbbk[x, y, z]$. Take the ideals $I = (x, y)$ and $J = (x, z)$. By Homework 4 Problem 1, their sum is

$$(x, y) + (x, z) = (x, y, z)$$

and their product is

$$(x, y)(x, z) = (x^2, xz, xy, yz).$$

Their intersection $(x, y) \cap (x, z)$ consists of the polynomials $p = \sum_{i,j,k\geq 0} c_{ijk} x^i y^j z^k$ satisfying the following equivalent conditions:

p has no terms z^k nor terms y^j.

$\iff$ $p = xq + r$, where $r = r(y, z)$ has no terms z^k nor terms y^j. Here we took

$$q = \sum_{\substack{i\geq 1\\ j,k\geq 0}} c_{ijk} x^{i-1} y^j z^k$$

$$r = \sum_{j,k\geq 0} c_{0jk} y^j z^k.$$

$\iff$ $p = xq + yzs$ for some polynomial $s = s(y, z)$. Here we took

$$s = \sum_{j,k\geq 1} c_{0jk} y^{j-1} z^{k-1}.$$

$\iff$ $p \in (x, yz)$.

Thus the intersection is

$$(x, y) \cap (x, z) = (x, yz).$$

Note that the inclusion

$$(x, y)(x, z) \subsetneq (x, y) \cap (x, z)$$

is strict: we have $x \in (x, y) \cap (x, z)$ but $x \notin (x, y)(x, z)$.

6.3 Product versus intersection

Lemma 6.3.1. *Let R be a commutative ring and $I, J \subseteq R$ ideals.*

1. *The inclusion $IJ \subseteq I \cap J$ always holds.*
2. *If moreover the ideals satisfy $I + J = (1)$, then the inclusion is an equality:*

$$IJ = I \cap J.$$

Proof. 1. It suffices to prove the inclusion for the generators of IJ, namely products xy with $x \in I$ and $y \in J$. Since I and J are ideals, we obtain:

$$x \in I \implies xy \in I$$
$$y \in J \implies xy \in J$$

and thus $xy \in I \cap J$.

2. By the assumption $I + J = (1)$, we can write $1 = i + j$ for some $i \in I$ and $j \in J$. Now let $a \in I \cap J$; we want to show $a \in IJ$. Writing

$$a = a \cdot 1 = a(i + j) = \overbrace{ai}^{\in IJ} + \overbrace{aj}^{\in IJ},$$

both terms lie in IJ:

$$a \in J \implies ai \in IJ$$
$$a \in I \implies aj \in IJ$$

and thus $a \in IJ$. □

Example 6.3.2. In Example 6.2.6, we saw the strict inclusion of ideals in $\mathbb{Z}$

$$(60) = (6)(10) \subsetneq (6) \cap (10) = (30).$$

Just for fun, a few more examples:

$$(24) = (4)(6) \subsetneq (4) \cap (6) = (12)$$

$$(9) = (3)(3) \subsetneq (3) \cap (3) = (3).$$

Definition 6.3.3. Two ideals $I, J \subseteq R$ are **coprime** if they together generate the whole ring:

$$I + J = (1) = R.$$

Example 6.3.4. In $\mathbb{Z}$, two nontrivial ideals (m) and (n) are coprime if and only if the numbers m and n are coprime, i.e., $\gcd(m, n) = 1$.

6.4 Generalized Chinese remainder theorem

Recall a few facts about the product of rings.

Definition 6.4.1. The **product** of rings R and S is the Cartesian product $R \times S$ endowed with the coordinatewise addition and multiplication:

$$(r, s) + (r', s') = (r + r', s + s')$$
$$(r, s)(r', s') = (rr', ss').$$

Lemma 6.4.2. *1. The definition of the product makes $R \times S$ into a ring, and the projection maps*

$$\begin{cases} p_R \colon R \times S \twoheadrightarrow R \\ p_S \colon R \times S \twoheadrightarrow S \end{cases}$$

into ring homomorphisms.

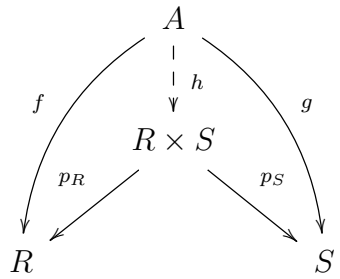
2. The product $R \times S$ is unital if and only if R and S are unital, in which case the unit is coordinatewise:

$$1_{R \times S} = (1_R, 1_S).$$

3. The product $R \times S$ is commutative if and only if R and S are commutative.

The next statement says that the product of rings is indeed the product of rings (in the categorical sense).

Proposition 6.4.3. *The product of rings $R \times S$ satisfies the following universal property. Given ring homomorphisms $f \colon A \to R$ and $g \colon A \to S$, there exists a unique ring homomorphism $h \colon A \to R \times S$ satisfying $p_R \circ h = f$ and $p_S \circ h = g$, as illustrated in the diagram*



This unique h is denoted $h = (f, g)$.

Remark 6.4.4. The product of an infinite family of rings $\prod_{\alpha \in \Lambda} R_\alpha$ is defined similarly and satisfies the same universal property. In other words, a ring homomorphism

$$A \to \prod_{\alpha \in \Lambda} R_\alpha$$

is the same data as a family of ring homomorphisms $f_\alpha \colon A \to R_\alpha$ for $\alpha \in \Lambda$.

Recall the following:

Theorem 6.4.5 (Classic Chinese remainder theorem)**.** *Let $n \in \mathbb{Z}$ be factored as $n = n_1 \cdots n_k$ where the numbers n_i are pairwise coprime. Then the ring homomorphism*

$$\varphi\colon \mathbb{Z}/n \xrightarrow{\cong} \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_k$$

is an isomorphism, where φ has as i^{th} coordinate the quotient map $q_{n_i}\colon \mathbb{Z}/n \twoheadrightarrow \mathbb{Z}/n_i$.

Example 6.4.6. 1. The factorization $12 = 3 \cdot 4$ yields the ring isomorphism

$$\mathbb{Z}/12 \xrightarrow[\cong]{(q_3,q_4)} \mathbb{Z}/3 \times \mathbb{Z}/4.$$

2. As a non-example, observe that the ring homomorphism

$$\mathbb{Z}/4 \xrightarrow{(q_2,q_2)} \mathbb{Z}/2 \times \mathbb{Z}/2$$

is not an isomorphism. In fact, the two sides are not even isomorphic as abelian groups.

Our next goal is to generalize that theorem to ideals rather than numbers.

Proposition 6.4.7. *Let R be a commutative ring and $I_1, \ldots, I_n \subseteq R$ ideals. Consider the ring homomorphism*

$$\varphi\colon R \to R/I_1 \times \cdots \times R/I_n$$

whose i^{th} coordinate is the quotient map $q_{I_i}\colon R \twoheadrightarrow R/I_i$.

1. *If the ideals $I_1, \ldots, I_n$ are pairwise coprime, then their product agrees with their intersection:*
$$\prod_{i=1}^{n} I_i = \bigcap_{i=1}^{n} I_i.$$
2. *The map φ is surjective if and only if the I_i are pairwise coprime.*
3. *The map φ is injective if and only if $\bigcap_{i=1}^{n} I_i = (0)$ holds.*

Proof. See [AM69, Proposition 1.10]. □

Corollary 6.4.8 (Generalized Chinese remainder theorem)**.** *Let R be a commutative ring and $I_1, \ldots, I_n \subseteq R$ ideals that are pairwise coprime. Then the ring homomorphism*

$$\varphi\colon R/(I_1 \cdots I_n) \xrightarrow{\cong} R/I_1 \times \cdots \times R/I_n$$

is an isomorphism.

The case $n = 2$ reads as follows.

Corollary 6.4.9. *Let R be a commutative ring and $I, J \subseteq R$ coprime ideals. Then the ring homomorphism*

$$(q_I, q_J)\colon R/(IJ) \xrightarrow{\cong} R/I \times R/J$$

is an isomorphism.

Exercise 6.4.10. Use Corollary 6.4.9 to produce an isomorphism of rings

$$\mathbb{Z}[x]/(x^2 - 5x + 6) \xrightarrow{\cong} \mathbb{Z} \times \mathbb{Z}$$

(Homework 4 Problem 3).

Remark 6.4.11. The condition that ideals be pairwise coprime means that for all indices $i \neq j$, the ideals I_i and I_j are coprime, i.e., $I_i + I_j = (1)$. That condition is stronger than the ideals being "jointly coprime", in the sense that they jointly generate the whole ring:

$$I_1 + \cdots + I_n = (1).$$

Example 6.4.12. The numbers $2, 3, 4 \in \mathbb{Z}$ are "jointly coprime", in fact 2 and 3 already generate all of $\mathbb{Z}$:

$$(2) + (3) + (4) = (2, 3, 4) = (2, 3) = (1).$$

However, $2, 3, 4$ are not *pairwise* coprime, since 2 and 4 are not coprime.

Example 6.4.13. For a more striking example, the numbers $6, 10, 15$ are "jointly coprime":

$$(6, 10, 15) = (\gcd(6, 10, 15)) = (1) = \mathbb{Z},$$

yet none of the pairs are coprime:

$$(6, 10) = (2)$$
$$(6, 15) = (3)$$
$$(10, 15) = (5).$$

6.5 Prime avoidance

Recall that for a prime element $p \in R$ in a commutative ring R, we have the implication

$$p \mid n_1 \cdots n_k \implies p \mid n_i \text{ for some } i.$$

More generally, for a prime ideal $P \subset R$, we have the implication

$$n_1 \cdots n_k \in P \implies n_i \in P \text{ for some } i.$$

Let us generalize this conclusion to products of ideals.

Proposition 6.5.1. *Let R be a commutative ring, $I_1, \ldots, I_n \subseteq R$ ideals, and $P \subset R$ a prime ideal containing the product of the I_i:*

$$\prod_{i=i}^{n} I_i \subseteq P.$$

Then $I_i \subseteq P$ holds for some index i.

If moreover $P = \bigcap_{i=1}^{n} I_i$ holds, then $P = I_i$ holds for some index i.

Proof. Let us show the contrapositive. Assume $I_i \nsubseteq P$ for all i and pick an element $x_i \in I_i \setminus P$ for each index i. Then the product of those elements

$$x_1 \cdots x_n \in \prod_{i=i}^{n} I_i$$

is not in P, since each factor x_i is not in P:

$$x_i \notin P \text{ for all } i \implies x_1 \cdots x_n \notin P.$$

This shows $\prod_{i=i}^{n} I_i \nsubseteq P$.

For the second part, the first part gave us $I_i \subseteq P$ for some index i. The reverse inclusion follows from the assumption:

$$P = \bigcap_{j=1}^{n} I_j \subseteq I_i. \qquad \square$$

Proposition 6.5.2 (Prime avoidance lemma)**.** *Let R be a commutative ring, $P_1, \ldots, P_n \subseteq R$ prime ideals, and $I \subset R$ an ideal contained in the union of the P_i:*

$$I \subseteq \bigcup_{i=i}^{n} P_i.$$

Then $I \subseteq P_i$ holds for some index i.

Proof. See [AM69, Proposition 1.11]. $\square$

7 Ideal quotients and radicals

7.1 Ideal quotients

Definition 7.1.1. Let R be a commutative ring and $I, J \subseteq R$ ideals. The **ideal quotient** of I by J is

$$(I : J) = \{r \in R \mid rJ \subseteq I\}.$$

Lemma 7.1.2. *The ideal quotient $(I : J) \subseteq R$ is an ideal.*

Remark 7.1.3. The inclusion $I \subseteq (I : J)$ always holds.

Definition 7.1.4. The **annihilator** of an ideal $J \subseteq R$ is the ideal

$$\mathrm{Ann}(J) = (0 : J) = \{r \in R \mid rJ = 0\}.$$

Example 7.1.5. In the ring $\mathbb{Z}/12$, here are a few annihilators of elements:

$$\mathrm{Ann}(3) = (4)$$
$$\mathrm{Ann}(2) = (6)$$
$$\mathrm{Ann}(5) = (0).$$

More generally, consider the ring $\mathbb{Z}/n$ for $n \geq 2$. The annihilator of an element $m \in \mathbb{Z}/n$ is the principal ideal

$$\mathrm{Ann}(m) = \left(\frac{n}{\gcd(m, n)}\right).$$

Remark 7.1.6. In an integral domain R, the annihilator of any non-zero element $x \in R$ is trivial: $\mathrm{Ann}(x) = (0)$.

More generally, in any commutative ring R, the set of zero-divisors is

$$\begin{aligned} D &= \{y \in R \mid \text{there is } x \neq 0 \text{ satisfying } xy = 0\} \\ &= \bigcup_{x \neq 0} \mathrm{Ann}(x). \end{aligned}$$

Example 7.1.7. In the ring $\mathbb{Z}$, here are a few ideal quotients:

$$(6 : 2) = (3)$$
$$(6 : 5) = (6)$$
$$(6 : 10) = (3).$$

Let us generalize those examples.

Proposition 7.1.8. *For integers $m, n \neq 0$, the ideal quotient of n by m is the principal ideal*

$$(n : m) = \left(\frac{n}{\gcd(m, n)}\right).$$

Proof. Consider the equivalent conditions on an integer $k \in \mathbb{Z}$:

$$\begin{aligned}
& k \in (n : m) \\
\iff & k \cdot (m) \subseteq (n) \\
\iff & km \subseteq (n) \\
\iff & n \mid km \\
\iff & \frac{n}{d} \mid k\frac{m}{d} \qquad \text{where } d = \gcd(m, n) \\
\iff & \frac{n}{d} \mid k \qquad \text{since } \gcd(\frac{m}{d}, \frac{n}{d}) = 1 \\
\iff & k \in \left(\frac{n}{d}\right)
\end{aligned}$$

which proves the claim. □

Example 7.1.9. Let R be an integral domain. In the polynomial ring $R[x, y]$, let us compute the ideal quotient

$$\big(x^2 : (x, y)\big) = (x^2).$$

To prove the equality, consider the equivalent conditions on a polynomial $f \in R[x, y]$:

$$\begin{aligned}
& f \in \big(x^2 : (x, y)\big) \\
\iff & f \cdot (x, y) \subseteq (x^2) \\
\iff & fx \in (x^2) \text{ and } fy \in (x^2) \\
\iff & x^2 \mid fx \text{ and } x^2 \mid fy \\
\iff & x \mid f \text{ and } x^2 \mid f \\
\iff & x^2 \mid f \\
\iff & f \in (x^2).
\end{aligned}$$

Exercise 7.1.10. Let R be a commutative ring, $I \subseteq R$ an ideal and $J_\alpha \subseteq R$ a family of ideals (indexed by $\alpha \in \Lambda$). Then we have the ideal quotient

$$\left(I : \sum_{\alpha \in \Lambda} J_\alpha\right) = \bigcap_{\alpha \in \Lambda} (I : J_\alpha)$$

[AM69, Exercise 1.12].

Remark 7.1.11. We can revisit Example 7.1.9 in light of Exercise 7.1.10:

$$\begin{aligned}
\big(x^2 : (x, y)\big) &= \big(x^2 : (x) + (y)\big) \\
&= (x^2 : x) \cap (x^2 : y) \\
&= (x) \cap (x^2) \\
&= (x^2).
\end{aligned}$$

7.2 The radical of an ideal

Definition 7.2.1. Let R be a commutative ring.

1. An $\boldsymbol{n^{\text{th}}}$ **root** of an element $a \in R$ is an element $x \in R$ satisfying $x^n = a$.
2. The **radical** of an ideal $I \subseteq R$ is the set of all roots of elements of I, denoted:
$$\operatorname{rad}(I) = \{x \in R \mid x^n \in I \text{ for some } n \geq 1\}.$$
The radical of I is also denoted $\sqrt{I} = \operatorname{rad}(I)$.
3. An ideal $I \subseteq R$ is **radical** if it contains all of its roots:
$$I = \operatorname{rad}(I),$$
in other words, the following implication holds:
$$x^n \in I \text{ for some } n \geq 1 \implies x \in I.$$

Remark 7.2.2. 1. The inclusion $I \subseteq \operatorname{rad}(I)$ always holds.

2. The formation of radicals preserves inclusions:
$$I \subseteq J \implies \operatorname{rad}(I) \subseteq \operatorname{rad}(J).$$

A bit of definition chasing shows the following:

Lemma 7.2.3. *Let $I \subseteq R$ be an ideal.*

1. *The radical of I consists of the elements that become nilpotent in the quotient ring R/I:*
$$\operatorname{rad}(I) = q^{-1}(\operatorname{nil}(R/I))$$
where $q\colon R \twoheadrightarrow R/I$ denotes the quotient map.
In particular, $\operatorname{rad}(I)$ *is an ideal.*
2. *The ideal I is radical if and only if the quotient ring R/I is reduced.*

Lemma 7.2.4. *Let $I \subseteq R$ be an ideal. The radical* $\operatorname{rad}(I)$ *is the smallest radical ideal containing I. Explicitly:*

1. *The radical* $\operatorname{rad}(I)$ *is radical.*
In other words, the equality $\operatorname{rad}(\operatorname{rad}(I)) = \operatorname{rad}(I)$ *always holds.*
2. *If $J \subseteq R$ is a radical ideal containing I, then the inclusion* $\operatorname{rad}(I) \subseteq J$ *holds.*

Proof. 1. Consider the quotient ring

$$\begin{aligned} R/\operatorname{rad}(I) &= R/q^{-1}(\operatorname{nil}(R/I)) && \text{by Lemma 7.2.3} \\ &\cong (R/I)/\operatorname{nil}(R/I) && \text{by the third isomorphism theorem} \\ &= (R/I)_{\text{red}}, \end{aligned}$$

which is reduced. Hence the ideal $\operatorname{rad}(I)$ is radical, by Lemma 7.2.3.

2. Let $J \subseteq R$ be a radical ideal containing I and let $x \in \operatorname{rad}(I)$, i.e., $x^n \in I$ holds for some $n \geq 1$. Then we have

$$\begin{aligned} & x^n \in I \subseteq J \\ \implies & x \in J \end{aligned}$$

since J is radical. □

Example 7.2.5. In the ring $\mathbb{Z}$, here are a few examples of radicals:

$$\begin{aligned} \operatorname{rad}(9) &= \operatorname{rad}(3^2) = (3) \\ \operatorname{rad}(24) &= \operatorname{rad}(2^3 \cdot 3) = (2 \cdot 3) = (6) \\ \operatorname{rad}(42) &= \operatorname{rad}(2 \cdot 3 \cdot 7) = (2 \cdot 3 \cdot 7) = (42). \end{aligned}$$

More generally, given a prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$, the radical of (n) is

$$\operatorname{rad}(n) = \operatorname{rad}(p_1^{e_1} \cdots p_k^{e_k}) = (p_1 \cdots p_k).$$

Thus the ideal (n) is radical if an only if n is a product of *distinct* prime factors.

Example 7.2.6. For k a field, consider the polynomial ring $k[x]$. Here are a few examples of radicals:

$$\begin{aligned} \operatorname{rad}(x^2 + 6x + 9) &= \operatorname{rad}\left((x+3)^2\right) = (x+3) \\ \operatorname{rad}\left((x-5)^3(x+8)\right) &= \left((x-5)(x+8)\right). \end{aligned}$$

More generally, given a factorization of a polynomial p into irreducible factors $p = p_1^{e_1} \cdots p_k^{e_k}$, the radical of (p) is

$$\operatorname{rad}(p) = \operatorname{rad}(p_1^{e_1} \cdots p_k^{e_k}) = (p_1 \cdots p_k).$$

Thus the ideal (p) is radical if an only if p is a product of *distinct* irreducible factors.

Note that the factorization of a polynomial p depends on the field k. In $\mathbb{Q}[x]$, we have

$$\operatorname{rad}(x^2 + 1) = (x^2 + 1)$$

whereas in $\mathbb{F}_2[x]$, we have

$$\operatorname{rad}(x^2 + 1) = \left((x+1)^2\right) = (x+1).$$

Example 7.2.7. In the polynomial ring $k[x, y]$, we have the radical

$$\operatorname{rad}\left((y - x^2)(x - 5)^3\right) = \left((y - x^2)(x - 5)\right).$$

Lemma 7.2.8. *Every prime ideal $P \subset R$ is radical.*

Proof. Assume $x^n \in P$ holds for some $n \geq 1$. Since P is prime, one of the factors must lie in P, which implies $x \in P$. Hence P is radical. □

Proposition 7.2.9. *For any ideal $I \subseteq R$, the radical of I is the intersection of the prime ideals containing I:*

$$\operatorname{rad}(I) = \bigcap_{\substack{P \subset R \text{ prime} \\ I \subseteq P}} P.$$

Proof. Let $q\colon R \twoheadrightarrow R/I$ denote the quotient map. By Lemma 7.2.3, the radical is:

$$\begin{aligned}
\operatorname{rad}(I) &= q^{-1}\left(\operatorname{nil}(R/I)\right) \\
&= q^{-1}\left(\bigcap_{Q \subset R/I \text{ prime}} Q\right) \\
&= \bigcap_{Q \subset R/I \text{ prime}} q^{-1}(Q) \\
&= \bigcap_{\substack{P \subset R \text{ prime} \\ I \subseteq P}} P.
\end{aligned}$$

□

Proposition 7.2.10. *1. For any ideals $I, J \subseteq R$, the radical of the product is*

$$\operatorname{rad}(IJ) = \operatorname{rad}(I \cap J) = \operatorname{rad}(I) \cap \operatorname{rad}(J).$$

2. For $n \geq 1$, we have

$$\operatorname{rad}(I^n) = \operatorname{rad}(I).$$

In particular, if I is radical, then $\operatorname{rad}(I^n) = I$.

Proof. 1. The first equality is left as an exercise [AM69, Exercise 1.13(iii)].

Let us prove the second equality $\operatorname{rad}(I \cap J) = \operatorname{rad}(I) \cap \operatorname{rad}(J)$.

($\subseteq$) The inclusion $I \cap J \subseteq I$ yields $\operatorname{rad}(I \cap J) \subseteq \operatorname{rad}(I)$ and likewise $\operatorname{rad}(I \cap J) \subseteq \operatorname{rad}(J)$, which gives

$$\operatorname{rad}(I \cap J) \subseteq \operatorname{rad}(I) \cap \operatorname{rad}(J).$$

($\supseteq$) Let $x \in \operatorname{rad}(I) \cap \operatorname{rad}(J)$. The conditions $x \in \operatorname{rad}(I)$ and $x \in \operatorname{rad}(J)$ mean

$$\begin{cases} x^m \in I & \text{for some } m \geq 1 \\ x^n \in J & \text{for some } n \geq 1. \end{cases}$$

Taking the higher exponent $N = \max\{m, n\}$, we obtain $x^N \in I \cap J$, which shows $x \in \operatorname{rad}(I \cap J)$.

2. By part (1), the radical of a power is

$$\begin{aligned} \operatorname{rad}(I^n) &= \operatorname{rad}(\overbrace{II \cdots I}^{n \text{ times}}) \\ &= \operatorname{rad}(I) \cap \operatorname{rad}(I) \cap \cdots \cap \operatorname{rad}(I) \\ &= \operatorname{rad}(I). \end{aligned}$$

□

In Example 7.2.5, we saw that a product of *distinct* prime elements generates a radical ideal. This fact can be generalized as follows.

Proposition 7.2.11. *Let R be a unique factorization domain (UFD). Given a prime factorization $f = p_1^{e_1} \cdots p_k^{e_k}$, the radical of the principal ideal (f) is*

$$\operatorname{rad}(f) = \operatorname{rad}(p_1^{e_1} \cdots p_k^{e_k}) = (p_1 \cdots p_k).$$

Thus the ideal (f) is radical if an only if f is a product of distinct *prime factors.*

Proof. Using Proposition 7.2.10, we compute the radical of the product:

$$\begin{aligned} \operatorname{rad}(f) &= \operatorname{rad}(p_1^{e_1} \cdots p_k^{e_k}) \\ &= \operatorname{rad}\left((p_1^{e_1}) \cdots (p_k^{e_k})\right) \\ &= \operatorname{rad}(p_1^{e_1}) \cap \cdots \cap \operatorname{rad}(p_k^{e_k}) \\ &= (p_1) \cap \cdots \cap (p_k) \\ &= (\operatorname{lcm}(p_1, \ldots, p_k)) \\ &= (p_1 \cdots p_k). \end{aligned}$$

The last equality relies on the p_i being distinct prime elements in a UFD. □

The situation with non-principal ideals is more delicate.

Example 7.2.12. For k a field, the polynomial ring $k[x, y]$ is a UFD. The prime ideals (x) and (x, y) are distinct, yet their product is not radical:

$$\begin{aligned} \operatorname{rad}\left((x)(x, y)\right) &= \operatorname{rad}(x) \cap \operatorname{rad}(x, y) \qquad \text{by Proposition 7.2.10} \\ &= (x) \cap (x, y) \qquad \text{by Lemma 7.2.8} \\ &= (x). \end{aligned}$$

One can also check directly the equality

$$\operatorname{rad}\left((x)(x, y)\right) = \operatorname{rad}(x^2, xy) = (x).$$

Note that $(x)(x, y)$ is a product of distinct prime ideals, but is not radical.

8 Extension and contraction

8.1 Definitions and basic properties

Definition 8.1.1. Let $f\colon R \to S$ be a ring homomorphism.

1. Given an ideal $I \subseteq R$, its **extension** along f is the ideal in S generated by the image $f(I)$, denoted
$$I^e = (f(I)) = Sf(I) \subseteq S.$$
2. Given an ideal $J \subseteq S$, its **contraction** along f is the preimage
$$J^c = f^{-1}(J) \subseteq R,$$
which is an ideal in R.

Lemma 8.1.2. *Let $f\colon R \to S$ be a ring homomoprhism.*

1. *Extension and contraction are order-preserving with respect to inclusion:*
$$\begin{cases} I_1 \subseteq I_2 \subseteq R \implies I_1^e \subseteq I_2^e \\ J_1 \subseteq J_2 \subseteq S \implies J_1^c \subseteq J_2^c. \end{cases}$$
2. *Extension and contraction preserve the two extreme cases, namely the trivial ideal* 0 *and the whole ring:*
$$\begin{cases} (0)^e = S \quad \textit{and} \quad R^e = S \\ (0)^c = R \quad \textit{and} \quad S^c = R. \end{cases}$$
3. *Given generators for an ideal $I = (g_1, \ldots, g_r)$, the extension I^e has generators*
$$I^e = (f(g_1), \ldots, f(g_r)).$$

Example 8.1.3. Consider the quotient map $q\colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/6$. Taking the ideal $I = (10) \subset \mathbb{Z}$, its extension along q is
$$I^e = (q(10)) = (\overline{10}) = (\overline{2}) \subset \mathbb{Z}/6,$$
whose contraction is
$$I^{ec} = q^{-1}\left((\overline{2})\right) = (2) \subset \mathbb{Z}.$$
More generally, for any $a \in \mathbb{Z}$, the principal ideal (a) has extension
$$(a)^e = (\overline{a}) = (\overline{\gcd(a,6)}) \subset \mathbb{Z}/6,$$
whose contraction is
$$(a)^{ec} = q^{-1}\left((\overline{\gcd(a,6)})\right) = (\gcd(a,6)) \subset \mathbb{Z}.$$

By the correspondence in Proposition 1.3.10, the previous example generalizes as follows.

Example 8.1.4. Let $K \subseteq R$ be an ideal and $q\colon R \twoheadrightarrow R/K$ the quotient map. For any ideal $I \subseteq R$, extending along q and then contracting yields

$$I^{ec} = q^{-1}\left((q(I)\right) = I + K \subseteq R.$$

For any ideal $J \subseteq R/K$, contracting along q and then extending yields

$$J^{ce} = \big(q(q^{-1}(J))\big) = (J) = J.$$

Recall from Remark 1.3.5 that any ring homomorphism $f\colon R \to S$ factors as a quotient map followed by an inclusion of a subring, namely the image of f:

$$R \xrightarrow{f'} \operatorname{im}(f) \xhookrightarrow{\text{inc}} S.$$

Example 8.1.4 tells us what happens for the first step $R \twoheadrightarrow \operatorname{im}(f)$.

Upshot: Extension and contraction is more interesting for the inclusion of a subring $R \subset S$. In that case, the contraction of an ideal $J \subseteq S$ is the ideal $J \cap R \subseteq R$.

8.2 Examples with fractions

Example 8.2.1. Consider the inclusion of subring $\mathbb{Z} \subset \mathbb{Q}$. For any non-trivial ideal $(n) \subseteq \mathbb{Z}$, its extension is

$$(n)^e = \mathbb{Q}$$

since $n \in \mathbb{Q}$ is invertible. Going backwards, the only non-trivial ideal $J \subseteq \mathbb{Q}$ is $(1) = \mathbb{Q}$, whose contraction is $\mathbb{Q} \cap \mathbb{Z} = \mathbb{Z}$.

The story becomes more exciting if we only invert *some* of the primes in $\mathbb{Z}$ instead of inverting them all. To that effect, let us introduce some terminology.

Definition 8.2.2. Let $p \in \mathbb{Z}$ be a prime. The ***p*-adic valuation** of a non-zero integer $n \in \mathbb{Z}$ is the exponent of p in the prime factorization of n, denoted

$$\nu_p(n) = \max\{k \geq 0 \mid p^k \mid n\}.$$

It is convenient to adopt the convention $\nu_p(0) = +\infty$.

Example 8.2.3. Consider the integer $n = 120 = 8 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5$. Its p-adic valuation for various primes p is given by

$$\begin{cases} \nu_2(120) = 3 \\ \nu_3(120) = 1 \\ \nu_5(120) = 1 \\ \nu_p(120) = 0 \quad \text{for any prime } p \geq 7. \end{cases}$$

Example 8.2.4. Let $p \in \mathbb{Z}$ be a prime. Consider the rational numbers that only have a power of p in the denominator:

$$\mathbb{Z}[\frac{1}{p}] = \left\{ \frac{a}{p^k} \in \mathbb{Q} \mid a \in \mathbb{Z},\ k \geq 0 \right\}.$$

Consider the inclusion map

$$\iota \colon \mathbb{Z} \hookrightarrow \mathbb{Z}[\frac{1}{p}]$$
$$\iota(a) = \frac{a}{1}.$$

For any non-trivial ideal $(n) \subseteq \mathbb{Z}$, its extension is

$$(n)^e = (\frac{n}{1}) = (\frac{n}{p^{\nu_p(n)}}) \subseteq \mathbb{Z}[\frac{1}{p}]$$

since $p \in \mathbb{Z}[\frac{1}{p}]$ is now invertible. Taking the contraction yields

$$(n)^{ec} = (\frac{n}{p^{\nu_p(n)}}) \subseteq \mathbb{Z}.$$

Going backwards, for any ideal $J \subseteq \mathbb{Z}[\frac{1}{p}]$, contracting then extending yields

$$J^{ce} = (J \cap \mathbb{Z}) = J.$$

Example 8.2.5. Take $p = 2$ and consider the inclusion map $\iota\colon \mathbb{Z} \hookrightarrow \mathbb{Z}[\frac{1}{2}]$. Taking the ideal $I = (120) \subset \mathbb{Z}$, its extension along ι is

$$(120)^e = (\frac{120}{1}) = (\frac{120}{8}) = (\frac{15}{1}) \subset \mathbb{Z}[\frac{1}{2}],$$

whose contraction is

$$(120)^{ec} = (\frac{15}{1}) \cap \mathbb{Z} = (15) \subset \mathbb{Z}.$$

Example 8.2.6. Now consider the p-local integers

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \mid p \nmid b \right\}.$$

as in Example 5.1.5, along with the inclusion map $\iota\colon \mathbb{Z} \hookrightarrow \mathbb{Z}_{(p)}$. For any non-trivial ideal $(n) \subseteq \mathbb{Z}$, its extension is

$$(n)^e = (\frac{n}{1}) = (\frac{p^{\nu_p(n)}}{1}) \subseteq \mathbb{Z}_{(p)}$$

since all the primes *other than* p are now invertible in $\mathbb{Z}_{(p)}$. Taking the contraction yields

$$(n)^{ec} = (p^{\nu_p(n)}) \subseteq \mathbb{Z}.$$

Going backwards, for any ideal $J \subseteq \mathbb{Z}_{(p)}$, contracting then extending yields

$$J^{ce} = (J \cap \mathbb{Z}) = J.$$

Example 8.2.7. Again take $p = 2$ and consider the inclusion map $\iota\colon \mathbb{Z} \hookrightarrow \mathbb{Z}_{(2)}$. Taking the ideal $I = (120) \subset \mathbb{Z}$, its extension along ι is

$$(120)^e = (\frac{120}{1}) = (\frac{120}{15}) = (\frac{8}{1}) \subset \mathbb{Z}_{(2)},$$

whose contraction is

$$(120)^{ec} = (\frac{120}{1}) \cap \mathbb{Z} = (8) \subset \mathbb{Z}.$$

Remark 8.2.8. In Chapter 3, we will see that $\mathbb{Z}[\frac{1}{p}]$, the p-local integers $\mathbb{Z}_{(p)}$, and the fraction field $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$ are localizations of $\mathbb{Z}$.

The ring $\mathbb{Z}[\frac{1}{p}]$ is sometimes called the "p-inverted integers", the "localization of $\mathbb{Z}$ by the element p", the "localization of $\mathbb{Z}$ away from p", or "$\mathbb{Z}$ adjoin p inverse". Note the prepositions! The localization of $\mathbb{Z}$ *away from* p, which is $\mathbb{Z}[\frac{1}{p}]$, is very different from the localization of $\mathbb{Z}$ *at* p, which is $\mathbb{Z}_{(p)}$.

Remark 8.2.9. The ring of p-local integers $\mathbb{Z}_{(p)}$ with the p-adic valuation ν_p is an example of *discrete valuation ring*, cf. Remark 3.2.9.

8.3 Examples with polynomials

Example 8.3.1. Consider the polynomial ring $\mathbb{Z}[x]$ and the subring $\mathbb{Z} \subset \mathbb{Z}[x]$ of constant polynomials. Taking the principal ideal $(x-5) \subset \mathbb{Z}[x]$, its contraction is

$$\begin{aligned}(x-5)^c &= (x-5) \cap \mathbb{Z} \\ &= \{(x-5)f \mid f \in \mathbb{Z}[x]\} \cap \mathbb{Z} \\ &= 0.\end{aligned}$$

Indeed, looking at the degree of the polynomial

$$\deg\left((x-5)f\right) = \deg(x-5) + \deg(f) = \deg(f) + 1,$$

the only way to obtain a *constant* polynomial $(x-5)f$ is by taking $f = 0$.

As another example, take the (non-principal) ideal $J = (x-1, x-5) \subset \mathbb{Z}[x]$. To compute its contraction, let us pick more convenient generators:

$$(x-1, x-5) = (x-1, x-1-(x-5)) = (x-1, 4).$$

The contraction is

$$J^c = (x-1, 4)^c = (4) \subset \mathbb{Z}.$$

Showing (a variant of) this is the content of Homework 5 Problem 2.

Proposition 8.3.2. *Let R be a commutative ring and consider the inclusion $R \subset R[x]$ viewing R as the subring of constant polynomials. Let $I \subseteq R$ be an ideal.*

1. *The extension of I is the ideal of polynomials with coefficients in I:*

$$I^e = I[x] := \left\{ \sum_{i=0}^{n} c_i x^i \in R[x] \mid c_i \in I \text{ for all } i \right\} \subseteq R[x].$$

2. *Extending then contracting I yields I again:*

$$I^{ec} = I.$$

Proof. Homework 5 Problem 3. □

8.4 Going back and forth

Proposition 8.4.1. *Let $f\colon R \to S$ be a ring homomorphism. For any ideals $I \subseteq R$ and $J \subseteq S$, extension and contraction along f satisfy the following:*

1. $I \subseteq I^{ec}$
2. $J^{ce} \subseteq J$
3. $I^{ece} = I^e$
4. $J^{cec} = J^c$.

Proof. 1. Consider the inclusions of subsets of R:

$$I \subseteq f^{-1}(f(I)) \subseteq f^{-1}(I^e) = I^{ec}.$$

2. Consider the inclusion of subsets of S

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

Taking ideals generated by the subsets, we deduce

$$(f(J^c)) = J^{ce} \subseteq J.$$

3. Applying extension to the inclusion $I \subseteq I^{ec}$ yields

$$I^e \subseteq I^{ece}.$$

On the other hand, applying part (2) to the ideal $J = I^e$ yields

$$I^{ece} \subseteq I^e,$$

hence the equality $I^{ece} = I^e$. The same argument works for part (4). □

Remark 8.4.2. The inclusions in Proposition 8.4.1 are strict in general.

As in Example 8.2.7, consider the inclusion map $\mathbb{Z} \hookrightarrow \mathbb{Z}_{(2)}$, and take the ideal $I = (6) \subset \mathbb{Z}$. Extending then contracting yields

$$(6)^{ec} = (2) \supset (6).$$

As in Example 8.3.1, consider the subring $R \subset R[x]$, and take the ideal $J = (x) \subset R[x]$. Contracting then extending yields

$$(x)^{ce} = (0)^e = (0) \subset (x).$$

Corollary 8.4.3. *Extension and contraction induce a bijection*

$$\begin{array}{ccc} \{\textit{contracted ideals of } R\} & \underset{\text{contraction}}{\overset{\text{extension}}{\underset{\cong}{\rightleftarrows}}} & \{\textit{extended ideals of } S\} \\ \| & & \| \\ \{I \subseteq R \mid I^{ec} = I\} & & \{J \subseteq S \mid J^{ce} = J\}. \end{array}$$

8.5 Gaussian integers

The inclusion $\mathbb{Z} \subset \mathbb{Z}[i]$ of the integers into the Gaussian integers provides interesting examples of extension and contraction.

Definition 8.5.1. The **norm** of a Gaussian rational $a + bi \in \mathbb{Q}[i]$ is

$$\boxed{N(a+bi) = a^2 + b^2} \in \mathbb{Q}.$$

Where does the formula come from? The norm of $z = a + bi$ is the determinant of the $\mathbb{Q}$-linear transformation

$$\lambda_z \colon \mathbb{Q}[i] \to \mathbb{Q}[i]$$

given by multiplication by z. Indeed, using the standard basis $\{1, i\}$ of $\mathbb{Q}[i]$ as a $\mathbb{Q}$-vector space, the linear transformation λ_z has representing matrix

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix},$$

whose determinant is $a^2 - (-b^2) = a^2 + b^2$.

Warning 8.5.2. The norm in the sense of algebraic number theory (as above), also called a *field norm*, is not a norm in the sense of *normed vector spaces*. The norm of $z \in \mathbb{Q}[i]$ is the square of the usual Euclidean norm: $N(z) = \|z\|^2$.

Now we focus on Gaussian integers $a + bi \in \mathbb{Z}[i]$, in which case the norm is an integer $a^2 + b^2 \in \mathbb{Z}$.

Lemma 8.5.3. *A Gaussian integer $z \in \mathbb{Z}[i]$ has norm 1 if and only if z is a unit:*

$$N(z) = 1 \iff z \in \mathbb{Z}[i]^\times.$$

Proof. Consider the equivalent conditions on a Gaussian integer $z = a + bi$:

$$\begin{aligned} & N(z) = a^2 + b^2 = 1 \\ \iff & (a, b) = (\pm 1, 0) \quad \text{or} \quad (a, b) = (0, \pm 1) \\ \iff & z \in \{1, -1, i, -i\} = \mathbb{Z}[i]^\times. \end{aligned}$$

□

Proposition 8.5.4. *A prime number $p \in \mathbb{Z}$ remains irreducible in $\mathbb{Z}[i]$ if and only if p is not a sum of squares $a^2 + b^2$.*

Proof. ($\implies$) Assume that p is a sum of squares $a^2 + b^2$ for some $a, b \in \mathbb{Z}$. This yields a factorization in $\mathbb{Z}[i]$

$$p = a^2 + b^2 = (a + bi)(a - bi).$$

The factorization is non-trivial, i.e., both $a + bi$ and $a - bi$ are non-units, since they have norm

$$N(a + bi) = a^2 + b^2 = p > 1.$$

Thus $p \in \mathbb{Z}[i]$ is reducible.

($\Longleftarrow$) Let $p = xy$ be a factorization in $\mathbb{Z}[i]$. Taking norms yields

$$\begin{aligned} & N(p) = N(xy) \\ \Longleftrightarrow\ & p^2 = N(x)N(y). \end{aligned}$$

By assumption, p is not a sum of squares, which ensures $N(x) \neq p$. The only remaining possible factorization of p^2 is $1 \cdot p^2$, i.e., the numbers $N(x)$ and $N(y)$ must be 1 and p^2. Hence one of x or y is a unit, by Lemma 8.5.3. Thus $p \in \mathbb{Z}[i]$ is irreducible. □

We now interpret those factorizations in terms of extension of ideals.

Example 8.5.5. Consider the subring inclusion $\iota\colon \mathbb{Z} \hookrightarrow \mathbb{Z}[i]$.

1. Taking the ideal $I = (2) \subset \mathbb{Z}$, its extension is

$$\begin{aligned} (2)^e &= (\iota(2)) \\ &= ((1+i)(1-i)) \\ &= (1+i)^2. \end{aligned}$$

   The equality of ideals $(1+i) = (1-i)$ holds since $1+i$ and $1-i$ are associate in $\mathbb{Z}[i]$:

$$i(1-i) = i - i^2 = i - (-1) = 1 + i.$$

   Moreover, the ideal $(1+i) \subset \mathbb{Z}[i]$ is prime. Indeed, the element $1+i \in \mathbb{Z}[i]$ is irreducible since its norm is $N(1+i) = 1^2 + 1^2 = 2$. Hence $1+i$ is prime since $\mathbb{Z}[i]$ is a unique factorization domain.

2. Taking the ideal $I = (5) \subset \mathbb{Z}$, its extension is

$$\begin{aligned} (5)^e &= (\iota(5)) \\ &= ((2+i)(2-i)) \\ &= (2+i)(2-i), \end{aligned}$$

   which is a product of distinct prime ideals.

3. Taking the ideal $I = (3) \subset \mathbb{Z}$, its extension $(3)^e \subset \mathbb{Z}[i]$ is still prime. Indeed, the Gaussian integer $3 \in \mathbb{Z}[i]$ is irreducible by Proposition 8.5.4, since $3 \in \mathbb{Z}$ is not a sum of squares.

Remark 8.5.6. Let us generalize the example $p = 3$. A square can only be congruent to 0 or 1 modulo 4:

$$a^2 \equiv 0 \text{ or } 1 \mod 4 \quad \text{for all } a \in \mathbb{Z}.$$

Hence a sum of squares $a^2 + b^2$ can only be congruent to 0, 1, or 2 modulo 4. If a prime $p \in \mathbb{Z}$ satisfies $p \equiv 3 \mod 4$, then p is not a sum of squares, hence p remains irreducible in $\mathbb{Z}[i]$ by Proposition 8.5.4.

9 Constructions with modules

Throughout these notes, we work with modules over a commutative ring R.

9.1 Product of an ideal with a module

Definition 9.1.1. Let M be an R-module and $I \subseteq R$ an ideal. The **product** of I and M is

$$IM := \left\{ \sum_{i=1}^{n} c_i x_i \mid n \geq 1,\ c_i \in I,\ x_i \in M \right\} \subseteq M.$$

Exercise 9.1.2. Check that $IM \subseteq M$ is a submodule of M.

Example 9.1.3. Consider the polynomial ring $R[x]$ viewed as an R-module, and let $I \subseteq R$ be an ideal. The product of I with the R-module $R[x]$ is

$$I(R[x]) = I[x] = \left\{ \sum_{i=0}^{n} c_i x^i \in R[x] \mid c_i \in I \text{ for all } i \right\}.$$

Example 9.1.4. If I is a principal ideal $I = (a)$, then the submodule in question is

$$\begin{aligned} IM = aM &= \{ax \mid x \in M\} \\ &= \operatorname{im}\left(M \xrightarrow{a} M\right). \end{aligned}$$

Here $M \xrightarrow{a} M$ denotes the endomorphism "multiply by the scalar a", also denoted

$$\lambda_a \colon M \to M$$

if there is a risk of confusion with the element $a \in R$ itself.

Example 9.1.5. Consider the abelian group

$$M = \mathbb{Z} \oplus \mathbb{Z}/9 \oplus \mathbb{Z}/5.$$

The subgroup $5M$ is

$$\begin{aligned} 5M &= 5\mathbb{Z} \oplus \mathbb{Z}/9 \oplus 0 \\ &= \{(5k, b, 0) \in \mathbb{Z} \oplus \mathbb{Z}/9 \oplus \mathbb{Z}/5 \mid k \in \mathbb{Z}\}. \end{aligned}$$

Indeed, any multiple of 5 in M is of that form, and any element of that form is a multiple of 5:

$$\begin{aligned} (5k, b, 0) &= (5k, 5\lambda_5^{-1} b, 5 \cdot 0) \\ &= (5k, 5(2b), 5 \cdot 0) \\ &= 5(k, 2b, 0). \end{aligned}$$

We used the fact that the endomorphism

$$\lambda_5 \colon \mathbb{Z}/9 \xrightarrow{\cong} \mathbb{Z}/9$$

is invertible with inverse $\lambda_5^{-1} = \lambda_2$.

The argument used above can be streamlined using the following fact.

Proposition 9.1.6. *For any ideal $I \subseteq R$ and family of R-modules $\{M_\alpha\}_{\alpha\in\Lambda}$, the following submodules of the direct sum $\bigoplus_{\alpha\in\Lambda} M_\alpha$ are equal:*

$$I(\bigoplus_{\alpha\in\Lambda} M_\alpha) = \bigoplus_{\alpha\in\Lambda} IM_\alpha.$$

Proof. The left-hand side is generated by the subset

$$S = \{c(m_{\alpha_1} + \cdots + m_{\alpha_k}) \mid c \in I,\ k \geq 0,\ \alpha_i \in \Lambda,\ m_{\alpha_i} \in M_{\alpha_i}\}.$$

The right-hand side is generated by the subset

$$T = \{cm_\alpha \mid c \in I,\ \alpha \in \Lambda,\ m_\alpha \in M_\alpha\}.$$

We have $T \subseteq S$. Also, the elements of S

$$c(m_{\alpha_1} + \cdots + m_{\alpha_k}) = cm_{\alpha_1} + \cdots + cm_{\alpha_k}$$

are generated by those of T. Therefore S and T generate the same submodule $\langle S\rangle = \langle T\rangle$. □

9.2 Annihilators

Definition 9.2.1. Let M be an R-module and $N, P \subseteq M$ submodules. Define the subset of R

$$\begin{aligned}(N : P) &:= \{r \in R \mid rP \subseteq N\} \\ &= \{r \in R \mid rp \in N \text{ for all } p \in P\}.\end{aligned}$$

Exercise 9.2.2. Check that $(N : P)$ is an ideal of R.

Definition 9.2.3. The **annihilator**[1] of an R-module M is

$$\begin{aligned}\mathrm{Ann}_R(M) := (0 : M) &= \{r \in R \mid rM = 0\} \\ &= \{r \in R \mid rm = 0 \text{ for all } m \in M\}.\end{aligned}$$

We may write $\mathrm{Ann}(M)$ if the ground ring R is clear from the context.

More generally, for any subset $S \subseteq M$, the annihilator of S is

$$\mathrm{Ann}(S) = \{r \in R \mid rs = 0 \text{ for all } s \in S\}.$$

This is not really a more general notion, because of the following fact.

Exercise 9.2.4. For any R-module M and subset $S \subseteq M$, show that the annihilator of S equals the annihilator of the submodule $\langle S \rangle$ generated by S:

$$\mathrm{Ann}(S) = \mathrm{Ann}(\langle S \rangle).$$

Lemma 9.2.5. *The annihilator of a cyclic R-module R/I is*

$$\mathrm{Ann}(R/I) = I.$$

Proof. Let us check both inclusions separately.

($\supseteq$) Let $i \in I$ and let $\overline{r} \in R/I$ denote the equivalence class of $r \in R$. We have the equality in R/I

$$i \cdot \overline{r} = \overline{ir} = \overline{0}$$

since $ir \in I$ holds. This shows $i \in \mathrm{Ann}(R/I)$.

[1] Also the name of a successful Canadian thrash metal band.

($\subseteq$) Let $r \in \operatorname{Ann}(R/I)$. In particular, r satisfies

$$r \cdot \overline{1} = \overline{r} = \overline{0},$$

so that $r \in I$ holds. □

Example 9.2.6. The annihilator of the abelian group $M = \mathbb{Z}/6 \oplus \mathbb{Z}/14$ is

$$\begin{aligned}
\operatorname{Ann}_{\mathbb{Z}}(\mathbb{Z}/6 \oplus \mathbb{Z}/14) &= \{n \in \mathbb{Z} \mid n(\overline{a}, \overline{b}) = (\overline{0}, \overline{0}) \text{ for all } (\overline{a}, \overline{b}) \in \mathbb{Z}/6 \oplus \mathbb{Z}/14\} \\
&= \{n \in \mathbb{Z} \mid n\overline{a} = \overline{0} \text{ and } n\overline{b} = \overline{0} \text{ for all } \overline{a} \in \mathbb{Z}/6,\ \overline{b} \in \mathbb{Z}/14\} \\
&= \operatorname{Ann}_{\mathbb{Z}}(\mathbb{Z}/6) \cap \operatorname{Ann}_{\mathbb{Z}}(\mathbb{Z}/14) \\
&= (6) \cap (14) \qquad \text{by Lemma 9.2.5} \\
&= (\operatorname{lcm}(6, 14)) \\
&= \boxed{(42)}.
\end{aligned}$$

The argument used in the example is an instance of the following fact.

Proposition 9.2.7. *Let $\{M_\alpha\}_{\alpha \in \Lambda}$ be a family of R-modules.*

1. *The annihilator of the direct sum is the intersection of the annihilators:*

$$\operatorname{Ann}\left(\bigoplus_{\alpha \in \Lambda} M_\alpha\right) = \bigcap_{\alpha \in \Lambda} \operatorname{Ann}(M_\alpha).$$

2. *The annihilator of the product is also the intersection of the annihilators:*

$$\operatorname{Ann}\left(\prod_{\alpha \in \Lambda} M_\alpha\right) = \bigcap_{\alpha \in \Lambda} \operatorname{Ann}(M_\alpha).$$

Proof. See Homework 6 Problem 2. □

Proposition 9.2.8. *Any R-module M is canonically a module over the quotient ring $R/\operatorname{Ann}(M)$.*

Proof. Define the scalar multiplication by $\overline{r} \in R/\operatorname{Ann}(M)$ on M by

$$\overline{r} \cdot m = r \cdot m,$$

which is independent of the choice of representative $r \in R$. Indeed, any other representative is of the form $r' = r + a$ for some $a \in \operatorname{Ann}(M)$, which acts on M by

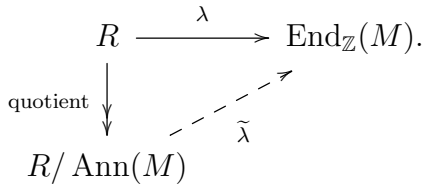
$$\begin{aligned}
r'm &= (r + a)m \\
&= rm + am \\
&= rm = 0 \qquad \text{since } a \in \operatorname{Ann}(M) \\
&= rm.
\end{aligned}$$

The formula $\overline{r} \cdot m$ still satisfies the properties of a scalar multiplication (bilinear, associative, unital), inherited from the same properties for $r \cdot m$. □

Alternate proof. The structure of R-module of M corresponds to a ring homomorphism

$$\lambda\colon R \to \operatorname{End}_{\mathbb{Z}}(M)$$

encoding the scalar multiplication $\lambda(r)(m) = r \cdot m$. By assumption, λ vanishes on the ideal $\operatorname{Ann}(M)$. By the universal property of the quotient ring, there is a unique ring homomorphism $\widetilde{\lambda}\colon R/\operatorname{Ann}(M) \to \operatorname{End}_{\mathbb{Z}}(M)$ making the following diagram commute:



The induced ring homomorphism $\widetilde{\lambda}\colon R/\operatorname{Ann}(M) \to \operatorname{End}_{\mathbb{Z}}(M)$ corresponds to an $R/\operatorname{Ann}(M)$-module structure on M. □

10 Direct sum and product of modules

Throughout these notes, we work with modules over a commutative ring R.

10.1 Direct sum of modules

Definition 10.1.1. The **direct sum** of R-modules M and N is the R-module

$$M \oplus N = \{m + n \mid m \in M,\, n \in N\}$$

with addition given by

$$(m + n) + (m' + n') = (m + m') + (n + n')$$

and scalar multiplication (necessarily) given by

$$r(m + n) = rm + rn.$$

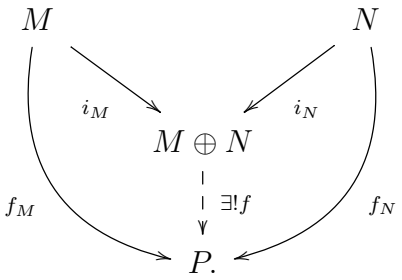
The direct sum comes equipped with the inclusion maps from each summand

$$\begin{cases} i_M \colon M \to M \oplus N \\ i_N \colon N \to M \oplus N, \end{cases}$$

which are R-module homomorphisms.

Proposition 10.1.2. *The direct sum of modules $M \oplus N$ along with inclusion maps i_M and i_N is the* coproduct *of R-modules, i.e., it satisfies the following universal property.*

For any R-module P along with maps $f_M \colon M \to P$ and $f_N \colon N \to P$, there is a unique map $f \colon M \oplus N \to P$ whose restrictions are $f \circ i_M = f_M$ and $f \circ i_N = f_N$, i.e., making the following diagram commute:



The map f is denoted in matrix notation as $f = \begin{bmatrix} f_M & f_N \end{bmatrix}$ or sometimes $f_M + f_N$.

Slogan: "A map out of $M \oplus N$ is the same data as a map out of M and a map out of N".

Proof. Since the values of f are prescribed on M and N, the only possible formula for f is

$$\begin{aligned} f(m + n) &= f(m) + f(n) \\ &= f_M(m) + f_N(n). \end{aligned}$$

One readily checks that this formula defines an R-module homomorphism $f \colon M \oplus N \to P$. □

We can generalize the construction of direct sums to arbitrary (infinite) families of modules.

Definition 10.1.3. The **direct sum** of a family of R-modules $\{M_\alpha\}_{\alpha\in\Lambda}$ is the R-module

$$\bigoplus_{\alpha\in\Lambda} M_\alpha = \{m_{\alpha_1} + \cdots + m_{\alpha_k} \mid k \geq 0,\ \alpha_i \in \Lambda,\ m_{\alpha_i} \in M_{\alpha_i}\}$$

where terms coming from the same summand can be added within the summand, but the addition of terms from different summands is formal.

As before, the direct sum comes equipped with inclusion maps from each summand:

$$i_\beta \colon M_\beta \to \bigoplus_\alpha M_\alpha.$$

Proposition 10.1.4. *The R-module $\bigoplus_\alpha M_\alpha$ along with the inclusion maps $i_\beta \colon M_\beta \to \bigoplus_\alpha M_\alpha$ is the coproduct of R-modules, i.e., it satisfies the following universal property.*

For any R-module P along with maps $f_\alpha \colon M_\alpha \to P$ for all $\alpha \in \Lambda$, there is a unique map $f \colon \bigoplus_\alpha M_\alpha \to P$ whose restrictions are $f \circ i_\alpha = f_\alpha$ for all $\alpha \in \Lambda$.

10.2 Product of modules

This section will look suspiciously dual to the previous section.

Definition 10.2.1. The **product** of R-modules M and N is the R-module with underlying set the Cartesian product

$$M \times N = \{(m, n) \mid m \in M,\ n \in N\}$$

endowed with coordinatewise addition and scalar multiplication:

$$(m, n) + (m', n') = (m + m', n + n')$$
$$r(m, n) = (rm, rn).$$

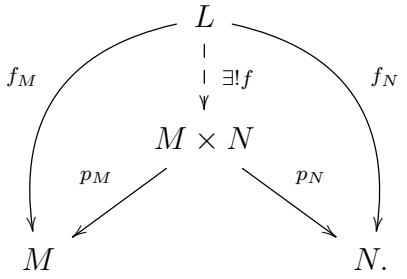
The product comes equipped with the projection maps onto each factor

$$\begin{cases} p_M \colon M \times N \to M \\ p_N \colon M \times N \to N, \end{cases}$$

which are R-module homomorphisms.

Proposition 10.2.2. *The product of modules $M \times N$ along with projection maps p_M and p_N is the* product *of R-modules (in the categorical sense), i.e., it satisfies the following universal property.*

For any R-module L along with maps $f_M \colon L \to M$ and $f_N \colon L \to N$, there is a unique map $f \colon L \to M \times N$ whose coordinates are $p_M \circ f = f_M$ and $p_N \circ f = f_N$, i.e., making the following diagram commute:



The map f is denoted $f = (f_M, f_N)$ or $\left[\begin{smallmatrix} f_M \\ f_N \end{smallmatrix}\right]$.

Slogan: "A map into $M \times N$ is the same data as a map into M and a map into N".

Proof. Since the coordinates of f into M and N are prescribed, the only possible formula for f is

$$f(x) = (f_M(x), f_N(x)).$$

One readily checks that this formula defines an R-module homomorphism $f \colon L \to M \times N$. □

We can generalize the construction of products to arbitrary (infinite) families of modules.

Definition 10.2.3. The **product** of a family of R-modules $\{M_\alpha\}_{\alpha\in\Lambda}$ is the R-module with underlying set the Cartesian product

$$\prod_{\alpha\in\Lambda} M_\alpha = \{(m_\alpha)_{\alpha\in\Lambda} \mid m_\alpha \in M_\alpha \text{ for all } \alpha \in \Lambda\}$$

endowed with coordinatewise addition and scalar multiplication:

$$(m_\alpha) + (m'_\alpha) = (m_\alpha + m'_\alpha)$$
$$r(m_\alpha) = (rm_\alpha).$$

Here $m = (m_\alpha)_{\alpha\in\Lambda}$ and $m' = (m'_\alpha)_{\alpha\in\Lambda}$ denote elements of the product $\prod_{\alpha\in\Lambda} M_\alpha$.

As before, the product comes equipped with projection maps onto each factor:

$$p_\beta \colon \prod_\alpha M_\alpha \to M_\beta.$$

Proposition 10.2.4. *The R-module $\prod_\alpha M_\alpha$ along with the projection maps $p_\beta \colon \prod_\alpha M_\alpha \to M_\beta$ is the product of R-modules (in the categorical sense), i.e., it satisfies the following universal property.*

For any R-module L along with maps $f_\alpha \colon L \to M_\alpha$ for all $\alpha \in \Lambda$, there is a unique map $f \colon L \to \prod_\alpha M_\alpha$ whose coordinates are $p_\alpha \circ f = f_\alpha$ for all $\alpha \in \Lambda$.

10.3 Relationship between direct sum and product

For any family of R-modules $\{M_\alpha\}_{\alpha\in\Lambda}$, there is a natural R-module homomorphism

$$\psi\colon \bigoplus_{\alpha\in\Lambda} M_\alpha \to \prod_{\alpha\in\Lambda} M_\alpha \tag{1}$$

whose restriction to the summand M_β and coordinate into M_γ is the map $\psi_{\beta,\gamma}\colon M_\beta \to M_\gamma$ given by

$$\psi_{\beta,\gamma} = \begin{cases} \mathrm{id}_{M_\beta} & \text{if } \beta = \gamma \\ 0 & \text{if } \beta \neq \gamma. \end{cases}$$

Proposition 10.3.1. *The R-module homomorphism ψ in Equation (1) is injective, with image consisting of the "finitely supported" elements of the product:*

$$\mathrm{im}(\psi) = \{m \in \prod_{\alpha\in\Lambda} M_\alpha \mid m_\alpha \neq 0 \text{ for finitely many } \alpha \in \Lambda\}.$$

In particular, *finite* direct sums and products agree:

Corollary 10.3.2. *For any R-modules M and N, the natural map*

$$M \oplus N \xrightarrow{\cong} M \times N$$
$$m + n \mapsto (m, n)$$

is an isomorphism.

In fancier terminology, the direct sum of R-modules $M \oplus N$ is a **biproduct**: simultaneously the product and coproduct of M and N.

Example 10.3.3. The map of abelian groups

$$\bigoplus_{n=1}^{\infty} \mathbb{Z} \hookrightarrow \prod_{n=1}^{\infty} \mathbb{Z}$$

is injective but not surjective, since its image does not contain elements such as $(1, 1, 1, \cdots) \in \prod_{n=1}^{\infty} \mathbb{Z}$.

It turns out that the target of the map in Example 10.3.3 is not isomorphic to the source. More is true:

Theorem 10.3.4. *The abelian group $\prod_{n=1}^{\infty} \mathbb{Z}$ is not free.*

Exercise 10.3.5. Let k be a field. Show that the k-vector space $\prod_{n=1}^{\infty} k$ has *uncountably* infinite dimension. In other words, it is not isomorphic to $\bigoplus_{n=1}^{\infty} k$ as a k-vector space.

11 Free modules, finitely generated modules

11.1 Free modules

Most of what you learned about vector spaces also works for free R-modules.

Definition 11.1.1. Let M be an R-module. A subset $B \subseteq M$ is called:

1. a **generating set** if every element $m \in M$ can be expressed as an R-linear combination of elements of B:
$$m = r_1 b_1 + \cdots + r_k b_k$$
for some scalars $r_i \in R$ and elements $b_i \in B$. In other words, the R-submodule generated by B is all of M.
2. **linearly independent** if the only R-linear combination of elements of B that yields zero
$$r_1 b_1 + \cdots + r_k b_k = 0$$
is the trivial combination $r_1 = \cdots = r_k = 0$.
3. a **basis** if it is a linearly independent generating set.

Lemma 11.1.2. *Let M be an R-module. For a subset $B = \{b_i \mid i \in I\}$ of M, the following conditions are equivalent.*

1. *B is a basis of M.*
2. *Every element $m \in M$ can be expressed* uniquely *as an R-linear combination of elements of B.*
3. *The R-module homomorphism that picks out the elements of B*
$$\bigoplus_{i \in I} R \to M$$
$$e_i \mapsto b_i$$
is an isomorphism.

Definition 11.1.3. An R-module M is called **free** if it admits a basis, i.e., if there is an isomorphism $M \cong \bigoplus_{i \in I} R$.

The module M is called **finite free** (as shorthand for *finitely generated free*) if it admits a finite basis $\{b_1, \ldots, b_d\}$, i.e., if there is an isomorphism $M \cong R^d$. The number $d \geq 0$ is called the **rank** of M.

We will prove later that the rank is well-defined, that is:

$$R^m \cong R^n \implies m = n$$

[AM69, §2 Exercise 11].

Example 11.1.4. The abelian group $\mathbb{Z}^3$ is free of rank 3, with the standard basis $B = \{e_1, e_2, e_3\}$.

Example 11.1.5. Consider the $\mathbb{Z}[x]$-module

$$M = \mathbb{Z}[x]/(x^3).$$

The underlying abelian group of M is free of rank 3, with basis the monomials $B = \{1, x, x^2\}$. Note that M is *not* free as a $\mathbb{Z}[x]$-module.

Example 11.1.6. In the abelian group $\mathbb{Z}$, the subset $\{5\}$ is linearly independent but *not* a generating set. The $\mathbb{Z}$-submodule generated by 5 is $5\mathbb{Z} \subset \mathbb{Z}$, the set of multiples of 5.

This example illustrates the following. Unlike in vector spaces, *not* every linearly independent subset of an R-module M can be completed to a basis, even if M happens to be free.

Example 11.1.7. In the abelian group $\mathbb{Z}/6$, the subset $\{\overline{1}\}$ is a generating set but is *not* linearly independent, due to the non-trivial linear combination

$$6 \cdot \overline{1} = \overline{0},$$

with coefficient $6 \neq 0 \in \mathbb{Z}$. In fact, the abelian group $\mathbb{Z}/6$ is not free. However, if we view $\mathbb{Z}/6$ as a $\mathbb{Z}/6$-module, then it *is* free with basis $\{\overline{1}\}$. The equation

$$\overline{r} \cdot \overline{1} = \overline{0}$$

with $\overline{r} \in \mathbb{Z}/6$ has as solution $r = 6k$ for $k \in \mathbb{Z}$, which ensures $\overline{r} = 0 \in \mathbb{Z}/6$.

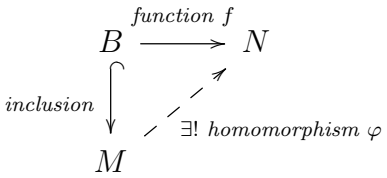
This example illustrates that the notion of "linear independence" depends on the ground ring R.

Example 11.1.8. The $\mathbb{Q}$-vector space $\mathbb{Q}$ is free with basis $\{1\}$. However, $\mathbb{Q}$ is *not* free as an abelian group; this can be shown using the fact that $\mathbb{Q}$ is divisible.

Note that the $\mathbb{Z}$-submodule of $\mathbb{Q}$ generated by 1 is $\mathbb{Z} \subset \mathbb{Q}$, whereas the $\mathbb{Q}$-submodule generated by 1 is all of $\mathbb{Q}$.

This example illustrates that the notion of "generating set" also depends on the ground ring R.

Proposition 11.1.9 (Universal property of free modules)**.** *Let M be a free R-module with basis B. For every R-module N and function of sets $f\colon B \to N$, there exists a unique R-module homomorphism $\varphi\colon M \to N$ extending f, i.e., making the following diagram commute:*



Proof. By Lemma 11.1.2, every element $m \in M$ can be written uniquely as an R-linear combination

$$m = r_1 b_1 + \cdots + r_k b_k.$$

If there exists an R-linear extension φ of f, it must be given by

$$\begin{aligned} \varphi(m) &= \varphi(r_1 b_1 + \cdots + r_k b_k) \\ &= r_1 \varphi(b_1) + \cdots + r_k \varphi(b_k) \\ &= r_1 f(b_1) + \cdots + r_k f(b_k). \end{aligned}$$

One readily checks that this formula defines an R-module homomorphism $\varphi\colon M \to N$. □

Remark 11.1.10. For psychological reasons, it might be convenient to write a basis B as an indexed set $B = \{b_i \mid i \in I\}$, as we did in Lemma 11.1.2. With that notation, a function $f\colon B \to N$ amounts to a family $\{n_i\}_{i \in I}$ of elements of N, writing $f(b_i) = n_i$.

The b_i had to be distinct, so we could view B as a subset $B \subseteq M$. In contrast, the n_i may be repeated, so it is important to view them as a *family* of elements of N, indexed by $i \in I$. As an extreme example, take $n_i = 0$ for all $i \in I$, which yields the R-linear extension $\varphi = 0\colon M \to N$.

11.2 Finitely generated modules

Definition 11.2.1. An R-module M is **finitely generated** if it admits a finite generating set $\{x_1, \ldots, x_k\}$.

That is, every element $m \in M$ can be expressed as an R-linear combination

$$m = r_1 x_1 + \cdots + r_k x_k$$

for some scalars $r_i \in R$.

Example 11.2.2. The abelian group

$$M = \mathbb{Z}^2 \oplus \mathbb{Z}/4 \oplus \mathbb{Z}/9$$

is finitely generated, by the four generators

$$(e_1, 0, 0), \quad (e_2, 0, 0), \quad (0, \overline{1}, 0), \quad (0, 0, \overline{1}),$$

where $e_1 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $e_2 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ denote the standard basis elements of $\mathbb{Z}^2$. By the Chinese remainder theorem, M is in fact generated by the three generators

$$(e_1, 0, 0), \quad (e_2, 0, 0), \quad (0, \overline{1}, \overline{1}).$$

Indeed, the element $(\overline{1}, \overline{1}) \in \mathbb{Z}/4 \oplus \mathbb{Z}/9$ corresponds to a generator of $\mathbb{Z}/36$ via the isomorphism

$$\mathbb{Z}/36 \xrightarrow[\cong]{(q_4, q_9)} \mathbb{Z}/4 \oplus \mathbb{Z}/9.$$

Example 11.2.2 illustrates the general form of a finitely generated abelian group, written in primary decomposition.

Theorem 11.2.3 (Fundamental theorem of finitely generated modules over a PID)**.** *Let R be a principal ideal domain. Every finitely generated R-module M is a direct sum of cyclic R-modules:*

$$M \cong R^d \oplus R/(a_1) \oplus \cdots \oplus R/(a_n)$$

for some $d \geq 0$ and non-zero (and non-unit) elements $a_i \in R$.

More precise statements can be found in [DF04, §12.1] as well as

`https://en.wikipedia.org/wiki/Structure_theorem_for_finitely_generated_modules_over_a_principal_ideal_domain`

Lemma 11.2.4. *For an R-module M, the following conditions are equivalent.*

1. *M is finitely generated.*

2. *There is a surjective homomorphism from a finite free R-module $R^k \twoheadrightarrow M$.*

3. *M is a quotient of a finite free R-module R^k.*

Proof. (1) $\iff$ (2). Given elements $x_1, \ldots, x_k \in M$, consider the R-module homomorphism that picks out those elements:

$$\varphi\colon R^k \to M$$
$$e_i \mapsto x_i.$$

The submodule $\langle x_1, \ldots, x_k \rangle \subseteq M$ generated by the x_i is the image of φ. Thus the x_i are generators of M if and only if φ is surjective.

(2) $\iff$ (3). By the first isomorphism theorem, given any surjective homomorphism $\varphi\colon R^k \twoheadrightarrow M$, the target is the quotient

$$M \cong R^k / \ker(\varphi). \qquad \square$$

Proposition 11.2.5. *1. A quotient of a finitely generated R-module is finitely generated.*

2. *If the R-modules M and N are finitely generated, then so is their direct sum $M \oplus N$.*

Proof. Exercise. $\square$

Warning 11.2.6. A submodule of a finitely generated module need **not** be finitely generated. For example, let k be a field and consider the polynomial ring in countably infinitely many variables

$$R = k[x_1, x_2, \ldots].$$

Then R itself as an R-module is finitely generated, namely by the generator $1 \in R$. However, the ideal of polynomials with zero constant term

$$I = (x_1, x_2, \ldots)$$

is **not** finitely generated as an R-module.

The problem here is that the ring R is not Noetherian. In Chapter 7, we will see that over a *Noetherian* ring R, a submodule of a finitely generated module must be finitely generated. This holds for instance over $\mathbb{Z}$ or a polynomial ring $k[x_1, \ldots, x_n]$.

12 Maps between free modules

Throughout these notes, we work over a commutative ring R. We will review some linear algebra and see that most of it goes through if we work with *free* modules. The main difference is that... we can't say "vector" anymore, although we want to.

Note that "R-linear map" is a synonym for "R-module homomorphism".

12.1 Working in the standard basis

Let us write elements of the finite free R-module R^n as columns

$$x = (x_1, \ldots, x_n) = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in R^n.$$

Proposition 12.1.1. *1. For every R-linear map $f\colon R^n \to R^m$, there is a unique $m \times n$ matrix A with entries in R satisfying*

$$f(x) = Ax$$

for all $x \in R^n$, given by the formula

$$A = \begin{bmatrix} f(e_1) & \ldots & f(e_n) \end{bmatrix}. \tag{2}$$

In other words, the columns of A are the values of f on the standard basis elements. We call A the matrix representing *f.*

2. The correspondence in part (1) defines an isomorphism of R-modules

$$\mathrm{Hom}_R(R^n, R^m) \xrightarrow{\cong} \mathrm{Mat}_{m\times n}(R).$$

3. Said isomorphism is compatible with composition. That is, given maps $g\colon R^p \to R^n$ and $f\colon R^n \to R^m$ represented by an $n \times p$ matrix B and an $m \times n$ matrix A, the composite $f \circ g\colon R^p \to R^m$ is represented by the $m \times p$ matrix AB, as illustrated in the diagram

$$\begin{array}{ccccc} R^p & \xrightarrow[B]{g} & R^n & \xrightarrow[A]{f} & R^m \\ & \searrow & & \nearrow & \\ & & \xrightarrow[AB]{f\circ g} & & \end{array}$$

In other words, the following diagram of R-modules commutes:

$$\begin{array}{ccc} \mathrm{Hom}_R(R^n, R^m) \otimes_R \mathrm{Hom}_R(R^p, R^n) & \xrightarrow{\circ} & \mathrm{Hom}_R(R^p, R^m) \\ \cong \downarrow & & \downarrow \cong \\ \mathrm{Mat}_{m\times n}(R) \otimes_R \mathrm{Mat}_{n\times p}(R) & \xrightarrow{product} & \mathrm{Mat}_{m\times p}(R). \end{array}$$

In particular, for square matrices, we obtain an isomorphism of R-algebras

$$\mathrm{End}_R(R^n) \xrightarrow{\cong} \mathrm{Mat}_n(R)$$

between the endomorphism algebra of R^n and the algebra of $n \times n$ matrices.

Example 12.1.2. Consider the map of abelian groups

$$f\colon \mathbb{Z}^2 \to \mathbb{Z}^3$$

given in the standard basis by

$$f(e_1) = 4e_1 + e_2 - 2e_3$$
$$f(e_2) = 3e_1 + e_3.$$

The map f is represented by the 3×2 matrix with integer entries

$$A = \begin{bmatrix} f(e_1) & f(e_2) \end{bmatrix} = \begin{bmatrix} 4 & 3 \\ 1 & 0 \\ -2 & 1 \end{bmatrix}.$$

Remark 12.1.3. In light of Proposition 12.1.1, we sometimes identify an R-linear map $f\colon R^n \to R^m$ with its representing matrix, saying that f is the matrix A in Equation (2). By default, this means the matrix representing f with respect to the *standard* bases.

Warning 12.1.4. For an R-linear map $f\colon R^n \to R^m$, the $m \times n$ matrix A representing f is characterized by

$$f(e_j) = \sum_{i=1}^{m} a_{ij} e_i,$$

i.e., we read off the value $f(e_j)$ in the j^{th} *column* of A. Some authors also use the transpose convention

$$f(e_i) = \sum_{i=1}^{m} b_{ij} e_j.$$

In the transpose convention, elements of R^n are written as *rows*, $f\colon R^n \to R^m$ is represented by an $n \times m$ matrix B whose i^{th} *row* is the value $f(e_i) \in R^m$, and matrices act by multiplication on the *right*.

The two conventions are related by transposition: $B = A^T$.

12.2 Changing bases

Let V be a finite free R-module of rank n. From the notes from October 6, recall that a choice of basis $\{v_1, \ldots, v_n\}$ of V is the same data as an isomorphism of R-modules $\varphi\colon V \xrightarrow{\cong} R^n$, which sends the basis $\{v_1, \ldots, v_n\}$ of V to the standard basis $\{e_1, \ldots, e_n\}$ of R^n. In other words, we have

$$\begin{aligned} \varphi\colon V &\xrightarrow{\cong} R^n \\ v_i &\mapsto e_i \\ v = c_1 v_1 + \ldots + c_n v_n &\mapsto \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix}. \end{aligned}$$

Definition 12.2.1. Let V be a finite free R-module of rank n. The **coordinates** of an element $v \in V$ with respect to a basis $\{v_1, \ldots, v_n\}$ of V are the coefficients $c_1, \ldots, c_n \in R$ satisfying

$$v = c_1 v_1 + \ldots + c_n v_n.$$

Denote the coordinates of v as a column

$$[v]_{\{v_i\}} := \begin{bmatrix} c_1 \\ \vdots \\ c_n \end{bmatrix} \in R^n.$$

As shorthand notation, let us name the basis $\mathcal{A} := \{v_1, \ldots, v_n\}$ and then write $[v]_{\mathcal{A}}$ for the coordinates of v with respect to the basis $\mathcal{A}$.

Note that the coordinates of $v \in V$ *depend* on the choice of basis.

Theorem 12.2.2. *Let $V \cong R^n$ and $W \cong R^m$ be finite free R-modules of rank n and m respectively, and $f\colon V \to W$ an R-linear map. Let $\mathcal{A} = \{v_1, \ldots, v_n\}$ be a basis of V and $\mathcal{B} = \{w_1, \ldots, w_m\}$ a basis of W. Then there is a unique $m \times n$ matrix A satisfying*

$$[f(v)]_{\mathcal{B}} = A[v]_{\mathcal{A}}$$

for all $v \in V$, given by the formula

$$A = \begin{bmatrix} [f(v_1)]_{\mathcal{B}} & \cdots & [f(v_n)]_{\mathcal{B}} \end{bmatrix}.$$

*We denote this matrix $[f]_{\mathcal{B}\mathcal{A}}$ and call it the matrix **representing** f with respect to the bases $\mathcal{A}$ and $\mathcal{B}$.*

Proof. The choice of bases $\mathcal{A}$ and $\mathcal{B}$ defines isomorphisms $\varphi\colon V \xrightarrow{\cong} R^n$ and $\psi\colon W \xrightarrow{\cong} R^m$. There is a unique R-linear map $A\colon R^n \to R^m$ making the diagram

$$\begin{array}{ccc} V & \xrightarrow{f} & W \\ {\scriptstyle\varphi}\downarrow{\scriptstyle\cong} & & {\scriptstyle\cong}\downarrow{\scriptstyle\psi} \\ R^n & \xrightarrow[A]{} & R^m \end{array}$$

commute, namely $A = \psi \circ T \circ \varphi^{-1}$. By Proposition 12.1.1, the R-linear map A corresponds to the $m \times n$ matrix A whose j^{th} column is

$$(\psi \circ f \circ \varphi^{-1})(e_j) = (\psi \circ f)(v_j) = [f(v_j)]_{\mathcal{B}}. \qquad \square$$

Remark 12.2.3. In Proposition 12.1.1, the matrix A was the matrix representing $f\colon R^m \to R^n$ with respect to the standard bases $\mathcal{S}$ of R^m and R^n, i.e., $A = [f]_{\mathcal{SS}}$.

Example 12.2.4. Consider the map of abelian groups $f\colon \mathbb{Z}^2 \to \mathbb{Z}^3$ from Example 12.1.2. As a basis $\mathcal{A} = \{v_1, v_2\}$ of $\mathbb{Z}^2$, take

$$v_1 = \begin{bmatrix} 3 \\ 2 \end{bmatrix}, \quad v_2 = \begin{bmatrix} 2 \\ 1 \end{bmatrix}.$$

As a basis $\mathcal{B} = \{w_1, w_2, w_3\}$ of $\mathbb{Z}^3$, take

$$w_1 = \begin{bmatrix} 1 \\ 0 \\ 2 \end{bmatrix}, \quad w_2 = \begin{bmatrix} 1 \\ -1 \\ 3 \end{bmatrix}, \quad w_2 = \begin{bmatrix} 1 \\ 2 \\ 1 \end{bmatrix}.$$

Find the matrix $[f]_{\mathcal{BA}}$ representing f with respect to the bases $\mathcal{A}$ and $\mathcal{B}$.

Solution. The diagram

$$\begin{array}{ccc} \mathbb{Z}^2_{\mathcal{A}} & \xrightarrow[[f]_{\mathcal{BA}}]{f} & \mathbb{Z}^3_{\mathcal{B}} \\ {\scriptstyle\text{id}}\downarrow{\scriptstyle[\text{id}]_{\mathcal{SA}}} & & {\scriptstyle\text{id}}\downarrow{\scriptstyle[\text{id}]_{\mathcal{SB}}} \\ \mathbb{Z}^2_{\mathcal{S}} & \xrightarrow[[f]_{\mathcal{SS}}]{f} & \mathbb{Z}^3_{\mathcal{S}} \end{array}$$

provides the matrix factorization

$$\begin{aligned}
[f]_{\mathcal{BA}} &= [\mathrm{id}]_{\mathcal{BS}}[f]_{\mathcal{SS}}[\mathrm{id}]_{\mathcal{SA}} \\
&= [\mathrm{id}]_{\mathcal{SB}}^{-1}[f]_{\mathcal{SS}}[\mathrm{id}]_{\mathcal{SA}} \\
&= \begin{bmatrix} 1 & 1 & 1 \\ 0 & -1 & 2 \\ 2 & 3 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 4 & 5 \\ 1 & 0 \\ -2 & 7 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix} \\
&= \begin{bmatrix} 1 & 1 & 1 \\ 0 & -1 & 2 \\ 2 & 3 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 18 & 11 \\ 3 & 2 \\ -4 & -3 \end{bmatrix} \\
&= \begin{bmatrix} 7 & -2 & -3 \\ -4 & 1 & 2 \\ -2 & 1 & 1 \end{bmatrix} \begin{bmatrix} 18 & 11 \\ 3 & 2 \\ -4 & -3 \end{bmatrix} \\
&= \boxed{\begin{bmatrix} 132 & 82 \\ -77 & -48 \\ -37 & -23 \end{bmatrix}}.
\end{aligned}$$

How to read this matrix? The first column says:

$$f(v_1) = 132w_1 - 77w_2 - 37w_3.$$

Let us check that this is correct:

$$\begin{aligned}
f(v_1) &= \begin{bmatrix} 4 & 5 \\ 1 & 0 \\ -2 & 7 \end{bmatrix} \begin{bmatrix} 3 \\ 2 \end{bmatrix} \\
&= \begin{bmatrix} 18 \\ 3 \\ -4 \end{bmatrix}
\end{aligned}$$

$$\begin{aligned}
132w_1 - 77w_2 - 37w_3 &= 132\begin{bmatrix}1\\0\\2\end{bmatrix} - 77\begin{bmatrix}1\\-1\\3\end{bmatrix} - 37\begin{bmatrix}1\\2\\1\end{bmatrix} \\
&= \begin{bmatrix}132\\0\\264\end{bmatrix} - \begin{bmatrix}77\\-77\\231\end{bmatrix} - \begin{bmatrix}37\\74\\37\end{bmatrix} \\
&= \begin{bmatrix}55\\77\\33\end{bmatrix} - \begin{bmatrix}37\\74\\37\end{bmatrix} \\
&= \begin{bmatrix}18\\3\\-4\end{bmatrix}. \qquad \checkmark
\end{aligned}$$

12.3 Determinant and invertibility

Definition 12.3.1. Let $V \cong R^n$ be a finite free R-module of rank n. The **determinant** of an endomorphism $f\colon V \to V$ is the determinant of the representing matrix $[f]_{\mathcal{B}\mathcal{B}}$ for any choice of basis $\mathcal{B}$ of V.

The determinant is well-defined since the representing matrices of f with respect to different bases are conjugate and thus have the same determinant:

$$\begin{aligned} A &= PBP^{-1} \\ \implies \det(A) &= \det(PBP^{-1}) \\ &= \det(P)\det(B)\det(P)^{-1} \\ &= \det(B). \end{aligned}$$

Proposition 12.3.2. *Let V be a finite free R-module. An endomorphism $f\colon V \to V$ is invertible if and only if its determinant is invertible in R, that is,* $\det(f) \in R^\times$.

Proof. ($\implies$) Assuming f is invertible, the equation $ff^{-1} = \mathrm{id}_V$ in $\mathrm{End}_R(V)$ yields the equation in R

$$\begin{aligned} \det(ff^{-1}) &= \det(\mathrm{id}_V) = 1 \\ \implies \det(f)\det(f^{-1}) &= 1 \\ \implies \det(f^{-1}) &= \det(f)^{-1} \end{aligned}$$

so that $\det(f) \in R$ is a unit.

($\impliedby$) Assume that $\det(f)$ is invertible. By choosing a basis of V, we may assume $V = R^n$ and f is an $n \times n$ matrix A. The adjugate matrix of A satisfies

$$A\,\mathrm{adj}(A) = \mathrm{adj}(A)A = \det(A)I.$$

Since $\det(A)$ is a unit, the matrix A is invertible with inverse

$$A^{-1} = \det(A)^{-1}\,\mathrm{adj}(A). \qquad \square$$

Example 12.3.3. An endomorphism $f\colon \mathbb{Z}^n \to \mathbb{Z}^n$ is invertible if and only if its determinant is $\det(f) = \pm 1$.

Corollary 12.3.4. *Elements $b_1, b_2, \ldots, b_n \in R^n$ form a basis of R^n if and only if the $n \times n$ matrix with the b_i as columns*

$$B = \begin{bmatrix} b_1 & b_2 & \cdots & b_n \end{bmatrix}$$

has an invertible determinant $\det(B) \in R^\times$.

Proposition 12.3.5. *An element* $\begin{bmatrix} a \\ b \end{bmatrix} \in \mathbb{Z}^2$ *can be completed to a basis if and only if a and b have no common factor.*

Proof. ($\Longrightarrow$) Assume that a and b have a common factor $p \geq 2$, so that we can write $a = pa'$ and $b = pb'$. Then for any $\begin{bmatrix} c \\ d \end{bmatrix} \in \mathbb{Z}^2$, the determinant

$$\begin{aligned} \det \begin{bmatrix} a & c \\ b & d \end{bmatrix} &= \begin{vmatrix} a & c \\ b & d \end{vmatrix} \\ &= \begin{vmatrix} pa' & c \\ pb' & d \end{vmatrix} \\ &= p \begin{vmatrix} a' & c \\ b' & d \end{vmatrix} \end{aligned}$$

is a multiple of p, hence not a unit in $\mathbb{Z}$. By Corollary 12.3.4, the set $\{ \begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} c \\ d \end{bmatrix} \}$ is not a basis of $\mathbb{Z}^2$.

($\Longleftarrow$) Assume that a and b have no common factor. (If one of the two is 0, this forces the other number to be ± 1.) Then their greatest common divisor is $\gcd(a, b) = 1$. By Bézout's identity, there exist $s, t \in \mathbb{Z}$ satisfying

$$sa + tb = \gcd(a, b) = 1.$$

But that number is the determinant

$$\begin{vmatrix} a & -t \\ b & s \end{vmatrix} = as - (-bt) = as + bt = 1.$$

By Corollary 12.3.4, the set $\{ \begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} -t \\ s \end{bmatrix} \}$ is a basis of $\mathbb{Z}^2$. □

12.4 Cayley–Hamilton theorem

Recall the following notion from linear algebra.

Definition 12.4.1. Let A be an $n \times n$ matrix with entries in R. The **characteristic polynomial** of A is

$$p_A(t) = \det(A - tI).$$

The characteristic polynomial is a formal polynomial with coefficients in R, that is: $p_A \in R[t]$. It has degree n, with leading term $(-1)^n t^n$.

Remark 12.4.2. Some authors prefer the convention $\det(tI - A)$, which agrees with our convention up to a sign:

$$\det(tI - A) = (-1)^n \det(A - tI).$$

The benefit of $\det(tI - A)$ is that it is always monic, i.e., its leading term is t^n. The benefit of $\det(A - tI)$ is that its computation introduces fewer signs and its constant term is always $\det(A)$.

Definition 12.4.3. Let $V \cong R^n$ be a finite free R-module of rank n. The **characteristic polynomial** of an endomorphism $f \colon V \to V$ is

$$p_f(t) = \det(f - t \cdot \mathrm{id}_V).$$

In other words, it is the characteristic polynomial of the representing matrix $A = [f]_{\mathcal{B}\mathcal{B}}$ for any choice of basis $\mathcal{B}$ of V:

$$p_f(t) = p_A(t).$$

Theorem 12.4.4 (Cayley–Hamilton theorem)**.** *Let V be a finite free R-module and $f \colon V \to V$ an endomorphism. Then f satisfies its characteristic equation, i.e., the following equation in $\mathrm{End}_R(V)$ holds:*

$$p_f(f) = 0.$$

Proof. We may assume without loss of generality $V = R^n$ and f is represented by an $n \times n$ matrix $A \in M_n(R)$. The characteristic matrix of A is $A - tI \in M_n(R[t])$. The adjugate formula yields the equality in $M_n(R[t])$

$$(A - tI)\,\mathrm{adj}(A - tI) = \det(A - tI) \cdot I = \begin{bmatrix} p_A(t) & 0 & \cdots & 0 \\ 0 & p_A(t) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & p_A(t) \end{bmatrix}.$$

For the rest of the proof, see [AM69, Proposition 2.4], [Rei95, §2.6], [DF04, §12.2 Proposition 20], as well as:

`https://en.wikipedia.org/wiki/Cayley%E2%80%93Hamilton_theorem#Proofs` □

Example 12.4.5. Let $f\colon \mathbb{Z}^2 \to \mathbb{Z}^2$ be the map of abelian groups represented (in the standard basis) by the matrix

$$A = \begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix}.$$

Let us verify the Cayley–Hamilton in this example. The characteristic polynomial of f is

$$\begin{aligned} p_A(t) = \det(A - tI) &= \begin{vmatrix} 2-t & -1 \\ 1 & 3-t \end{vmatrix} \\ &= (2-t)(3-t) - (-1) \\ &= (t-2)(t-3) + 1 \\ &= t^2 - 3t - 2t + 6 + 1 \\ &= t^2 - 5t + 7. \end{aligned}$$

Evaluating the polynomial $p_A(t) \in \mathbb{Z}[t]$ at $t = A$ in the endomorphism ring $\mathrm{Mat}_2(\mathbb{Z})$ yields the 2×2 matrix

$$\begin{aligned} p_A(A) &= A^2 - 5A + 7I \\ &= \begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix} - 5 \begin{bmatrix} 2 & -1 \\ 1 & 3 \end{bmatrix} + 7 \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 3 & -5 \\ 5 & 8 \end{bmatrix} - \begin{bmatrix} 10 & -5 \\ 5 & 15 \end{bmatrix} + \begin{bmatrix} 7 & 0 \\ 0 & 7 \end{bmatrix} \\ &= \begin{bmatrix} -7 & 0 \\ 0 & -7 \end{bmatrix} + \begin{bmatrix} 7 & 0 \\ 0 & 7 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0. \qquad \checkmark \end{aligned}$$

Example 12.4.6. Let k be a field and consider the polynomial ring $R = k[x]$. Let $f\colon k[x]^2 \to k[x]^2$ be the map of $k[x]$-modules represented (in the standard basis) by the matrix

$$A = \begin{bmatrix} x+2 & x-1 \\ 3x & 5 \end{bmatrix}.$$

Let us verify the Cayley–Hamilton in this example. Careful! The ground ring $R = k[x]$ happens to consist of polynomials, while the characteristic polynomial $p_A(t)$ is a formal polynomial in $R[t] = k[x][t] \cong k[x,t]$. In this setup, polynomials appear in two unrelated ways.

The characteristic polynomial of f is

$$\begin{aligned} p_A(t) = \det(A - tI) &= \begin{vmatrix} x+2-t & x-1 \\ 3x & 5-t \end{vmatrix} \\ &= (x+2-t)(5-t) - 3x(x-1) \\ &= 5(x+2) - (x+2)t - 5t + t^2 - 3x(x-1) \\ &= t^2 - (x+7)t + 5(x+2) - 3x(x-1) \\ &= t^2 - (x+7)t + 5x + 10 - 3x^2 + 3x \\ &= t^2 - (x+7)t + (-3x^2 + 8x + 10). \end{aligned}$$

Evaluating the polynomial $p_A(t) \in R[t]$ at $t = A$ in the endomorphism ring $\mathrm{Mat}_2(R)$ yields the 2×2 matrix

$$\begin{aligned} p_A(A) &= A^2 - (x+7)A + (-3x^2 + 8x + 10)I \\ &= \begin{bmatrix} x+2 & x-1 \\ 3x & 5 \end{bmatrix} \begin{bmatrix} x+2 & x-1 \\ 3x & 5 \end{bmatrix} - (x+7) \begin{bmatrix} x+2 & x-1 \\ 3x & 5 \end{bmatrix} + (-3x^2 + 8x + 10) \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \\ &= \begin{bmatrix} 4x^2 + x + 4 & (x-1)(x+7) \\ 3x(x+7) & 3x^2 - 3x + 25 \end{bmatrix} - \begin{bmatrix} (x+7)(x+2) & (x+7)(x-1) \\ 3x(x+7) & 5(x+7) \end{bmatrix} \\ &\quad + \begin{bmatrix} -3x^2 + 8x + 10 & 0 \\ 0 & -3x^2 + 8x + 10 \end{bmatrix} \\ &= \begin{bmatrix} 3x^2 - 8x - 10 & 0 \\ 0 & 3x^2 - 8x - 10 \end{bmatrix} + \begin{bmatrix} -3x^2 + 8x + 10 & 0 \\ 0 & -3x^2 + 8x + 10 \end{bmatrix} \\ &= \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = 0. \qquad \checkmark \end{aligned}$$

13 Nakayama's lemma

Throughout these notes, we work over a commutative ring R.

13.1 Nakayama's lemma

Proposition 13.1.1. *Let M be a finitely generated R-module, $I \subseteq R$ an ideal, and $\varphi\colon M \to M$ an R-module endomorphism satisfying $\varphi(M) \subseteq IM$. Then φ satisfies an equation of the form*

$$\varphi^n + c_{n-1}\varphi^{n-1} + \cdots + c_1\varphi + c_0\mathrm{id} = 0$$

with coefficients $c_i \in I$.

Proof. Let $x_1, \ldots, x_n \in M$ be generators and let $q\colon R^n \twoheadrightarrow M$ be the corresponding surjective R-module homomorphism, given by $q(e_i) = x_i$. For each generator x_i, by assumption we have $\varphi(x_i) \in IM$, so that there is an R-linear combination

$$\varphi(x_i) = \sum_{j=1}^{n} a_{ji}x_j$$

with coefficients $a_{ji} \in I$. Those choices correspond to a lift $\psi\colon R^n \to R^n$ in the diagram

$$\begin{array}{ccc} R^n & \overset{\psi}{\dashrightarrow} & R^n \\ \downarrow{\scriptstyle q} & & \downarrow{\scriptstyle q} \\ M & \xrightarrow{\varphi} & M, \end{array}$$

represented by the $n \times n$ matrix $A = [a_{ij}]$. The matrix A has characteristic polynomial

$$p_A(t) = \det(tI - A) = t^n + c_{n-1}t^{n-1} + \cdots + c_0$$

with coefficients $c_i \in I$, since all entries of A lie in I. By the Cayley–Hamilton theorem, the endomorphism ψ satisfies its characteristic equation, i.e., the following equality holds in the R-algebra $\mathrm{End}_R(R^n) \cong \mathrm{Mat}_n(R)$:

$$p_\psi(\psi) = p_A(\psi) = \psi^n + c_{n-1}\psi^{n-1} + \cdots + c_0\mathrm{id} = 0.$$

Postcomposing with q yields the equal maps $R^n \to M$

$$\begin{aligned} & q\psi^n + c_{n-1}q\psi^{n-1} + \cdots + c_0q = 0 \\ \iff & \varphi^n q + c_{n-1}\varphi^{n-1}q + \cdots + c_0q = 0 \\ \iff & (\varphi^n + c_{n-1}\varphi^{n-1} + \cdots + c_0\mathrm{id})q = 0. \end{aligned}$$

Since $q\colon R^n \twoheadrightarrow M$ is an epimorphism, the second step of the composite must be zero:

$$\varphi^n + c_{n-1}\varphi^{n-1} + \cdots + c_0\mathrm{id} = 0. \qquad \square$$

Corollary 13.1.2. *Let M be a finitely generated R-module and $I \subseteq R$ an ideal satisfying $IM = M$. Then there is a scalar $r \in R$ satisfying $r \equiv 1 \mod I$ and $rM = 0$.*

Proof. By assumption, the identity endomorphism $\varphi = \mathrm{id}_M$ satisfies $\mathrm{id}_M(M) = M \subseteq IM$. By Proposition 13.1.1, there are coefficients $c_i \in I$ such that the following equality in $\mathrm{End}_R(M)$ holds:

$$\begin{aligned} &\mathrm{id} + c_{n-1}\mathrm{id} + \cdots + c_0\mathrm{id} = 0 \\ \iff &(1 + c_{n-1} + \cdots + c_0)\mathrm{id} = 0. \end{aligned}$$

Taking the scalar $r = 1 + c_{n-1} + \cdots + c_0$ yields the result. □

Proposition 13.1.3 (Nakayama's lemma)**.** *Let M be a finitely generated R-module and $I \subseteq R$ an ideal contained in the Jacobson radical* $\mathrm{Jac}(R)$*. Then the condition $IM = M$ implies $M = 0$.*

Proof. Assuming $IM = M$, let $r \in R$ be a scalar as in Corollary 13.1.2, i.e., satisfying $r \equiv 1 \mod I$ and $rM = 0$. The condition $r \equiv 1 \mod \mathrm{Jac}(R)$ implies that r is a unit in R, which yields:

$$r^{-1}rM = 0 \implies M = 0.$$ □

13.2 Application to generating sets

Nakayama's lemma is useful for determining whether some elements $x_1, \ldots, x_n \in M$ in a finitely generated module M are generators.

Corollary 13.2.1. *Let M be a finitely generated R-module, $N \subseteq M$ a submodule, and $I \subseteq R$ an ideal contained in the Jacobson radical* $\mathrm{Jac}(R)$*. Then the condition $M = IM + N$ implies $M = N$.*

Proof. In the quotient module M/N, we have the equality of submodules

$$I(M/N) = (IM + N)/N.$$

The condition $M = IM + N$ then yields

$$\begin{aligned} & I(M/N) = M/N \\ \implies & M/N = 0 \qquad \text{by Proposition 13.1.3} \\ \implies & M = N. \end{aligned}$$

□

Corollary 13.2.2. *Let M be a finitely generated R-module and $x_1, \ldots, x_n \in M$, and let $I \subseteq R$ be an ideal contained in the Jacobson radical* $\mathrm{Jac}(R)$*. If the images in the quotient module*

$$\overline{x_1}, \ldots, \overline{x_n} \in M/IM$$

generate M/IM, then the elements $x_1, \ldots, x_n$ generate M.

Note: The converse is also true, by Homework 7 Problem 1.

Proof. Consider the submodule of M generated by the x_i

$$N = \langle x_1, \ldots, x_n \rangle = \sum_{i=1}^{n} Rx_i.$$

The assumption that the $\overline{x_i}$ generate M/IM can be expressed as $IM + N = M$. By Corollary 13.2.1, we conclude

$$M = N = \langle x_1, \ldots, x_n \rangle.$$

□

Next, we focus on finding a generating set without redundant generators.

Definition 13.2.3. Let M be an R-module. A generating set $X \subseteq M$ is **minimal** if any proper subset $X' \subsetneq X$ does not generate M.

Example 13.2.4. Over a field k, a generating set (a.k.a. spanning set) $B \subset V$ of a k-vector space V is minimal if and only if it is a basis. Any two minimal generating sets $B, B' \subset V$ have the same cardinality, namely the dimension of V over k.

The analogous statement is **not** true over a general commutative ring R. A basis (if it exists) is always minimal, but a minimal generating set need not be a basis, and different minimal generating sets may have different cardinalities.

Example 13.2.5.
1. In the free abelian group $\mathbb{Z}$, the subsets $\{1\}$, $\{2,3\}$, and $\{6,10,15\}$ are minimal generating sets. Of those, only $\{1\}$ is a basis.
2. In the abelian group $\mathbb{Z}/6$, the subsets $\{\overline{1}\}$ and $\{\overline{2},\overline{3}\}$ are minimal generating sets. The abelian group $\mathbb{Z}/6$ does not have a basis, since it is not free (as a $\mathbb{Z}$-module). Note however that $\{\overline{1}\}$ is a basis of $\mathbb{Z}/6$ as a $\mathbb{Z}/6$-module.

Proposition 13.2.6. *Let M be a finitely generated R-module and $x_1,\dots,x_n \in M$, and let $I \subseteq R$ be an ideal contained in the Jacobson radical. Denote by $\overline{x} \in M/IM$ the reduction of $x \in M$ modulo I.*

1. *The set $\{x_1,\dots,x_n\}$ generates M if and only if the set $\{\overline{x_1},\dots,\overline{x_n}\}$ generates the quotient module M/IM.*
2. *The set $\{x_1,\dots,x_n\}$ is a minimal generating set of M if and only if the set $\{\overline{x_1},\dots,\overline{x_n}\}$ is a minimal generating set of M/IM.*

Proof. (1) The statement was Corollary 13.2.2.

(2) By part (1), a proper subset $X' \subsetneq X = \{x_1,\dots,x_n\}$ generates M if and only if the reduction $\overline{X'}$ generates M/IM. Therefore, X is a minimal generating set of M if and only if $\overline{X}$ is a minimal generating set of M/IM. □

The next statement is [AM69, §2 Exercise 10].

Proposition 13.2.7. *Let $f\colon M \to N$ be an R-module homomorphism where N is finitely generated, and let $I \subseteq R$ be an ideal contained in the Jacobson radical. If the reduction of f modulo I*

$$\overline{f}\colon M/IM \to N/IN$$

is surjective, then $f\colon M \to N$ is surjective.

Proof. Denote the cokernel of f by $C = \operatorname{coker}(f) = N/\operatorname{im}(f)$. Since N is a finitely generated module, so is the quotient module C. The reduction of the cokernel is the cokernel of the reduction:

$$C/IC \cong \operatorname{coker}\left(M/IM \xrightarrow{\overline{f}} N/IN\right).$$

(Show this as an exercise.) We deduce the equivalent conditions:

$$\begin{aligned}
&f \text{ is surjective}\\
\iff &C = \operatorname{coker}(f) = 0\\
\iff &C/IC = 0 \quad \text{by Nakayama}\\
\iff &\operatorname{coker}(\overline{(}f)) = 0\\
&\overline{f} \text{ is surjective.}
\end{aligned}$$

□

13.3 Over local rings

The above statements are particular useful over a *local* ring $(R, \mathfrak{m})$, in which case the Jacobson radical is the unique maximal ideal $\mathfrak{m} \subset R$. Specializing Proposition 13.2.6 to that setup yields the following.

Proposition 13.3.1. *Let $(R, \mathfrak{m})$ be a local ring with residue field $k = R/\mathfrak{m}$, M a finitely generated R-module, and $x_1, \dots, x_n \in M$. Denote by $\overline{x} \in M/\mathfrak{m}M$ the reduction of $x \in M$ modulo the maximal ideal.*

1. *The set $\{x_1, \dots, x_n\}$ generates M if and only if the set $\{\overline{x_1}, \dots, \overline{x_n}\}$ spans the k-vector space $M/\mathfrak{m}M$.*
2. *The set $\{x_1, \dots, x_n\}$ is a minimal generating set of M if and only if the set $\{\overline{x_1}, \dots, \overline{x_n}\}$ is a basis of the k-vector space $M/\mathfrak{m}M$.*

In particular, any two minimal generating sets of M have the same cardinality, namely $\dim_k(M/\mathfrak{m}M)$.

Remark 13.3.2.
1. If we pick any basis $\{b_1, \dots, b_n\}$ of the k-vector space $M/\mathfrak{m}M$ and any lifts $x_i \in M$ with $\overline{x_i} = b_i$, then Proposition 13.3.1 guarantees that $\{x_1, \dots, x_n\}$ is a minimal generating set of M.
2. Such a minimal generating set $\{x_1, \dots, x_n\}$ of M need *not* be a basis, since M might not be free. See for instance Homework 8 Problem 1.

Example 13.3.3. Let $\mathbb{Z}_{(5)}$ denote the 5-local integers and consider the $\mathbb{Z}_{(5)}$-module

$$M = \mathbb{Z}_{(5)} \oplus \mathbb{Z}_{(5)}/(5^8).$$

Show that the elements

$$a = \begin{bmatrix} \frac{1}{2} \\ \frac{13}{4} \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} \frac{8}{3} \\ \frac{1}{7} \end{bmatrix}$$

form a minimal generating set of M.

Solution. The ring $\mathbb{Z}_{(5)}$ is local with maximal ideal $(5) \subset \mathbb{Z}_{(5)}$ and residue field $\mathbb{Z}_{(5)}/(5) \cong \mathbb{F}_5$. Since M is a finitely generated $\mathbb{Z}_{(5)}$-module, it suffices to show that the reductions modulo the maximal ideal $\{\overline{a}, \overline{b}\}$ form a basis of the $\mathbb{F}_5$-vector space $M/5M$ to conclude that $\{a, b\}$ is a minimal generating set of M, by Proposition 13.3.1. Let us compute said vectors in

$M/5M \cong \mathbb{F}_5^2$:

$$\begin{aligned}
\overline{a} &= \begin{bmatrix} \frac{1}{2} \\ \frac{13}{4} \end{bmatrix} \\
&= \begin{bmatrix} (1)(2^{-1}) \\ (13)(4^{-1}) \end{bmatrix} \\
&= \begin{bmatrix} (1)(3) \\ (3)(4) \end{bmatrix} \\
&= \begin{bmatrix} 3 \\ 12 \end{bmatrix} \\
&= \begin{bmatrix} 3 \\ 2 \end{bmatrix}
\end{aligned}$$

$$\begin{aligned}
\overline{b} &= \begin{bmatrix} \frac{8}{3} \\ \frac{1}{7} \end{bmatrix} \\
&= \begin{bmatrix} (8)(3^{-1}) \\ (1)(7^{-1}) \end{bmatrix} \\
&= \begin{bmatrix} (3)(3^{-1}) \\ (1)(2^{-1}) \end{bmatrix} \\
&= \begin{bmatrix} 1 \\ 3 \end{bmatrix}.
\end{aligned}$$

The determinant

$$\begin{vmatrix} \overline{a} & \overline{b} \end{vmatrix} = \begin{vmatrix} 3 & 1 \\ 2 & 3 \end{vmatrix} = 9 - 2 = 7 \equiv 2 \in \mathbb{F}_5^\times$$

is invertible in $\mathbb{F}_5$. Therefore $\{\overline{a}, \overline{b}\}$ is indeed a basis of the $\mathbb{F}_5$-vector space $\mathbb{F}_5^2$, by Corollary 12.3.4. □

14 Exact sequences

Throughout these notes, we work with modules over a commutative ring R.

14.1 Exact sequences

Definition 14.1.1. A sequence of R-modules

$$\cdots \longrightarrow A_{n+1} \xrightarrow{f_{n+1}} A_n \xrightarrow{f_n} A_{n-1} \longrightarrow \cdots \tag{3}$$

is **exact at A_n** if the image of the previous map is the kernel of the next map:

$$\operatorname{im}(f_{n+1}) = \ker(f_n).$$

The sequence is called **exact** if it is exact at every position.

Remark 14.1.2. The inclusion $\operatorname{im}(f_{n+1}) \subseteq \ker(f_n)$ says that two consecutive maps compose to zero:

$$f_n \circ f_{n+1} = 0.$$

A sequence satisfying this weaker condition is called a **chain complex**, an important tool in homological algebra and algebraic topology. See MATH 842 and MATH 843 for more details.

Example 14.1.3. 1. The sequence

$$0 \longrightarrow A \longrightarrow 0$$

is exact if and only if $A = 0$ holds.

2. The sequence

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

is exact if and only if f is a monomorphism, i.e., an injective map.

Note that exactness of the sequence means exactness at A, because that is the only position where exactness makes sense. Exactness at B is not defined since the sequence does not have a map out of B.

3. The sequence

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

is exact if and only if g is an epimorphism, i.e., a surjective map.

As before, exactness of the sequence means exactness at C, because that is the only position where exactness makes sense. Exactness at B is not defined since the sequence does not have a map into B.

4. The sequence
$$0 \longrightarrow A \xrightarrow{f} B \longrightarrow 0$$
is exact if and only if f is an isomorphism.

Definition 14.1.4. A **short exact sequence** is an exact sequence of the form
$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0. \tag{4}$$

More explicitly:

- Exactness at A says that $f\colon A \hookrightarrow B$ is injective.
- Exactness at C says that $g\colon B \twoheadrightarrow C$ is surjective.
- Exactness at B says that the two maps are related by $\operatorname{im}(f) = \ker(g)$.

Remark 14.1.5. A sequence that extends infinitely in both directions as in Equation (3) is called a **long exact sequence**.

Example 14.1.6. Given any R-modules A and C, the sequence
$$0 \longrightarrow A \xrightarrow{\mathrm{inc}_A} A \oplus C \xrightarrow{\mathrm{proj}_C} C \longrightarrow 0 \tag{5}$$
is a short exact sequence. Here inc_A denotes the inclusion of the summand A and proj_C denotes the projection onto the factor C.

A short exact sequence isomorphic to one of the form (5) is called **split**.

I will resist the urge to mention the *splitting lemma*.

Example 14.1.7.

1. Any monomorphism of R-modules $f\colon A \hookrightarrow B$ extends to a short exact sequence
$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{q} \operatorname{coker}(f) \longrightarrow 0.$$
Here $q\colon B \twoheadrightarrow B/\operatorname{im}(f) = \operatorname{coker}(f)$ denotes the quotient map.
2. Any epimorphism of R-modules $g\colon B \twoheadrightarrow C$ extends to a short exact sequence
$$0 \longrightarrow \ker(g) \xrightarrow{\mathrm{inc}} B \xrightarrow{g} C \longrightarrow 0.$$
3. Since the maps appearing in a short exact sequence are of a special form, an arbitrary map of R-modules $f\colon A \to B$ need not appear in a short exact sequence. The next best thing is this: f extends to a 4-term exact sequence
$$0 \longrightarrow \ker(f) \xrightarrow{\mathrm{inc}} A \xrightarrow{f} B \xrightarrow{q} \operatorname{coker}(f) \longrightarrow 0.$$
Note that this construction generalizes the previous two parts.

Example 14.1.8. Let $n \geq 2$ be an integer.

1. The sequence of abelian groups

$$0 \longrightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{q} \mathbb{Z}/n \longrightarrow 0$$

   is a short exact sequence, where $q\colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$ denotes the quotient map.

2. The sequence of abelian groups

$$0 \longrightarrow \mathbb{Z}/n \xrightarrow{n} \mathbb{Z}/n^2 \xrightarrow{q} \mathbb{Z}/n \longrightarrow 0$$

   is also a short exact sequence.

Neither of those two short exact sequences is split.

What's that you say? You prefer polynomials rather than integers? Alright, here you go.

Example 14.1.9. Let k be a commutative ring and consider the polynomial algebra $k[x]$.

1. The sequence of $k[x]$-modules

$$0 \longrightarrow k[x] \xrightarrow{x} k[x] \xrightarrow{q} k \longrightarrow 0$$

   is a short exact sequence. Here $q\colon k[x] \twoheadrightarrow k[x]/(x) \cong k$ denotes the quotient map.

2. The sequence of $k[x]$-modules

$$0 \longrightarrow k \xrightarrow{x} k[x]/(x^2) \xrightarrow{q} k \longrightarrow 0$$

   is also a short exact sequence.

Neither of those two short exact sequences is split.

Warning 14.1.10. When saying that the sequence

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

is exact, we (and most authors) mean exact at B, because that is the only position where exactness makes sense, cf. Example 14.1.3.

14.2 Exact functors

For a commutative ring R, let Mod_R denote the category of R-modules.

Definition 14.2.1. A functor $F\colon \mathrm{Mod}_R \to \mathrm{Mod}_S$ is **additive** if it preserves the zero module $F(0) \cong 0$ and preserves direct sums:

$$F(A \oplus B) \cong F(A) \oplus F(B).$$

Lemma 14.2.2. *A functor $F\colon \mathrm{Mod}_R \to \mathrm{Mod}_S$ is additive if and only if it preserves the addition on each hom module, i.e., for all R-modules A and B, the induced map on hom sets*

$$F_{A,B}\colon \mathrm{Hom}_R(A,B) \to \mathrm{Hom}_S(FA, FB)$$

satisfies $F(f+g) = F(f) + F(g)$, and thus is a map of abelian groups.

In the next lecture, we will see that Hom functors and tensors products provide many examples of additive functors.

Example 14.2.3. The (Cartesian) square functor

$$F(A) = A^2 = A \times A$$

is additive. Indeed, the fact that finite products coincide with finite direct sums yields:

$$\begin{aligned} F(A \oplus B) &= (A \oplus B) \times (A \oplus B) \\ &\cong (A \oplus B) \oplus (A \oplus B) \\ &\cong (A \oplus A) \oplus (B \oplus B) \\ &\cong (A \times A) \oplus (B \times B) \\ &= F(A) \oplus F(B). \end{aligned}$$

In fact, this functor F is given by tensoring with the free R-module R^2:

$$\begin{aligned} F(A) &= A \times A \\ &\cong A \oplus A \\ &\cong (R \otimes_R A) \oplus (R \otimes_R A) \\ &\cong (R \oplus R) \otimes_R A \\ &\cong (R \times R) \otimes_R A \\ &= R^2 \otimes_R A. \end{aligned}$$

Example 14.2.4. The tensor square functor

$$F(A) = A^{\otimes 2} = A \otimes_R A$$

is **not** additive. Indeed, the fact that the tensor product preserves direct sums in each variable yields:

$$\begin{aligned} F(A \oplus B) &= (A \oplus B) \otimes_R (A \oplus B) \\ &\cong (A \otimes_R A) \oplus (A \otimes_R B) \oplus (B \otimes_R A) \oplus (B \otimes_R B) \\ &\cong F(A) \oplus F(B) \oplus (A \otimes_R B) \oplus (B \otimes_R A). \end{aligned}$$

The extra terms $(A \otimes_R B) \oplus (B \otimes_R A)$ are not always zero.

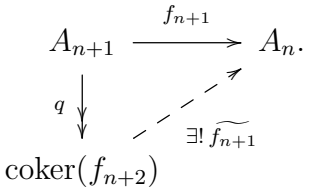
Lemma 14.2.5. *Consider a long exact sequence of R-modules*

$$\cdots \longrightarrow A_{n+2} \xrightarrow{f_{n+2}} A_{n+1} \xrightarrow{f_{n+1}} A_n \xrightarrow{f_n} A_{n-1} \xrightarrow{f_{n-1}} A_{n-2} \longrightarrow \cdots$$

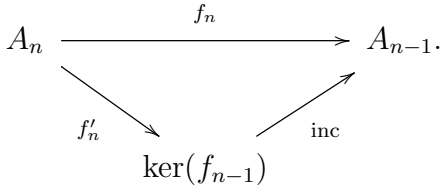
1. *For each index $n \in \mathbb{Z}$, we can extract a short exact sequence centered at the object A_n:*

$$0 \longrightarrow \operatorname{coker}(f_{n+2}) \xrightarrow{\widetilde{f_{n+1}}} A_n \xrightarrow{f'_n} \ker(f_{n-1}) \longrightarrow 0. \tag{6}$$

   Here $f'_n \colon A_n \to \operatorname{im}(f_n) = \ker(f_{n-1})$ denotes the corestriction of f_n onto its image, whereas $\widetilde{f_{n+1}}$ denotes the (unique) map induced by f_{n+1} out of the quotient:



2. *Conversely, given the short exact sequences* (6) *for all $n \in \mathbb{Z}$, we can recover the long exact sequence by expressing each map f_n as a composite*



Proof. Exercise. □

Definition 14.2.6. An additive functor $F \colon \mathrm{Mod}_R \to \mathrm{Mod}_S$ is **exact** if it preserves exact sequences, i.e., for every long exact sequence of R-modules (3), the induced sequence of S-modules

$$\cdots \longrightarrow F(A_{n+1}) \xrightarrow{F(f_{n+1})} F(A_n) \xrightarrow{F(f_n)} F(A_{n-1}) \longrightarrow \cdots$$

is also exact.

Lemma 14.2.7. *For an additive functor $F\colon \mathrm{Mod}_R \to \mathrm{Mod}_S$, the following conditions are equivalent.*

1. *F is exact.*
2. *F preserves short exact sequences, i.e., for every short exact sequence of R-modules (4), the induced sequence of S-modules*

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

   is also exact.

3. *For every exact sequence of R-modules $A \xrightarrow{f} B \xrightarrow{g} C$ (see Warning 14.1.10), the induced sequence of S-modules*

$$F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C)$$

   is also exact.

Proof. The equivalence (1) $\iff$ (2) follows from Lemma 14.2.5. The remaining implications are left as an exercise. □

Definition 14.2.8. An additive functor $F\colon \mathrm{Mod}_R \to \mathrm{Mod}_S$ is:

1. **left exact** if for every short exact sequence of R-modules (4), the induced sequence of S-modules

$$0 \longrightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \tag{7}$$

   is also exact. In particular, a left exact functor preserves injective maps.

2. **right exact** if for every short exact sequence of R-modules (4), the induced sequence of S-modules

$$F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \longrightarrow 0 \tag{8}$$

   is also exact. In particular, a right exact functor preserves surjective maps.

Lemma 14.2.9. *Let $F\colon \mathrm{Mod}_R \to \mathrm{Mod}_S$ be an additive functor.*

1. *F is left exact if and only if for every exact sequence of R-modules of the form*

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

   the induced sequence of S-modules (7) is also exact.

2. F is right exact if and only if for every exact sequence of R-modules of the form

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

the induced sequence of S-modules (8) *is also exact.*

Proof. Exercise. □

In the next lecture, we will learn that tensoring with a module $M \otimes_R -$ is right exact, whereas the Hom functors $\mathrm{Hom}_R(M, -)$ and $\mathrm{Hom}_R(-, M)$ are left exact.

14.3 Snake lemma

Proposition 14.3.1. *Consider a morphism of short exact sequences of R-modules, i.e., a commutative diagram*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\ 0 & \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & \longrightarrow & 0 \end{array}$$

where the rows are exact. There is an induced 6-term exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker(\alpha) & \xrightarrow{f_1} & \ker(\beta) & \xrightarrow{g_1} & \ker(\gamma) & & \\ & & & & & \searrow^{\delta} & & & \\ & & \operatorname{coker}(\alpha) & \xrightarrow{f_0} & \operatorname{coker}(\beta) & \xrightarrow{g_0} & \operatorname{coker}(\gamma) & \longrightarrow & 0 \end{array}$$

where:

- *The maps f_1 and g_1 are the restrictions of f and g to the kernels;*
- *The maps f_0 and g_0 are the maps induced on cokernels by f' and g';*
- *The connecting homomorphism $\delta\colon \ker(\gamma) \to \operatorname{coker}(\alpha)$ is defined as follows.*

Given an element $x \in \ker(\gamma)$, pick a preimage of x under g, apply β, then pick a (unique) preimage under f', then take the equivalence class modulo $\operatorname{im}(\alpha)$. The formula is illustrated schematically here:

$$\begin{array}{ccc} & & \widetilde{x} \xleftarrow{g^{-1}} x \\ & & \downarrow{\scriptstyle \beta} \\ & \overset{(f')^{-1}}{\longleftarrow} & \beta(\widetilde{x}) \\ \overline{x} & & \\ \downarrow{\scriptstyle q} & & \end{array}$$

$$q(\overline{x}) = \delta(x) \in \operatorname{coker}(\alpha).$$

Proof. Do it! It's a fun diagram chase. □

By mathematical law, I am obligated to refer you to the following explanation:

`https://www.youtube.com/watch?v=aXBNPjrvx-I`

Example 14.3.2. Consider the diagram of abelian groups with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{1} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle \begin{bmatrix} -1 \\ 1 \end{bmatrix}} & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z}^2 & \xrightarrow{\text{id}} & \mathbb{Z}^2 & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

The middle map $\beta = \left[\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right] : \mathbb{Z} \to \mathbb{Z}^2$ has kernel 0 and cokernel

$$\mathbb{Z}^2 / \langle \begin{bmatrix} -1 \\ 1 \end{bmatrix} \rangle \cong \mathbb{Z}$$

generated by the equivalence classes $[e_1] = [e_2]$. In this case, the 6-term exact sequence from the snake lemma

$$0 \longrightarrow \ker(\alpha) \longrightarrow \ker(\beta) \longrightarrow \ker(\gamma) \xrightarrow{\delta} \operatorname{coker}(\alpha) \longrightarrow \operatorname{coker}(\beta) \longrightarrow \operatorname{coker}(\gamma) \longrightarrow 0 \tag{9}$$

becomes

$$0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z} \xrightarrow{\delta = \left[\begin{smallmatrix} -1 \\ 1 \end{smallmatrix}\right]} \mathbb{Z}^2 \xrightarrow{[1\ 1]} \mathbb{Z} \longrightarrow 0 \longrightarrow 0.$$

Example 14.3.3. Consider the diagram of abelian groups with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{4} & \mathbb{Z} & \xrightarrow{q} & \mathbb{Z}/4 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 2} & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle q} & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{2} & \mathbb{Z} & \xrightarrow{q} & \mathbb{Z}/2 & \longrightarrow & 0 \end{array}$$

The left map $2\colon \mathbb{Z} \to \mathbb{Z}$ is injective with cokernel $\mathbb{Z}/2$. The middle map $1\colon \mathbb{Z} \to \mathbb{Z}$ is an isomorphism. The right map $q\colon \mathbb{Z}/4 \to \mathbb{Z}/2$ is surjective with kernel $\langle 2 \rangle \cong \mathbb{Z}/2$. The 6-term exact sequence (9) becomes

$$0 \longrightarrow 0 \longrightarrow 0 \longrightarrow \mathbb{Z}/2 \xrightarrow{\delta = 1} \mathbb{Z}/2 \longrightarrow 0 \longrightarrow 0 \longrightarrow 0.$$

In this case, exactness of the sequence forces $\delta = 1$. Nevertheless, we can compute the connecting homomorphism δ explicitly using the formula. It is given on the generator $\overline{2} \in \ker(\mathbb{Z}/4 \xrightarrow{q} \mathbb{Z}/2)$ by $\delta(\overline{2}) = \overline{1}$, as illustrated schematically here:

$$\begin{array}{ccc} & & 2 \xleftarrow{q^{-1}} \overline{2} \\ & & \downarrow{\scriptstyle 1} \\ 1 & \xleftarrow{2^{-1}} & 2 \\ \downarrow{\scriptstyle q} & & \\ \overline{1} = \delta(x) & \in & \operatorname{coker}(\mathbb{Z} \xrightarrow{2} \mathbb{Z}) = \mathbb{Z}/2. \end{array}$$

15 Hom modules

We introduced Hom modules in the lecture from September 29. In these notes, we look at more properties and examples of Hom modules, as well as the exactness properties of Hom functors.

15.1 Definitions and properties

Definition 15.1.1. Let R be a (not necessarily commutative) ring, and let M and N be left R-modules. The **Hom module** from M to N is the set of R-module homomorphisms from M to N:

$$\mathrm{Hom}_R(M,N) = \{f\colon M \to N \mid f \text{ is } R\text{-linear}\}.$$

Proposition 15.1.2. *Let R be a (not necessarily commutative) ring, and let M and N be left R-modules.*

1. *Pointwise addition of homomorphisms*

$$(f+g)(x) := f(x) + g(x)$$

makes $\mathrm{Hom}_R(M,N)$ *into an abelian group.*

2. *If the ring R is commutative, then pointwise scalar multiplication*

$$(rf)(x) := r \cdot f(x)$$

makes $\mathrm{Hom}_R(M,N)$ *into an R-module.*

Proof. 1. Exercise.

2. It suffices to show that for any scalar $r \in R$ and R-linear map $f\colon M \to N$, the pointwise scalar multiple $rf\colon M \to N$ is still R-linear. First, rf preserves addition:

$$\begin{aligned}(rf)(x+y) &= r \cdot f(x+y)\\ &= r \cdot (f(x) + f(y))\\ &= r \cdot f(x) + r \cdot f(y)\\ &= (rf)(x) + (rf)(y).\end{aligned}$$

Next, rf preserves scalar multiplication by R. For any scalar $c \in R$ and $x \in M$, we have:

$$\begin{aligned}(rf)(cx) &= r \cdot f(cx)\\ &= r \cdot (c \cdot f(x))\\ &= (rc) \cdot f(x)\\ &= (cr) \cdot f(x) \qquad \text{since } R \text{ is commutative}\\ &= c \cdot (r \cdot f(x))\\ &= c \cdot ((rf)(x)).\end{aligned}$$

□

Proposition 15.1.3. *Let R be a (not necessarily commutative) ring, and let M, N, and P be left R-modules.*

1. *Composition of homomorphisms is $\mathbb{Z}$-bilinear, thus inducing a composition map*

$$\begin{aligned} \mathrm{Hom}_R(N,P) \otimes_{\mathbb{Z}} \mathrm{Hom}_R(M,N) &\xrightarrow{\circ} \mathrm{Hom}_R(M,P) \\ g \otimes f &\longmapsto g \circ f \end{aligned}$$

2. *If the ring R is commutative, then composition of homomorphisms is R-bilinear, thus inducing a composition map*

$$\mathrm{Hom}_R(N,P) \otimes_R \mathrm{Hom}_R(M,N) \xrightarrow{\circ} \mathrm{Hom}_R(M,P)$$

Corollary 15.1.4. *Let R be a (not necessarily commutative) ring, and let M be a left R-module.*

1. *The composition product $\circ$ makes $\mathrm{End}_R(M) := \mathrm{Hom}_R(M,M)$ into a ring, called the **endomorphism ring** of M.*
2. *If the ring R is commutative, then $\mathrm{End}_R(M)$ is an R-algebra (usually non-commutative).*

As you can see, there are two stories running in parallel, depending whether R is assumed commutative or not. For the rest of the notes, let us focus on the case where R is commutative.

Proposition 15.1.5. *Let R be a commutative ring.*

1. *Given R-modules M_1, M_2, and N, restriction to the two summands yields a natural isomorphism of R-modules*

$$\begin{aligned} \mathrm{Hom}_R(M_1 \oplus M_2, N) &\xrightarrow{\cong} \mathrm{Hom}_R(M_1,N) \times \mathrm{Hom}_R(M_2,N) \\ f &\longmapsto (f|_{M_1}, f|_{M_2}). \end{aligned}$$

   More generally, given a family of R-modules $\{M_i\}_{i\in I}$, restriction to the summands yields a natural isomorphism of R-modules

$$\begin{aligned} \mathrm{Hom}_R(\textstyle\bigoplus_{i\in I} M_i, N) &\xrightarrow{\cong} \prod_{i\in I} \mathrm{Hom}_R(M_i,N) \\ f &\longmapsto (f|_{M_i})_{i\in I}. \end{aligned} \tag{10}$$

2. *Given R-modules M, N_1, and N_2, let $\mathrm{pr}_1 \colon N_1 \times N_2 \to N_1$ denote the projection onto the factor N_1. Projection onto the two factors yields a natural isomorphism of R-modules*

$$\begin{aligned} \mathrm{Hom}_R(M, N_1 \times N_2) &\xrightarrow{\cong} \mathrm{Hom}_R(M, N_1) \times \mathrm{Hom}_R(M, N_2) \\ f &\longmapsto (\mathrm{pr}_1 \circ f, \mathrm{pr}_2 \circ f). \end{aligned}$$

More generally, given a family of R-modules $\{N_i\}_{i \in I}$, projection onto the factors yields a natural isomorphism of R-modules

$$\begin{aligned} \mathrm{Hom}_R(M, \textstyle\prod_{i \in I} N_i) &\xrightarrow{\cong} \prod_{i \in I} \mathrm{Hom}_R(M, N_i) \\ f &\longmapsto (\mathrm{pr}_i \circ f)_{i \in I}. \end{aligned}$$

Proof. Let us prove the first part; the second part is dual. For each index $i \in I$, restriction onto the i^{th} summand

$$\begin{aligned} \mathrm{inc}_i^* \colon \mathrm{Hom}_R(\textstyle\bigoplus_{j \in I} M_j, N) &\longrightarrow \mathrm{Hom}_R(M_i, N) \\ f &\longmapsto f|_{M_i} = f \circ \mathrm{inc}_i \end{aligned}$$

is an R-module homomorphism. As i varies, those restriction maps assemble into an R-module homomorphism (10). Since the direct sum $\bigoplus_{i \in I} M_i$ is the coproduct in R-modules, the map (10) is a bijection, hence an isomorphism. □

Warning 15.1.6. Since the infinite direct sum $\bigoplus_{i \in I} N_i$ is not a product of R-modules in general, the Hom module

$$\mathrm{Hom}_R(M, \bigoplus_{i \in I} N_i)$$

could be strange. Dually, since the infinite product $\prod_{i \in I} M_i$ is not a coproduct of R-modules in general, the Hom module

$$\mathrm{Hom}_R(\prod_{i \in I} M_i, N)$$

could be strange.

For example, Specker's theorem says that

$$\mathrm{Hom}_{\mathbb{Z}}(\prod_{i=1}^{\infty} \mathbb{Z}, \mathbb{Z}) \cong \bigoplus_{i=1}^{\infty} \mathbb{Z}$$

is a free abelian group with basis the projection maps $\mathrm{pr}_i \colon \prod_{j=1}^{\infty} \mathbb{Z} \to \mathbb{Z}$, a fact that still blows my mind to this day. I felt the need to express my feelings publicly:

`https://uregina.ca/~franklam/Frankland_HawaiianEarring_20170222.pdf`

15.2 Some examples

Lemma 15.2.1. *Let R be a commutative ring, let M and N be R-modules, and $m \in M$ any element. Then evaluation at m*

$$\begin{aligned} \mathrm{ev}_m \colon \mathrm{Hom}_R(M,N) &\longrightarrow N \\ f &\longmapsto f(m) \end{aligned}$$

is an R-module homomorphism.

Proposition 15.2.2. *Let R be a commutative ring. For any R-module M, there is a natural isomorphism of R-modules*

$$\mathrm{Hom}_R(R,M) \xrightarrow{\cong} M.$$

Proof. Evaluation at $1 \in R$

$$\mathrm{ev}_1 \colon \mathrm{Hom}_R(R,M) \xrightarrow{\cong} M$$

is the desired isomorphism. Checking the details is left as an exercise. □

Now let us generalize Proposition 15.2.2.

Proposition 15.2.3. *Let R be a commutative ring and F a free R-module with basis $\{b_i\}_{i\in I}$. For any R-module M, there is an isomorphism of R-modules*

$$\mathrm{Hom}_R(F,M) \xrightarrow{\cong} \prod_{i\in I} M \tag{11}$$

which is natural in M.

In particular, we have

$$\mathrm{Hom}_R(R^n,M) \cong M^n.$$

Proof. For each index $i \in I$, evaluation at the basis element b_i

$$\mathrm{ev}_{b_i} \colon \mathrm{Hom}_R(F,M) \to M$$

is an R-module homomorphism, by Lemma 15.2.1. As i varies, those evaluation maps assemble into an R-module homomorphism (11). By the universal property of free modules, the map (11) is a bijection, hence an isomorphism. □

Remark 15.2.4. Given a free R-module F, a choice of basis $\{b_i\}_{i\in I}$ is the same data as an isomorphism of R-modules

$$\begin{aligned} \varphi \colon \textstyle\bigoplus_{i\in I} R &\xrightarrow{\cong} F \\ e_i &\longmapsto b_i. \end{aligned}$$

The isomorphism in Proposition 15.2.3 is the composite of the three isomorphisms

$$\operatorname{Hom}_R(F, M) \xrightarrow[\cong]{\varphi^*} \operatorname{Hom}_R(\textstyle\bigoplus_{i\in I} R, M) \xrightarrow[\cong]{(\mathrm{inc}_i^*)_{i\in I}} \prod_{i\in I} \operatorname{Hom}_R(R, M) \xrightarrow[\cong]{\prod_{i\in I} \mathrm{ev}_1} \prod_{i\in I} M$$

from Propositions 15.1.5 and 15.2.2.

Example 15.2.5. Let R be a commutative ring. In the notes from October 13 §1, we saw there there is an isomorphism of R-modules

$$\operatorname{Hom}_R(R^n, R^m) \cong \operatorname{Mat}_{m\times n}(R)$$

between maps $R^n \to R^m$ and $m \times n$ matrices with entries in R. As an R-module, the module of matrices is free of rank mn:

$$\operatorname{Hom}_R(R^n, R^m) \cong (R^m)^n \cong R^{mn}$$

by Proposition 15.2.3. However, matrix notation allows us to express the composition product from Proposition 15.1.3 as matrix multiplication. In particular, the isomorphism

$$\operatorname{End}_R(R^n) \cong \operatorname{Mat}_n(R)$$

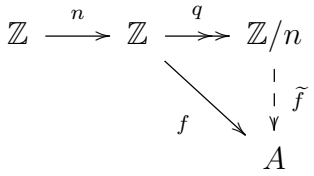
is an isomorphism of R-algebras.

Proposition 15.2.6. *For any integer $n \geq 1$ and abelian group A, there is a natural isomorphism of abelian groups*

$$\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, A) \cong \{a \in A \mid na = 0\},$$

the n-torsion subgroup of A.

Proof. By the universal property of the quotient module:



a map $\mathbb{Z}/n \to A$ is the same as a map $\mathbb{Z} \to A$ that vanishes on the submodule $n\mathbb{Z}$. This yields natural isomorphisms:

$$\begin{aligned}\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, A) &\cong \{f\colon \mathbb{Z} \to A \mid f \circ n = 0\} \\ &\cong \{a \in A \mid na = 0\} \qquad \text{by Proposition 15.2.2} \\ &= \ker\left(A \xrightarrow{n} A\right).\end{aligned}$$

□

Remark 15.2.7. The n-torsion subgroup of A is sometimes denoted ${}_nA$, a notation I picked up in classic work of Cartan [Car54].

The same proof shows the following more general fact.

Proposition 15.2.8. *Let R be a commutative ring. For any scalar $r \in R$ and R-module M, there is a natural isomorphism of R-modules*

$$\begin{aligned}\mathrm{Hom}_R(R/r, M) &\cong \{x \in M \mid rx = 0\} \\ &= \ker\left(M \xrightarrow{r} M\right),\end{aligned}$$

the r-torsion submodule of M.

Example 15.2.9. Working over $R = \mathbb{Z}$, let us compute some Hom abelian groups.

1. $\mathrm{Hom}(\mathbb{Z}/n, \mathbb{Z}) = 0$, since $\mathbb{Z}$ is torsion-free.
2. $$\mathrm{Hom}(\mathbb{Z}/2, \mathbb{Z}/6) \cong {}_2(\mathbb{Z}/6) = 3(\mathbb{Z}/6) \cong \mathbb{Z}/2.$$
   Alternately, we can use the Chinese remainder theorem:
   $$\begin{aligned}\mathrm{Hom}(\mathbb{Z}/2, \mathbb{Z}/6) &\cong \mathrm{Hom}(\mathbb{Z}/2, \mathbb{Z}/2 \oplus \mathbb{Z}/3) \\ &\cong \mathrm{Hom}(\mathbb{Z}/2, \mathbb{Z}/2) \oplus \mathrm{Hom}(\mathbb{Z}/2, \mathbb{Z}/3) && \text{by Proposition 15.1.5} \\ &\cong {}_2(\mathbb{Z}/2) \oplus {}_2(\mathbb{Z}/3) && \text{by Proposition 15.2.6} \\ &= \mathbb{Z}/2 \oplus 0 && \text{since 2 acts invertibly on } \mathbb{Z}/3 \\ &\cong \mathbb{Z}/2.\end{aligned}$$
3. $$\mathrm{Hom}(\mathbb{Z}/6, \mathbb{Z}/10) \cong {}_6(\mathbb{Z}/10) = 5(\mathbb{Z}/10) \cong \mathbb{Z}/2.$$
   Alternately, we can use the Chinese remainder theorem:
   $$\begin{aligned}\mathrm{Hom}(\mathbb{Z}/6, \mathbb{Z}/10) &\cong \mathrm{Hom}(\mathbb{Z}/2 \oplus \mathbb{Z}/3, \mathbb{Z}/2 \oplus \mathbb{Z}/5) \\ &\cong \mathrm{Hom}(\mathbb{Z}/2, \mathbb{Z}/2) \oplus \mathrm{Hom}(\mathbb{Z}/2, \mathbb{Z}/5) \oplus \mathrm{Hom}(\mathbb{Z}/3, \mathbb{Z}/2) \oplus \mathrm{Hom}(\mathbb{Z}/3, \mathbb{Z}/5) \\ &\cong {}_2(\mathbb{Z}/2) \oplus {}_2(\mathbb{Z}/5) \oplus {}_3(\mathbb{Z}/2) \oplus {}_3(\mathbb{Z}/5) \\ &\cong \mathbb{Z}/2 \oplus 0 \oplus 0 \oplus 0 \\ &\cong \mathbb{Z}/2.\end{aligned}$$

Proposition 15.2.10. *The* Hom *abelian group between cyclic abelian groups is*

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/m, \mathbb{Z}/n) \cong \mathbb{Z}/\gcd(m, n)$$

for all integers $m, n \geq 1$.

Proof. The Hom abelian group in question is the m-torsion subgroup of $\mathbb{Z}/n$. Writing $d := \gcd(m, n)$, we have:

$$\begin{aligned}\mathrm{Hom}(\mathbb{Z}/m, \mathbb{Z}/n) &\cong {}_m(\mathbb{Z}/n) \\ &= \langle \frac{n}{d} \rangle \qquad \text{as a submodule of } \mathbb{Z}/n \\ &\cong \mathbb{Z}/d,\end{aligned}$$

since $\frac{n}{d} \in \mathbb{Z}/n$ has (additive) order d. □

Example 15.2.11. $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = 0$, since no integer is infinitely divisible. More precisely, let $f \colon \mathbb{Q} \to \mathbb{Z}$ be a linear map. For any rational number $r \in \mathbb{Q}$, the value of f is

$$f(r) = f(\frac{n}{n} r) = n f(\frac{r}{n})$$

for any integer $n \neq 0$, since f is $\mathbb{Z}$-linear. Hence $f(r)$ is divisible by every integer $n \neq 0$, which forces $f(r) = 0$.

Exercise 15.2.12. Compute the Hom abelian group

$$\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z} \oplus \mathbb{Z}/9 \oplus \mathbb{Q}, \mathbb{Z}^2 \oplus \mathbb{Z}/15).$$

15.3 Left exactness of Hom

The Hom functor is left exact in each variable, in the following sense.

Proposition 15.3.1. *Let R be a commutative ring, let M and N be R-modules, and*

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

a short exact sequence of R-modules.

1. *The sequence of R-modules*

$$0 \longrightarrow \mathrm{Hom}_R(M, A) \xrightarrow{f_*} \mathrm{Hom}_R(M, B) \xrightarrow{g_*} \mathrm{Hom}_R(M, C)$$

   is exact. In other words, the covariant Hom *functor* $\mathrm{Hom}_R(M, -)\colon \mathrm{Mod}_R \to \mathrm{Mod}_R$ *is left exact.*

2. *The sequence of R-modules*

$$0 \longrightarrow \mathrm{Hom}_R(C, N) \xrightarrow{g^*} \mathrm{Hom}_R(B, N) \xrightarrow{f^*} \mathrm{Hom}_R(A, N)$$

   is exact. In other words, the contravariant Hom *functor* $\mathrm{Hom}_R(-, N)\colon \mathrm{Mod}_R^{\mathrm{op}} \to \mathrm{Mod}_R$ *is left exact.*

Proof. Let us prove the first statement; the proof of the second statement is similar.

Exactness at $\mathrm{Hom}_R(M, A)$. We want to show that $f\colon A \hookrightarrow B$ being a monomorphism ensures that the postcomposition map $f_*\colon \mathrm{Hom}_R(M, A) \to \mathrm{Hom}_R(N, B)$ is also a monomorphism. Let $\varphi \in M \to A$ be a map satisfying $f_*(\varphi) = f\varphi = 0\colon M \to B$. Since f is a monomorphism, we deduce:

$$\begin{aligned} & f(\varphi(x)) = 0 \quad \text{for all } x \in M \\ \implies & \varphi(x) = 0 \quad \text{for all } x \in M \\ \implies & \varphi = 0, \end{aligned}$$

which shows that f_* is a monomorphism.

Exactness at $\mathrm{Hom}_R(M, B)$. We will prove $\mathrm{im}(f_*) = \ker(g_*)$ by showing the two inclusions separately.

($\mathrm{im}(f_*) \subseteq \ker(g_*)$) Because of the relation $gf = 0$, for any map $\varphi \in M \to A$, we have

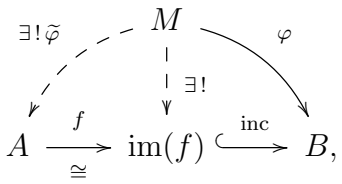
$$g_*(f_*(\varphi)) = gf\varphi = 0$$

and thus $f_*(\varphi) \in \ker(g_*)$.

($\ker(g_*) \subseteq \operatorname{im}(f_*)$) Let $\varphi\colon M \to B$ be a map whose postcomposition by g vanishes: $g_*(\varphi) = g\varphi = 0\colon M \to C$. Then φ lands in the kernel of g:

$$\begin{aligned} & g(\varphi(x)) = 0 \quad \text{for all } x \in M \\ \implies & \varphi(x) \in \ker(g) \quad \text{for all } x \in M \\ \implies & \operatorname{im}(\varphi) \subseteq \ker(g). \end{aligned}$$

But exactness of the original sequence at B says $\ker(g) = \operatorname{im}(f)$. Moreover, $f\colon A \hookrightarrow B$ is an isomorphism onto its image $\operatorname{im}(f) \subseteq B$, since f is a monomorphism. Therefore $\varphi\colon M \to B$ lifts (uniquely) to a map $\widetilde{\varphi}\colon M \to A$, as illustrated in the diagram



where $f\colon A \to \operatorname{im}(f)$ denotes the corestriction of f (by abuse of notation). The equation $\varphi = f\widetilde{\varphi} = f_*(\widetilde{\varphi})$ shows $\varphi \in \operatorname{im}(f_*)$. □

Remark 15.3.2. The statement holds more generally for any (not necessarily commutative) ring R and (say) left R-modules, as long as we view the Hom modules $\operatorname{Hom}_R(M, A)$ merely as abelian groups, as in Proposition 15.1.2. I didn't feel like using the word "left" in two completely different ways in the same sentence.

Example 15.3.3. Consider the short exact sequence of abelian groups

$$0 \longrightarrow \mathbb{Z} \xrightarrow{n} \mathbb{Z} \xrightarrow{q} \mathbb{Z}/n \longrightarrow 0 \tag{12}$$

where $q\colon \mathbb{Z} \twoheadrightarrow \mathbb{Z}/n$ denotes the quotient map. Applying the functor $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, -)$ yields the sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) & \xrightarrow{n_*} & \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) & \xrightarrow{q_*} & \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/n) & \longrightarrow & 0 \\ & & \| & & \| & & \downarrow \cong & & \\ & & 0 & & 0 & & \mathbb{Z}/n & & \end{array}$$

which is **not** exact at the third object $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}/n)$. This shows that the functor $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, -)$ is not exact.

Now apply the functor $\operatorname{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ to (12), yielding the sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}/n, \mathbb{Z}) & \xrightarrow{q^*} & \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) & \xrightarrow{n^*} & \operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}) & \longrightarrow & 0 \\ & & \| & & \downarrow \cong & & \downarrow \cong & & \\ & & 0 & & \mathbb{Z} & \xrightarrow{\quad n \quad} & \mathbb{Z} & & \end{array}$$

which is **not** exact at the third object $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z})$. This shows that the functor $\operatorname{Hom}_{\mathbb{Z}}(-, \mathbb{Z})$ is not exact.

For some modules, Hom functors happen to be exact.

Example 15.3.4. Given a short exact sequence of R-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$, applying the functor $\mathrm{Hom}_R(R, -)$ yields a sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_R(R, A) & \xrightarrow{f_*} & \mathrm{Hom}_R(R, B) & \xrightarrow{g_*} & \mathrm{Hom}_R(R, C) & \longrightarrow & 0 \\ & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \\ & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & & \end{array}$$

which is isomorphic to the original sequence, hence still exact. This shows that the functor $\mathrm{Hom}_R(R, -)$ is exact.

This holds more generally for $\mathrm{Hom}_R(F, -)$ for any free R-module F, by Proposition 15.2.3 and the fact that products of exact sequences are exact.

Definition 15.3.5. An R-module M is **projective** if the functor $\mathrm{Hom}_R(M, -)$ is exact. The module M is **injective** if the functor $\mathrm{Hom}_R(-, M)$ is exact.

Example 15.3.3 shows that the abelian group $\mathbb{Z}/n$ is not projective and $\mathbb{Z}$ is not injective. Example 15.3.4 shows that $\mathbb{Z}$ is projective, as is any free abelian group $\bigoplus_{i \in I} \mathbb{Z}$.

Projective modules and injective modules play an important role in homological algebra. See MATH 843 for more details.

16 A note on $\lim^1$

These notes supplement a presentation on completions. More details about $\lim^1$ can be found in [BK72, §IX.2], [MP12, §2.2–2.4], [Wei94, §3.5], as well as here:

`https://ncatlab.org/nlab/show/lim%5E1+and+Milnor+sequences`

and the references therein.

16.1 Diagrams of abelian groups

Notation 16.1.1. For a small category I and a category $\mathcal{C}$, denote by $\mathcal{C}^I = \mathrm{Fun}(I, \mathcal{C})$ the category of I-shaped diagrams in $\mathcal{C}$, i.e., functors $I \to \mathcal{C}$ and natural transformations between them.

Example 16.1.2. Consider the natural numbers $\mathbb{N}$ as a totally ordered set $\{1 < 2 < 3 < \cdots\}$, viewed as a category. Then $\mathcal{C}^{\mathbb{N}}$ is the category of sequences in $\mathcal{C}$:

$$X_1 \xrightarrow{f_1} X_2 \xrightarrow{f_2} X_3 \longrightarrow \cdots$$

A morphism of sequences $\varphi\colon X \to Y$ is a commutative diagram

$$\begin{array}{ccccccc} X_1 & \xrightarrow{f_1} & X_2 & \xrightarrow{f_2} & X_3 & \longrightarrow & \cdots \\ \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_3} & & \\ Y_1 & \xrightarrow{g_1} & Y_2 & \xrightarrow{g_2} & Y_3 & \longrightarrow & \cdots \end{array}$$

Example 16.1.3. Taking the opposite order $\mathbb{N}^{\mathrm{op}}$, the category $\mathcal{C}^{\mathbb{N}^{\mathrm{op}}}$ is the category of towers in $\mathcal{C}$:

$$X_1 \xleftarrow{f_1} X_2 \xleftarrow{f_2} X_3 \longleftarrow \cdots$$

For psychological reasons, I like to display towers vertically:

$$\begin{array}{c} \vdots \\ \downarrow \\ X_3 \\ \downarrow{\scriptstyle f_2} \\ X_2 \\ \downarrow{\scriptstyle f_1} \\ X_1. \end{array}$$

Notation 16.1.4. Denote by $c\colon \mathcal{C} \to \mathcal{C}^I$ the constant diagram functor, also called the diagonal functor and denoted Δ. More explicitly, the constant diagram $c(X)$ has the object $c(X)_i = X$ at every index $i \in I$ and id_X as transition maps.

Assuming that $\mathcal{C}$ admits I-shaped limits, the limit functor $\lim_I$ is right adjoint to the constant functor:

$$c\colon \mathcal{C} \rightleftarrows \mathcal{C}^I \colon \lim_I .$$

For the rest of this note, let us specialize to the category of abelian groups Ab. Since Ab is a complete and cocomplete abelian category, so is any diagram category Ab^I.

Proposition 16.1.5. *The limit functor*

$$\lim_I \colon : \mathrm{Ab}^I \to \mathrm{Ab}$$

is left exact.

Proof. Since the functor $\lim_I$ is a right adjoint, it preserves all limits, in particular finite limits. Hence $\lim_I$ is additive and left exact. □

Definition 16.1.6. The functor $\lim_I^s \colon : \mathrm{Ab}^I \to \mathrm{Ab}$ is the s^{th} right derived functor of $\lim_I$.

16.2 The $\lim^1$ functor

Now we specialize further to *towers* of abelian groups, taking the indexing category $\mathbb{N}^{\mathrm{op}}$. We will write lim or $\lim_n$ instead of $\varprojlim_{\mathbb{N}^{\mathrm{op}}}$.

Proposition 16.2.1. *The functors* $\lim^s \colon \mathrm{Ab}^{\mathbb{N}^{\mathrm{op}}} \to \mathrm{Ab}$ *are trivial for* $s \geq 2$.

Proposition 16.2.2. *Given a tower of abelian groups* $A = \left(\cdots \xrightarrow{f_2} A_2 \xrightarrow{f_1} A_1\right)$, *consider the map of abelian groups*

$$\prod_{n=1}^{\infty} A_n \xrightarrow{\partial} \prod_{n=1}^{\infty} A_n$$

$$(a_n) \longmapsto (a_n - f_n(a_{n+1})).$$

Then we have

$$\ker(\partial) \cong \varprojlim_n A_n$$

$$\mathrm{coker}(\partial) \cong \lim_n^1 A_n.$$

Note that $\ker(\partial)$ is the standard construction of the limit as a subset of the product. The content of the proposition is providing an explicit construction of $\lim^1 A$.

Definition 16.2.3. A tower of abelian groups $A = \left(\cdots \xrightarrow{f_2} A_2 \xrightarrow{f_1} A_1\right)$ satisfies the **Mittag-Leffler condition** if for all $k \geq 1$, the images in A_k stabilize, i.e., there exists an index $i = i(k)$ such that for all $j \geq i$, the following equality holds:

$$\mathrm{im}(A_j \to A_k) = \mathrm{im}(A_i \to A_k).$$

Example 16.2.4. If the transition maps $f_n \colon A_{n+1} \to A_n$ are surjective for n large enough, then the tower A satisfies the Mittag-Leffler condition.

Proposition 16.2.5. *If a tower of abelian groups* A *satisfies the Mittag-Leffler condition, then its* $\lim^1$ *is trivial:* $\lim^1 A = 0$.

16.3 A small example

For an integer $p \geq 2$, denote by $\mathbb{Z}[p]$ the tower with $\mathbb{Z}$ in every degree and the multiplication map $p\colon \mathbb{Z} \to \mathbb{Z}$ as transition maps:

$$\begin{array}{c} \vdots \\ \downarrow \\ \mathbb{Z} \\ \downarrow{\scriptstyle p} \\ \mathbb{Z} \\ \downarrow{\scriptstyle p} \\ \mathbb{Z}. \end{array}$$

Proposition 16.3.1. $\lim^1 \mathbb{Z}[p] \cong \mathbb{Z}_p/\mathbb{Z}$, *where* $\mathbb{Z}_p$ *denotes the* p*-adic integers.*

Proof. Consider the short exact sequence of towers of abelian groups

$$0 \to \mathbb{Z}[p] \to c(\mathbb{Z}) \to \mathbb{Z}/p^\bullet \to 0,$$

displayed more explicitly in the diagram of abelian groups with exact rows

$$\begin{array}{ccccccccc} & & \vdots & & \vdots & & \vdots & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{p^3} & \mathbb{Z} & \xrightarrow{q} & \mathbb{Z}/p^3 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle q} & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{p^2} & \mathbb{Z} & \xrightarrow{q} & \mathbb{Z}/p^2 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle 1} & & \downarrow{\scriptstyle q} & & \\ 0 & \longrightarrow & \mathbb{Z} & \xrightarrow{p} & \mathbb{Z} & \xrightarrow{q} & \mathbb{Z}/p & \longrightarrow & 0 \end{array}$$

where each map labeled q is the canonical quotient map. Applying the left exact functor lim yields a long exact sequence of abelian groups

$$0 \to \lim \mathbb{Z}[p] \to \lim c(\mathbb{Z}) \to \lim \mathbb{Z}/p^\bullet \to \lim^1 \mathbb{Z}[p] \to \lim^1 c(\mathbb{Z}) \to \lim^1 \mathbb{Z}/p^\bullet \to 0. \tag{13}$$

The first term vanishes:

$$\lim_n \mathbb{Z}[p] = 0,$$

since no integer is infinitely divisible by p. The next terms are

$$\lim_n c(\mathbb{Z}) \cong \mathbb{Z}$$

and the p-adic integers

$$\lim_n \mathbb{Z}/p^n = \mathbb{Z}_p.$$

The last two terms are

$$\lim{}^1 c(\mathbb{Z}) = 0$$
$$\lim{}^1 \mathbb{Z}/p^\bullet = 0$$

by Proposition 16.2.5, since both towers $c(\mathbb{Z})$ and $\mathbb{Z}/p^\bullet = \{\mathbb{Z}/p^n\}_{n\geq 1}$ have surjective transition maps. The six-term exact sequence (13) thus simplifies to

$$0 \to 0 \to \mathbb{Z} \to \mathbb{Z}_p \to \lim{}^1 \mathbb{Z}[p] \to 0 \to 0 \to 0,$$

which yields the isomorphism

$$\lim{}^1 \mathbb{Z}[p] \cong \mathbb{Z}_p/\mathbb{Z}$$

as claimed. □

Remark 16.3.2. The example in Proposition 16.3.1 is found in [BK72, Example IX.2.5] and [Wei94, Example 3.5.5]. It also appears in topology; see for instance:

`https://math.stackexchange.com/questions/766364/is-there-any-simple-example-that-lim1-terms-appear`

Next, we revisit the calculation above using a more hands-on method.

Alternate proof. Proposition 16.2.2 gives a formula $\lim^1 \mathbb{Z}[p] \cong \operatorname{coker}(\partial)$. For the tower $\mathbb{Z}[p]$, the map ∂ is

$$\prod_{n=1}^\infty \mathbb{Z} \xrightarrow{\partial} \prod_{n=1}^\infty \mathbb{Z}$$

$$(a_n) \longmapsto (a_n - pa_{n+1}).$$

Writing $e_k \in \prod_{n=1}^\infty \mathbb{Z}$ for the sequence with a 1 in the k^{th} coordinate, we have

$$\partial(e_k) = (0, \ldots, \overbrace{-p}^{k-1}, \overbrace{1}^{k}, 0, \ldots)$$

which is modded out in $\operatorname{coker}(\partial)$. This imposes the following relation in $\operatorname{coker}(\partial)$:

$$(0, \ldots, \overbrace{p}^{k-1}, 0, \ldots) = (0, \ldots, \overbrace{1}^{k}, 0, \ldots).$$

These relations for all $k \geq 2$ are the same as those imposed on p-adic expansions

$$\sum_{n=1}^\infty b_n p^{n-1}.$$

Let us describe the image of ∂. For general $a = (a_n)$ and $b = (b_n)$ in $\prod_{n=1}^{\infty} \mathbb{Z}$, the equation $\partial(a) = b$ is equivalent to

$$\begin{aligned} & a_n - pa_{n+1} = b_n \\ \iff & a_n = b_n + pa_{n+1} \end{aligned}$$

for all $n \geq 1$. Applying these equations recursively yields

$$\begin{aligned} a_1 &= b_1 + b_2 p + b_3 p^2 + \cdots \\ a_2 &= b_2 + b_3 p + b_4 p^2 + \cdots \\ a_3 &= b_3 + b_4 p + b_5 p^2 + \cdots \\ &\vdots \end{aligned}$$

Since the a_n must be integers, the p-adic expansion

$$a_1 = \sum_{n=1}^{\infty} b_n p^{n-1}$$

must stop. The argument shows that the (surjective) map

$$\begin{array}{ccc} \prod_{n=1}^{\infty} \mathbb{Z} & \xrightarrow{\quad \varphi \quad} & \mathbb{Z}_p \\ (b_n) & \longmapsto & \sum_{n=1}^{\infty} b_n p^{n-1} \end{array}$$

satisfies $\varphi(\mathrm{im}(\partial)) = \mathbb{Z}$, equivalently, $\mathrm{im}(\partial) \subseteq \varphi^{-1}(\mathbb{Z})$. The reverse inclusion also holds: $\mathrm{im}(\partial) = \varphi^{-1}(\mathbb{Z})$. By the first and third isomorphism theorems, we obtain

$$\begin{aligned} \mathrm{coker}(\partial) &= \left(\prod_{n=1}^{\infty} \mathbb{Z} \right) / \mathrm{im}(\partial) \\ &= \left(\prod_{n=1}^{\infty} \mathbb{Z} \right) / \varphi^{-1}(\mathbb{Z}) \\ &\cong \mathbb{Z}_p / \mathbb{Z}. \end{aligned}$$

□

References

[AM69] M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. MR0242802

[BK72] A. K. Bousfield and D. M. Kan, *Homotopy limits, Completions and Localizations*, Lecture Notes in Mathematics, vol. 304, Springer-Verlag, 1972.

[Car54] H. Cartan, *Sur les groupes d'Eilenberg-Mac Lane. II*, Proc. Nat. Acad. Sci. U. S. A. **40** (1954), 704–707 (French). MR0065161

[DF04] D. S. Dummit and R. M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236

[MP12] J. P. May and K. Ponto, *More concise algebraic topology*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 2012. Localization, completion, and model categories. MR2884233

[Rei95] M. Reid, *Undergraduate commutative algebra*, London Mathematical Society Student Texts, vol. 29, Cambridge University Press, Cambridge, 1995. MR1458066

[Wei94] C. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, Cambridge University Press, 1994.

[Bra17] M. Brandenburg, *The nil-radical is an intersection of all prime ideals proof* (July 7, 2017), `https://math.stackexchange.com/questions/859390/the-nil-radical-is-an-intersection-of-all-prime-ideals-proof`. Accessed Sep. 19, 2022.

