Some Notes on Rings

Greyson C. Wesley

Version of February 5, 2024 at 11:53am EST

Abstract

These notes follow MATH 6111—Abstract Algebra 1 in the second half of the Fall 2023 semester at The Ohio State University, and mostly follow lectures by Professor Stefan Patrikis (MWF) and recitation sessions (TR) by Dr. Ariel Weiss. These notes cover rings, ideals,w zerodivisors, domains, monoid rings and group rings, ideals and subrings, quotient rings, ring homomorphisms, the correspondence theorem, and polynomial rings. We will then explore modules over rings, direct sums, and exact sequences. This is followed by a study of ideals in commutative rings that includes the Chinese remainder theorem, prime and maximal ideals, and the prime avoidance theorem. Next, we will study local rings and their spectra, localizations, modules of fractions, and detecting exactness with localization. We then examine finiteness conditions on modules, namely by studying Noetherian and Artinian rings and modules, primary decompositions. This leads us to factorization in rings, UFDs, and irreducibility in polynomials. Finally, we will discuss the structure of modules over PIDs with applications in linear and multilinear algebra.

Contents

1 Rings and Ideals

1.1 Rings, Units, and Examples

Definition 1.1.

A **ring** is a set R equipped with two binary operations $+, \cdot : \mathbb{R} \to \mathbb{R}$ such that

(1) $(R, +)$ is an abelian group,

(2) $(R, \cdot)$ is a monoid, and

(3) For all $x, y, z \in \mathbb{R}$, $x \cdot (y + z) = x \cdot y + x \cdot z$, and $(x + y) \cdot z = x, z + y \cdot z$.

Unless the context suggests otherwise, we usually write 0 for the identity of $(R, +)$ and 1 for the identity of $(R, \cdot)$. We also tend to write xy to mean $x \cdot y$.

Notation 1.2.

- We allow $0 = 1$, in which case R is called a (the) zero ring; such a ring R is unique, since any $x \in R$ has $x = x \cdot 1 = x \cdot 0 = 0$, forcing $R = 0$; conversely, if a ring R has $0 = 1$, then $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$, and by adding $-(x \cdot 0)$ to be both sides we obtain $x \cdot 0 = 0$, and hence $0 = 1$ in R.

- We do not in general require multiplication to be commutative, although we will mostly discuss this case. When multiplication in the ring is commutative, we call it a **commutative ring**. #

Definition 1.3.

Let R be a ring.

- A **unit** of R is an element $u \in R$ such that there exist elements $v, w \in R$ satisfying
$$u \cdot v = 1 = w \cdot u.$$
(This forces $v = w$ because $w \cdot 1 = w \cdot (u \cdot v)$, so $w = (w \cdot u) \cdot v = 1 \cdot v = v$.) We denote by $R^\times$ the set of units of R. We call any element $v \in R$ such that $u \cdot v$ a **right-inverse** of x, and we call any element $w \in R$ such that $w \cdot u$ a **left-inverse** of x. If R is noncommutative, there can exist elements $x \in R$ with right inverses but without left inverses, and vice-versa.
- A nonzero ring R such that $R \setminus \{0\} = R^\times$ is called a **division ring**.
- A commutative division ring is called a **field**.

We will leave the ring operations implicit as '+' and '$\cdot$'.

Example 1.4.

- $\mathbb{Z}$ is a ring with $\mathbb{Z}^\times = \{\pm 1\}$.
- $\mathbb{Q}$ is a field.
- $M_n(\mathbb{C})$, the set of all n-by-n matrices with entries in $\mathbb{C}$, is a ring under the usual matrix multiplication and addition. Likewise, $M_n(R)$ is a ring for *any* (not necessarily commutative) ring R. One can check that associativity of matrix multiplication is inherited from associativity of the ring R. This is one of the most important examples of noncommutative rings. //

Example 1.5. Let $\mathbb{H}$ be the **quaternions**, which is defined as follows. Start with a 4-dimensional real vector space with ordered basis $(1, i, j, k)$. Then
$$\mathbb{H} = 1\mathbb{R} \times i\mathbb{R} \times j\mathbb{R} \times j\mathbb{R}.$$
Endow $\mathbb{H}$ with the associative, but *not* commutative multiplication determined by

- $1\mathbb{R} \cong \mathbb{R}$ is central in $\mathbb{H}$. For all $z \in \mathbb{R}$, $x \in H$, $zh = xz$,
- $ij = k$, $ji = -k$, $i^2 = j^2 = k^2 = -1$.

Thus, the underlying abelian group of bH, that is, $\{\pm 1, \pm i, \pm j, \pm k\}$ under addition, is isomorphic to the quaternion group Q_8 we have already seen. //

Proposition 1.6.

$\mathbb{H}$ is a division ring.

The proof of Proposition 1.6 can be found here.

Example 1.7. For any set S and ring R, the set

$$R^S \coloneqq \mathrm{Map}(S, R) = \{\text{set functions } f\colon S \to R\}$$

is a ring under "pointwise" operations, by which we mean for all $f, g \in \mathrm{Map}(S, R)$,

- $(f + g)(x) = f(x) + g(x)$ for all $x \in S$, and
- $(f \cdot g)(x) = f(x) \cdot g(x)$ for all $x \in S$. //

Example 1.8. Let A be an abelian group. Define the **endomorphism ring** of A by

$$\mathrm{End}_{\mathsf{Grp}}(A) \coloneqq \mathrm{Hom}_{\mathsf{Grp}}(A, A).$$

Then $\mathrm{End}_{\mathsf{Grp}}(A)$ a ring with operations

- $(f + g)(x) = f(x) + g(x)$ for all $x \in A$, and
- $(f \cdot g)(x) = f(g(x))$. //

1.2 Zerodivisors, Integral Domains, and Examples

Definition 1.9.

An element a in a ring R is a **zerodivisor** if $a \neq 0$ and there exists $b \in R \setminus \{0\}$ such that $a \cdot b = 0$.

Definition 1.10.

A nonzero commutative ring with no zerodivisors is called an **integral domain**. In other words, an integral domain is a nonzero commutative ring such that the product of nonzero elements is nonzero.

Integral domains are named as such because they have the most important properties of the integers (which consequently give division with remainder, and more)

Example 1.11. We have been using $(\mathbb{Z}/n\mathbb{Z})^\times$ to be the group of integers coprime to n, and the notation $(\mathbb{Z}/n\mathbb{Z})^\times$ is because this subgroup is precisely the group of units of $\mathbb{Z}/n\mathbb{Z}$. This is made precise by the following lemma. //

Proposition 1.12.

The ring $\mathbb{Z}/n\mathbb{Z}$ is an integral domain if and only if n is prime.

The proof of Proposition 1.12 can be found here.

Exercise 1.13.

$\mathbb{Z}[\sqrt{n}] = \{a + b\sqrt{n} \mid a, b \in \mathbb{Z}\}$, where n is any integer that is not a perfect square. This is an integral domain. Its set of units depends on n.

Example 1.14. $M_n(\mathbb{C})$ is a noncommutative ring, so it cannot be an integral domain. But we can say that $(M_n(\mathbb{C}))^\times = \mathrm{GL}_n(\mathbb{C})$. //

Example 1.15. Consider the collection of continuous functions on $[0,1]$, denoted $C[0,1]$. Its additive identity element is the constant function 0, its multiplicative identity element is the constant function 1, and for all $x, y \in [0,1]$ we have $(f+g)(x) = f(x) + f(y)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$. Now $f^{-1}(x)f(x) = 1$ for all x, $f^{-1}(x) = 1/f(x)$, and we see

$$C[0,1]^\times = \{\text{continuous } f\colon [0,1] \to \mathbb{R}^\times\}.$$

But $C[0,1]$ is *not* an integral domain, because the product of the nonzero functions that are nonzero (that is, that are supported) on disjoint parts of $[0,1]$ multiply to 0. //

1.3 Monoid Rings, Group Rings, and Examples

Given everything we know about groups, we can construct a very rich plethora of rings with the following construction.

Definition 1.16.

Let S be a monoid and let R be a ring. Define the **monoid ring** $R[S]$ by the collection

$$R[S] \coloneqq \bigoplus\nolimits_{s\in S} R \coloneqq \left\{ \sum\nolimits_{s\in S} a_s[s] \;\middle|\; {\scriptstyle a_s\in R \text{ for all } s\in S \text{ and } a_s=0 \text{ for all but finitely many } s} \right\}$$

(where $[s]$ is a formal symbol[a] indexed by elements $s \in S$), with addition defined by

$$\sum\nolimits_{s\in S} a_s[s] + \sum\nolimits_{s\in S} b_s[s] \coloneqq \sum\nolimits_{s\in S} (a_s + b_s)[s],$$

and multiplication defined by

$$\left(\sum\nolimits_{s\in S} a_s \cdot [s]\right) \cdot \left(\sum\nolimits_{t\in S} b_t \cdot [t]\right) \coloneqq \sum\nolimits_{w\in S} \left(\sum\nolimits_{s\cdot t = w \text{ in } S} a_s b_t\right) \cdot [w].$$

The multiplicative identity of $R[G]$ is $1[1] = 1_R[1_S]$, which we will simply write as 1 in $R[G]$. In the special case the monoid S is a group G, we call $R[G]$ a **group ring**.

[a] We are writing $[s]$ instead of s to avoid confusion, since it is possible that elements of R and elements of S are denoted similarly.

Thus the elements of a monoid ring $R[S]$ are formal finite linear combinations of elements of the monoid G, whose coefficients are elements of R. One can check that if S is a monoid and R is any ring, then the monoid ring $R[S]$ is indeed a ring.

Note 1.17. If R is a ring and G is a group, an equivalent definition of the corresponding group ring is that $R[G]$ is the set of functions $f\colon G \to R$ with finite support. One can show the equivalence of these definitions by showing such functions f are determined by $\{f(g)\}_{g\in G}$, which is an element of $\bigoplus_{g\in G} R[G] = \sum_{g\in G} f(g) \cdot [g]$, and the reverse inclusion is similar. //

Example 1.18. Let $R = \mathbb{Z}$ and $G = D_8 = \langle \rho, \tau \mid \rho^4, \tau^2, \rho\tau\rho\tau \rangle$. Let us do a sample calculation in $R[G] = \mathbb{Z}[D_8]$. Consider the elements $a = 2[\rho] + 2[\tau]$, $b = [\rho^2] - [\tau\rho] \in R[G]$. Then

$$\begin{aligned} ab &= (2[\rho] + 2\varphi[\tau]) \cdot ([\rho^2] - [\tau\rho]) = 2[\rho^3] - 2[\rho\tau\rho] + 2[\tau\rho^2] - 2[\tau^2\rho] \\ &= 2[\rho^3] - 2[\tau] + 2[\tau\rho^2] - 2[\rho]. \end{aligned}$$

On the other hand,

$$ba = ([\rho^2] - [\tau\rho]) \cdot (2[\rho] + 2[\tau]) = 2[\rho^3] + 2[\rho^2\tau] - 2[\tau\rho^2] - 2[\tau\rho\tau]$$

$$= 2[\rho^3] + 2[\tau\rho^2] - 2[\tau\rho^2] - 2[\rho^3] = 0.$$

Thus $ab \neq 0$ but $ba = 0$, which demonstrates how bizarre noncommutative rings can be. //

Example 1.19. Consider $R = \mathbb{C}$, and let $G = C_n$, say with $G = \langle x \rangle$. The following is a sample computation in the ring $\mathbb{C}[C_n]$:

$$(\underbrace{1}_{=[1_{C_n}]} - [x])(1 + [x] + [x^2] + \cdots + [x^{n-1}]) = 1 - x^n = 0,$$

since where $G = C_n$, $x^n = 1_G$, so $[x^n] = 1$ in $\mathbb{C}[C_n]$. In particular, note that $1 - [x] \in \mathbb{C}[C_n]$ is a zerodivisor. //

Exercise 1.20.

Show that if R is a commutative ring and G is a group, then $R[G]$ is commutative if and only if G is commutative (abelian). In this way we obtain an extremely rich class of noncommutative rings.

Example 1.21. Consider $R[G]$, where $R = \mathbb{R}$, $G = Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Consider the elements $a = \pi[i] + e[j] + \sqrt{2}[-k]$ and $b = [1] + [-1] (\neq [1] - [1]!)$. The computation of ab and ba is left as a straightforward exercise.

Note that $\mathbb{R}[Q_8]$ looks a lot like $\mathbb{H}$, which we recall is $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$. But in $\mathbb{H}$ we have $1 + -1 = 0$, whereas this is not true in $\mathbb{R}[Q_8]$. //

Theorem 1.22: Universal Mapping Property of Group Rings.

If R and A are commutative rings, $\varphi \colon R \to A$ is a ring homomorphism, and $\alpha \colon G \to A^\times$ is a group homomorphism, then there exists a unique ring homomorphism $\varphi_\alpha \colon R[G] \to A$ such that both diagrams

$$\begin{tikzcd}
R \arrow[rr, "\varphi"] \arrow[dr, hook, "r \mapsto r \cdot [1]"'] & & A \\
& R[G] \arrow[ur, "\varphi_\alpha"'] &
\end{tikzcd}$$

and

$$\begin{tikzcd}
G \arrow[rr, "\alpha"] \arrow[dr, hook, "g \mapsto 1 \cdot [g]"'] & & A^\times \\
& R[G]^\times \arrow[ur] &
\end{tikzcd}$$

commute.

The proof of Theorem 1.22 can be found here.

1.4 Ideals and Subrings

Definition 1.23.

Let R be a ring. A subset $I \subset R$ is

- a **left ideal** if $(I, +)$ is a subgroup of $(R, +)$ and for all $r \in R$, $x \in I$, $r \cdot x \in I$,
- a **right ideal** if $(I, +)$ is a subgroup of $(R, +)$ and for all $r \in R$, $x \in I$, $x \cdot r \in I$, and
- a (two-sided) **ideal** if I is both a left and right ideal.

Exercise 1.24.

For *commutative* rings, the notions of left ideals, right ideals, and two-sided ideals all coincide.

Definition 1.25.

Let X be any subset of R. The (two-sided) **ideal generated by** $\boldsymbol{X}$, denoted (X), is defined as smallest ideal of R containing X, that is,

$$(X) \coloneqq \bigcap\nolimits_{\substack{\text{ideals } J \text{ of } R \\ \text{containing X}}} J.$$

We define the **left (resp. right) ideal generated by** $\boldsymbol{X}$ using the same definition, except with the intersection indexing over all left (resp. right) ideals of R containing X.

Exercise 1.26.

Show that

$$(X) = \left\{ \sum\nolimits_{i=1}^{n} r_i x_i r_i' \;\middle|\; n \in \mathbb{Z}_{\geqslant 0} \text{ and } x_i \in X, r_i, r_i' \in R \text{ for all } i \in \{1, \dots, n\} \right\}.$$

Show that the left (resp. right) ideal generated by X is given by the same formula, except with the "r_i'" (resp. the "r_i") omitted.

Notation 1.27. If $X = \{x_1, \dots, x_n\} \subset R$, we will simply write

$$(X) = (x_1, \dots x_n).$$

In particular, if $X = \{a\}$ is a singleton, we write $X = (a)$; such an ideal is called a **principal ideal**.

When R is commutative, to say ideal $I = (a)$ is principal means $I = Ra = aR = \{r \cdot a \mid r \in R\}$. (We cannot write principal ideals like this in the general case with noncommutative rings.) #

Definition 1.28.

A subset $R' \subset R$ is a **subring** if it is a subgroup of $(R, +)$, contains 1, and is closed under multiplication (that is, a submonoid under '$\cdot$').

Example 1.29. (1) $n\mathbb{Z} \subset \mathbb{Z}$ for $n \in \mathbb{Z}$ is an ideal (and is principal).

(2) Let k be a field. The only ideals of k are (0) and k.

(3) $R = \mathbb{Z}[\sqrt{-5}] \coloneqq \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. Consider the ideal $I =$

$(2, 1+\sqrt{-5})$ of R. (That is, $I = \{2x + (1+\sqrt{-5})y \mid x, y \in R\}$). The ideal I is *not* principal.

(3) For a noncommutative example, consider $R = M_n(\mathbb{C})$, and let I be the left ideal

$$R \cdot \underbrace{\begin{pmatrix} 1 & 0 \cdots\cdots 0 \\ 0 & 0 \cdots\cdots \vdots \\ \vdots & \ddots \vdots \\ 0 & 0 \cdots\cdots 0 \end{pmatrix}}_{\coloneqq E_{1,1}} = \{A \cdot E_{1,1} \mid A \in M_n(\mathbb{C})\} = \left\{ \begin{pmatrix} a_1 & 0 \cdots\cdots 0 \\ a_2 & 0 \cdots\cdots \vdots \\ \vdots & \ddots \vdots \\ a_n & 0 \cdots\cdots 0 \end{pmatrix} \right\}$$

Then one can show that I is *not* a right ideal. It turns out that $M_n(\mathbb{C})$ has no nonzero proper (two-sided) ideals. We call any ring R with this property **simple ring**, so this is to say $M_n(\mathbb{C})$ is a simple ring. More generally, we will show in Exercise 7.4 that for any (possibly noncommutative) division ring D, $M_n(D)$ is a simple ring. //

1.5 Operations on Ideals

There are several ways to construct new ideals from ideals of a commutative ring.

Theorem 1.30.

(i) Let R be a ring and let I and J be ideals of R. Then the following are ideals of R.

- $I \cap J$.
- $I + J \coloneqq \{x + y \mid x \in I, y \in J\}$.
- $IJ \coloneqq I \cdot J \coloneqq \{\sum_{i=1}^{n} x_i y_i \mid n \in \mathbb{Z}_{\geqslant 0}, x_i \in I, y_i \in J \text{ for all } i \in \{1, \dots, n\}\}$.

(ii) In general, we have

$$I \cdot J \quad \subset \quad I \cap J \quad \subset \quad I, J \quad \subset \quad I + J,$$

and there exist examples where any of these inclusions are strict.

The proof of Theorem 1.30 can be found here.

Exercise 1.31.

If A is a commutative ring and $a, b \in A$, then $(a, b) = (a) + (b)$ and $(ab) = (a)(b)$.

1.6 Quotient Rings and Ring Homomorphisms

The significance of ideals in ring theory mirrors that of normal subgroups in group theory: we can quotient our ring by them, and ideals are kernels of ring homomorphisms (to be defined soon).

Theorem 1.32: Construction of Quotient Rings.

Let R be any ring and let I be a (two-sided) ideal. We define the **quotient ring** R/I by letting $(R/I, +)$ be the additive group quotient, and we define multiplication in R/I by

$$\begin{aligned} \cdot\colon R/I \times R/I &\longrightarrow R/i, \\ (a+I)\cdot(b+I) &\longmapsto ab + I. \end{aligned}$$

Then R/I is indeed a ring under $+$ and $\cdot$.

The proof of Theorem 1.32 can be found here.

Example 1.33. If $R = \mathbb{Z}$ and $I = n\mathbb{Z}$ for some $n \in \mathbb{Z}$, then $R/I = \mathbb{Z}/n\mathbb{Z}$. //

Definition 1.34.

Let A and B be any rings. A **ring homomorphism** $\varphi\colon A \to B$ is a set map such that

(1) φ is a group homomorphism as a map $(A, +) \to (B, +)$ that is, $\varphi(x+y) = \varphi(x)+\varphi(y)$ for all $x, y \in A$ (which we recall *implies* $\varphi(0) = 0$), and

(2) φ is a monoid homomorphism as a map $(A, \cdot) \to (B, \cdot)$, that is, for all $x, y \in A$, $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ and $p(1) = 1$.

A ring homomorphism $\varphi\colon A \to B$ is a **ring isomorphism** if there exists a ring homomorphism $\psi\colon B \to A$ such that $\varphi \circ \psi = \mathrm{id}_B$ and $\psi \circ \varphi = \mathrm{id}_A$.

Example 1.35. Let R be a ring, I an ideal of R. Then the surjective map $\pi\colon R \twoheadrightarrow R/I$ given by $x \mapsto x + I$ is a ring homomorphism. //

Note 1.36. (1) Just like for groups, a ring homomorphism is a ring isomorphism if and only if it is bijective.

(2) For all ring homomorphisms $\varphi\colon A \to B$, $\ker\varphi := \{x \in A \mid \varphi(x) = 0\}$ is indeed an ideal of A. On the other hand, $\operatorname{im}\varphi = \{\varphi(x) \mid x \in X\}$ is only a subring of B, but not necessarily an ideal. //

Example 1.37. $R = \mathbb{Z}\times\mathbb{Z}$, $(a, b) + (c, d) = (a + c, b + d)$, $(a, b)(c, d) = (ac, bd)$, $(1, 0)(0, 1) = (0, 0)$. Consider the ideal $I = (2) = \{2(a, b) \mid a, b \in \mathbb{Z}\}$. Then $R/I \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. //

Example 1.38. Consider $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. We call R the **Gaussian integers**. We can think of the Gaussian integers as the integer lattice in the complex plane. Then $I = (2) = \{2a + 2bi \mid a, b \in \mathbb{Z}\}$, which we can think of as the bottom-left corner of 2-by-2 squares with vertices at points whose coordinates are integers, and when these tile the complex plane, the points of the ideal is all the bottom-left points of the squares in the tiling. Then

$$R/I = \{0 + I, 1 + I, i + I, 1 + i + I\}.$$

$\times$	0	1	i	$1+i$
0	0	0	0	0
1	0	1	i	$i+1$
i	0	i	1	$i+1$
$1+i$	0	$1+i$	$i+1$	0

Table 1: Multiplication table of R/I

In particular, this shows that R/I is not an integral domain. //

Example 1.39. Let $R = \mathbb{Z}[\omega]$, where $\omega = e^{2\pi i/3}$. Then $(\omega^3 - 1) = (\omega - 1)(\omega^2 + \omega + 1)$. The roots of $\omega^2+\omega+1$ are $\omega = (-1+\sqrt{-3})/2$. Then $(a+b\omega)(c+d\omega) = ac+(ad+bc)\omega+bd\omega^2 = ac-bd+(ad+bc-bd)\omega$. Then, using the relation $\omega^2+\omega+1 = 0$, $R/I = \{0+I, 1+I, \omega+I, 1+\omega+I\}$.

$\times$	0	1	ω	$1+\omega$
0	0	0	0	0
1	0	1	ω	$i+\omega$
i	0	ω	$1+\omega$	1
$1+i$	0	$1+\omega$	1	ω

Table 2: Multiplication table of R/I

From the multiplication table of R/I, we see that R/I is a *field*, and this field is denoted $\mathbb{F}_4$. //

Example 1.40. Is there an ideal I such that $(2) \subset I \subset \mathbb{Z}[i]$? Consider $I = (2, 1+i)$. Then $I = \{2(a+bi) + (1+i)(c+di)\} = \{a+bi \mid a \equiv b \pmod 2\}$. Is I principal? Well, we since $(1+i)^2 = 2i$, we can write $2 = [(1+i)][(1+i)(-i)]$. Thus $2 \in (1+i)$, so $I = (1+i)$. Hence I is principal. The note that $R/I \cong \mathbb{Z}/2\mathbb{Z}$. //

Example 1.41. Again $R = \mathbb{Z}[\omega]$ where ω is as above, and let $I = (2)$. Is there an ideal J such that $I \subset J \subset \mathbb{Z}[\omega]$? No. And this is not a coincidence—no such ideal exists because I is a maximal ideal, which we will soon define. To see, this one can use a to-be-seen fact that R/I is a field, and an ideal I of any ring R is maximal if and only if R/I is a field. //

Example 1.42. Now consider $R = \mathbb{Z}[\sqrt{-5}]$. Then $R = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. One can show $(2) \subset (2, 1+\sqrt{-5}) \subset \mathbb{Z}[\sqrt{-5}]$. Is $(2, 1+\sqrt{-5})$ principal? To answer this, suppose we can write $(2, 1+\sqrt{-5}) = (a + b\sqrt{-5})$ for some integers a and b. Then

$$2 = (a + b\sqrt{-5})(c + d\sqrt{-5}).$$

Taking the square of the modulus of both sides, we obtain

$$4 = (a^2 + 5b^2)(c^2 + 5d^2).$$

But this forces $b = d = 0$, since otherwise one of the terms on the right-hand side exceeds 5, and the product of two integers, one of which is 5, cannot equal 4. But then $a + b\sqrt{-5} = \pm 2$, so $(a + b\sqrt{-5}) = \pm 2(c + d\sqrt{-5})$. But this is impossible, so $(2, 1+\sqrt{-5})$ is *not* a principal ideal. //

Example 1.43. Again consider $\mathbb{Z}[\sqrt{-5}]$. Then $(1+\sqrt{-5} \subsetneq (2, 1+\sqrt{-5})) \subsetneq (3, 1+\sqrt{-5})$, and

$$(1+\sqrt{-5})(1-\sqrt{-5}) = 6 = 2 \cdot 3,$$

so $\mathbb{Z}[\sqrt{-5}]$ is not what we will soon call a unique factorization domain. //

1.7 The Correspondence Theorem and the Isomorphism Theorems

Theorem 1.44: Universal Mapping Property of Quotient Rings.

Let A, B be rings, let $I \subset A$ be an ideal, and let $\varphi\colon A \to B$ be a ring homomorphism such that $I \subset \ker\varphi$. Then there exists a unique ring homomorphism $\overline{\varphi}$ such that the diagram

$$\begin{tikzcd} A \arrow[rr, "\varphi"] \arrow[dr, "\pi"'] & & B \\ & A/I \arrow[ur, "\overline{\varphi}"'] & \end{tikzcd}$$

commutes, where $\pi\colon A \to A/I$ is the natural quotient map. In the case $I = \ker\varphi$, then $\overline{\varphi}$ is a ring isomorphism $A/\ker\varphi \xrightarrow{\cong} \operatorname{im}\varphi$.

The proof of Theorem 1.44 can be found here.

We also have analogs of similar results we proved for groups, and one of the most important is the correspondence theorem:

Theorem 1.45: Correspondence Theorem.

Let I be an ideal of a ring A. Then, where $\pi\colon A \to A/I$ is the natural quotient map, there exists a bijection

$$\begin{aligned} \left\{ \begin{matrix} \text{ideals } J \text{ of } A \\ \text{containing } I \end{matrix} \right\} &\longleftrightarrow \left\{ \begin{matrix} \text{ideals } \overline{J} \\ \text{of } A/I \end{matrix} \right\}, \\ J &\longmapsto \pi(J) =: J/I, \\ \pi^{-1}(J) &\longleftarrow \overline{J}. \end{aligned}$$

The proof of Theorem 1.45 can be found here.

Theorem 1.46: Second Isomorphism Theorem.

For all ideals J containing I, there exists a ring isomorphism

$$\frac{A/I}{J/I} \xrightarrow{\cong} A/J.$$

The proof of Theorem 1.46 can be found here.

Example 1.47. For any ring R, there is a unique ring homomorphism $\varphi\colon \mathbb{Z} \to \mathbb{R}$ given by

$\varphi(1) = 1$, so $\varphi(n)$ for $n > 0$ is determined as

$$\varphi(n) = \varphi(\underbrace{1 + 1 + \cdots + 1}_{n \text{ copies of } 1}) = \varphi(1) + \cdots + \varphi(1) = 1 + \cdots + 1,$$

and for $n < 0$, $\varphi(n) = -\varphi(-n)$. Note $\ker\varphi$ is an ideal of $\mathbb{Z}$, and every such has the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$. Thus for $\ker\varphi = n\mathbb{Z}$, we get a canonical isomorphism of $\mathbb{Z}/n\mathbb{Z}$ onto a subring of R ($\mathbb{Z}/n\mathbb{Z} \hookrightarrow R$). The integer n, which we may assume to be nonnegative, is called the **characteristic** of R. In particular, if R has no zerodivisors, then n can only be 0 or a prime number. We say, for example, $\mathbb{Q}$ has characteristic 0. //

Exercise 1.48.

Show that a ring R has characteristic 0 if the canonical map $\mathbb{Z} \to \mathbb{R}$ sending $1 \mapsto 1$ is injective.

1.8 Algebras and Polynomial Rings

Definition 1.49.

If R is any (possibly noncommutative) ring, an R-algebra is a (possibly noncommutative) ring S equipped with a ring homomorphism $\varphi\colon R \to S$ such that $\varphi(R) \subset S$, where $Z(S)$ denotes the **center** of S, that is, the collection of all elements $x \in S$ such that $xy = yx$ for all $y \in S$. We call S **finitely generated (as an *R*-algebra)** if there exist $s_1, \ldots, s_n \in S$ such that $B = \varphi(R)[s_1, \ldots, s_n]$.

Note 1.50. In the common situation A is a commutative ring and B is a finitely generated commutative A-algebra, we obtain a surjective ring homomorphism sending x_i to b_i for each $i \in \{1, \ldots, n\}$ such that the diagram

$$\begin{tikzcd}
A[x_1, \ldots, x_n] \arrow[rr, two heads, "x_i \mapsto b_i"] & & B \\
& A \arrow[ul, hook] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

commutes. //

Note 1.51. If A is a commutative ring, then any commutative A-algebra B is an A-module. Indeed, since we have a ring isomorphism from A to B, B is an A-module with multiplication given by the map $\varphi\colon A \to B$ (from the definition of B being an A-algebra), and defining the ring action on B to make B an A-module by $a \cdot b \coloneqq \varphi(a)b$. //

Example 1.52. $\mathbb{Z}[\sqrt{-5}]$ as a subring of $\mathbb{C}$. In the notation of the construction above, we have $S = \left\{\sqrt{-5}\right\}$, so $\mathbb{Z}[\sqrt{-5}]$ is the collection of finite sums $\sum_{n \in \mathbb{Z}_{\geq 0}} a_n(\sqrt{-5})^n$ for some $a_n \in \mathbb{Z}$. Observe that since $(\sqrt{-5})^2 = -5 \in \mathbb{Z}$, we can write $\mathbb{Z}[\sqrt{-5}]$ as $b_0 + b_1\sqrt{-5}$ for some $b_1, b_2 \in \mathbb{Z}$. //

Definition 1.53.

If I is any set and R is any (possibly noncommutative) ring, define the **polynomial ring** (over R with variables indexed by I) as the monoid ring $R[M]$, where M is the commutative monoid

$$M = \left\{ \{a_i\}_{i\in I} \in \bigoplus_{i\in I} \mathbb{Z} \;\middle|\; a_i \geqslant 0 \text{ for all } i \in I \right\}.$$

Notation 1.54. In the context of Definition 1.53, we will usually write the element $\{a_i\}_{i\in I}$ as $\prod_{i\in I} x_i^{a_i}$. For example, the element $(1,3,0,2,0,0,0,0,\dots) \in M$ will be written as $x_1^1 x_2^3 x_3^0 x_4^2 x_5^0 x_6^0 x_7^0 \cdots$, or simply $x_1 x_2^3 x_4^2$. #

Note 1.55. Formally, polynomial rings are monoid algebras. //

Example 1.56. Applying Definition 1.53 in the case the ring R is a commutative ring A and I is any set, then the polynomial ring with variables over R with variables indexed by I, $A[\{x_i\}_{i\in I}]$, is the collection of finite formal sums of the form

$$A[\{x_i\}_{i\in I}] = \left\{ \sum_{\substack{i=(i_1,\dots,i_k)\in I^k \\ d=(d_{i_1},\dots,d_{i_k})\in\mathbb{Z}^k_{\geqslant 0}}} a_{i,d} x_{i_1}^{d_{i_1}} \cdots x_{i_k}^{d_{i_k}} \;\middle|\; \begin{smallmatrix} k\in\mathbb{Z}_{\geqslant 0} \text{ and } a_{i,d}\in A \\ \text{for all } i\in I^k,\ d\in\mathbb{Z}^k_{\geqslant 0} \end{smallmatrix} \right\},$$

and is a ring under addition of coefficients and multiplication described in Example 1.56. In the case $I = \{1,\dots,n\}$ for $n \in \mathbb{Z}_{\geqslant 1}$, we will usually write $A[\{x\}_{i\in I}]$ as $A[x_1,\dots,x_n]$. For example, $3x + 1(4x+2) + 1$ is an element of $\mathbb{Z}[\{x,y,z\}]$. //

Example 1.57. In the special case A is commutative and the index set I is a singleton, we write $A[x]$ for the ring of polynomials in variables indexed by I over A. Then by Example 1.56, the underlying set of $A[x]$ is

$$A[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid n \in \mathbb{Z}_{\geqslant 0} \text{ and } a_1,\dots,a_n \in A\}.$$

By Example 1.56, addition in $A[x]$ is given by

$$(a_0 + a_1 x + \cdots + a_n x^n) + (b_0 + b_1 x + b_2 x^2 + \cdots + b_m x^m) = (a_0 + b_0) + (a_1 + b_1)x + \cdots + \lambda,$$

where $\lambda = (a_m + b_m)x^m$ if $m \geqslant n$ and $\lambda = (a_n + b_n)x^n$ if $m < n$, and multiplication in $A[x]$ is given by

$$\left(\sum_{i=0}^{m} a_i x^i\right) \cdot \left(\sum_{j=0}^{n} b_j x^j\right) = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j\right) x^k,$$

that is, by the (unique) commutative, associative, and distributive multiplication such that $x^i \cdot x^j = x^{i+j}$ in $A[x]$. In this setting, given an element $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in A[x]$ with $a_n \neq 0$, we call n the **degree** of f, and denote it by $\deg(f(x))$. We call any term of degree 0 a **constant term**, terms of degree 1 **linear terms**, terms of degree 2 **quadratic terms**, and so on, and the terms with the highest degree are called **max order terms** or **leading terms**. //

Example 1.58. The case $n = 2$ yields the ring $R[x_1, x_2]$, whose element are of the form

$$\underbrace{a}_{\substack{\text{constant}\\\text{term}}} + \underbrace{a_{10}X_1 + a_{01}X_2}_{\text{linear terms}} + \underbrace{(a_{20}X_1^2 + a_{11}X_1X_2 + a_{02}X_2^2)}_{\text{quadratic terms}} + \cdots + \underbrace{\cdots}_{\text{max order terms}}.$$

//

Theorem 1.59: Universal Mapping Property of Polynomial Rings.

If $\varphi\colon A \to B$ is any homomorphism of commutative rings, then for any choice of $\alpha \in B$, there exists a unique ring homomorphism $\mathrm{ev}_\alpha\colon A \to B$ such that the diagram

$$\begin{tikzcd}
A \arrow[rr, "\varphi"] \arrow[dr, hook] & & B \\
& A[x] \arrow[ur, "\mathrm{ev}_\alpha \colon f(x) \mapsto (\varphi(f))(\alpha)"'] &
\end{tikzcd}$$

commutes. More precisely, if $\varphi\colon A \to B$ is a homomorphism of commutative rings, we get a homomorphism

$$\begin{aligned} A[\{x_i\}_{i\in I}] &\longmapsto B, \\ f &\longmapsto \varphi(f), \end{aligned}$$

where $\varphi(f)$ is the polynomial obtained by applying φ to the coefficients of f, and for all choices of $\alpha = (\alpha_i)_{i\in I} \in B^I$, the map

$$\begin{aligned} B[\{X_i\}_{i\in I}] &\longrightarrow B, \\ f &\longmapsto f(\alpha), \end{aligned}$$

is a ring homomorphism (Our ev_α map in the 1-variable case was a composition of two such maps.)

The proof of Theorem 1.59 can be found here.

Warning 1.60. Theorem 1.59 only applies to commutative rings. Indeed, if A is a noncommutative ring R, then although the univariate polynomial ring over R makes sense by Theorem 1.59, the evaluation homomorphism is not well-defined in general. For example, consider $A = \mathbb{H}$, $B = \mathbb{H}$, and $\varphi = \mathrm{id}_H$. Indeed, in $\mathbb{H}[x]$, we have $xj = jx$ but $ij \neq ji$, so ev_i is not well-defined.

Although we will mostly consider the case $|I| < \infty$, the following result is an important result that holds for arbitrary index sets I.

Theorem 1.61.

Let A be *any* commutative ring. Then A is isomorphic to the quotient of a polynomial ring of the form

$$A \cong \frac{\mathbb{Z}[\{x_i\}_{i\in I}]}{J},$$

for some indes set I and some ideal J of $\mathbb{Z}[\{x_i\}_{i\in I}]$.

The proof of Theorem 1.61 can be found here.

Note 1.62. The argument shows more than the statement: it says that if you can find a generating set of A with n variables, then by indexing that set with a set I and using the ring homomorphism obtained from the universal mapping property of polynomial rings, you can get the precise isomorphism $A \xrightarrow{\cong} Z[\{X_i\}_{i\in I}]/\ker\Phi$. So, if you took $A = \mathbb{C}$, you would need *a lot* of variables, so the cardinality of the set would be quite large. //

2 Modules Over Rings

2.1 Definitions

Just a groups act on sets via group actions (and sometimes these objects are called ***G*-modules**), rings act on abelian groups via **scalar multiplication**, sometimes called a **ring action**, to form an R-module.

The theory of modules over rings is the analog of the theory of vector spaces over fields.

Definition 2.1.

Let R be any ring. A **left *R*-module** is an abelian group M equipped with a map

$$\begin{aligned} R \times M &\longrightarrow M, \\ (r, m) &\longmapsto r \cdot m, \end{aligned}$$

such that for all $m, m_1, m_2 \in M$ and all $r, r_1, r_2 \in R$,

(i) $r_1 \cdot (r_2 \cdot m) = (r_1 r_2) \cdot m$ and $1 \cdot m = m$,

(ii) $(r_1 + r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$, and

(iii) $r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$.

Example 2.2. The set $\mathbb{C}^n$ of n-dimensional column vectors with entries in $\mathbb{C}$ is a left $M_n(\mathbb{C})$-module under matrix multiplication. The set $(\mathbb{C}^n)^t$ of n-dimensional row vectors with entries in $\mathbb{C}$ is a right $M_n(\mathbb{C})$-module under matrix multiplication. //

There is nothing special about rings acting on abelian groups from the *left*; we define right modules similarly:

Definition 2.3.

Likewise, a **right *R*-module** is an abelian group N and a map

$$\begin{aligned} N \times R &\longrightarrow N, \\ (n, r) &\longmapsto n \cdot r, \end{aligned}$$

such that

(i) $n \cdot 1 = n$ for all $n \in N$ and $n \cdot (r_1 r_2) = (n_1 \cdot r_1) \cdot r_2$ for all $r_1, r_2 \in R$ and all $n \in N$,

(ii) $n_1(r_1 + r_2) = n.r_1 + n \cdot r_2$, and

(iii) $(n_1 + n_2) \cdot r = n_1 \cdot r + n_2 \cdot r$ for all $n_1, n_2 \in N, r \in R$.

Notation 2.4. It is generally clear from context when one is referring to the additive identity of the ring R or the additive identity of the abelian group M, so we will usually denote these both by 0 without issue. We may also write simply rm (resp. mr) instead of $r \cdot m$ (resp. $m \cdot r$) for the left (resp. right) scalar multiple of $m \in M$ by the ring element $r \in R$. #

Example 2.5. If R is a field k, then a left (or right) R-module is a k-vector space. //

Example 2.6. If R is commutative, then any left R-module M is canonically a right R-module by defining $m \cdot r = r \cdot m$.

Indeed, for all $r_1, r_2 \in R$ and all $m \in M$, our proposed definition of the right action is

$$m \cdot (r_1 r_2) = (r_1 r_2) \cdot m = r_1 \cdot (r_2 \cdot m) = r_1 \cdot (m \cdot r_2) = (m \cdot r_2) \cdot r_1 = m \cdot (r_2 r_1),$$

and this must equal $m \cdot (r_1 r_2)$ if R is commutative, so we are done. (Note that despite this result, this is *not* a valid right R-module action in general!)

Thus, for commutative rings, we typically do not distinguish between left and right R-modules, and instead simply say "R-module". //

Example 2.7. Consider $R = \mathbb{Z}$. Then $\mathbb{Z}$-modules and abelian groups are "the same". More formally, any abelian group is uniquely a $\mathbb{Z}$-module (and $\mathbb{Z}$-modules are abelian groups by definition): given an abelian group A, for any $n \in \mathbb{Z}$ and $a \in A$, define

$$n \cdot a = \begin{cases} \overbrace{a + a + \cdots + a}^{n \text{ copies of } a} & \text{if } n > 0, \\ 0 & \text{if } n = 0, \\ -((-n) \cdot a) & \text{if } n < 0. \end{cases}$$

(As an exercise, show that for any ring R and any left R-module M, we have $0 \cdot m = 0$ for all $m \in M$ and $(-r) \cdot m = -(r \cdot m)$ for all $r \in R$ and $m \in M$.) //

Example 2.8. For any ring R, a left (resp. right) ideal is a left (resp. right) R-module under left (resp. right) multiplication. Indeed, any additive subgroup $I \subset R$ that is stable under left (resp. right) R-multiplication is a left (resp. right) ideal. //

Example 2.9. In the special case of Example 2.8 above, the For any ring R, R is both a left and right R-module via multiplication. (And these actions commute: $(r_1 r) r_2 = r_1 (r r_2)$.) More generally, the ring

$$R^n \coloneqq \{(a_1, \ldots, a_n) \mid a_i \in \mathbb{R} \text{ for all } 1 \leqslant i \leqslant n\}$$

is a left (resp. right) R-module under $r \cdot (a_1, \ldots, a_n) = (ra_1, \ldots, ra_n)$ (resp. $(a_1, \ldots, a_n) \cdot r = (a_1 r, \ldots, a_n r)$). The R-module R^n is called a **free left (resp. right) $\boldsymbol{R}$-module of rank $\boldsymbol{n}$**. (Note this implies $R \cdot N = N$ because $1 \in R$.) //

Definition 2.10.

Let M be a left R-module. A **submodule** N of M is an additive subgroup of M such that $R \cdot N \subset N$ (resp. such that $N \cdot R \subset N$). Submodules of a right R-modules are defined similarly.

Definition 2.11.

Let M be a left R-module and let N be a submodule of M. We define the **left (resp. right) quotient *R*-module** M/N as the quotient of abelian groups equipped with the left R-action given by

$$r \cdot (m + N) = (r \cdot m) + N \text{ for all } r \in R, m \in M.$$

Exercise 2.12.

Show that Definition 2.11 indeed produces a left (resp. right) R-module.

2.2 Homomorphisms of (Left) R-Modules

Definition 2.13.

Let M, N be left R-modules. A map $\varphi\colon M \to N$ **left *R*-module homomorphism** is a group homomorphism of the underlying abelian groups such that for all $r \in R$ and $m \in M$,

$$\varphi(r \cdot m) = r \cdot \varphi(m).$$

We write $\operatorname{Hom}_R(M, N)$ for the set of (left) R-module homomorphisms $M \to N$.

Note 2.14. Let R be any ring and let M, N be (left) R-modules.

- $\operatorname{Hom}_R(M, N)$ is an abelian group under addition, that is, the operation $(\varphi + \psi)(m) = \varphi(m) + \psi(m)$.
- If R is commutative, then in fact $\operatorname{Hom}_R(M, N)$ is an R-module with the operation given for all $r \in R$ and all $\varphi \in \operatorname{Hom}_R(M, N)$ by

  $$(r \cdot \varphi)(m) = r \cdot (\varphi(m)) \text{ for all } m \in M.$$

  This gives a homomorphism that is *internal* to R-modules, that is, an internal hom in the following categorical sense. An **internal hom** in a category is a hom set that is itself an object in the category. (Note: $r \cdot \varphi$ is an abelian group homomorphism if R is noncommutative. But in order to be an R-module homomorphism, we need for all $\sigma \in R$ that

  $$\underbrace{(r \cdot \varphi)(sm)}_{\substack{\coloneqq r\cdot\varphi(sm),\\ \text{which equals } r\cdot s\cdot\varphi(m)\\ \text{because } \varphi\in\operatorname{Hom}_R(M,N)}} = \underbrace{s \cdot (r \cdot \varphi)(m)}_{= s\cdot r\cdot\varphi(m)},$$

  and $r \cdot s \cdot \varphi(m) = s \cdot r \cdot \varphi(m)$ in general only when R is commutative.) //

Definition 2.15.

Let $\varphi \in \operatorname{Hom}_R(M, N)$.

- The **kernel** $\ker \varphi \coloneqq \{m \in M \mid \varphi(m) = 0\}$ and **image** $\operatorname{im}(\varphi) \coloneqq \varphi(M)$ of φ are R-submodules of M and N, respectively.

- Define the **cokernel** of R-modules by $\operatorname{coker}\varphi \coloneqq N/\operatorname{im}\varphi$.
- φ is an **isomorphism** if there exists $\psi \in \operatorname{Hom}_R(N, M)$ such that $\varphi\circ\psi = \mathrm{id}_N$ and $\psi\circ\varphi = \mathrm{id}_M$. It is necessary and sufficient for φ to be a bijective R-module homomorphism.

Exercise 2.16.

Prove the assertions made in Definition 2.15. In addition, show that the usual isomorphism theorems hold. (For example, show that for any $\varphi \in \operatorname{Hom}_R(M, N)$, the map

$$\begin{aligned} M/\ker\varphi &\xrightarrow{\cong} \operatorname{im}\varphi \\ m + \ker\varphi &\longmapsto \varphi(m) \end{aligned}$$

is an isomorphism of R-modules.)

Example 2.17. Consider $R = \mathbb{Z}$. The $\mathbb{Z}$-modules are abelian groups, and a $\mathbb{Z}$-module homomorphism is the same as an abelian group homomorphism. //

Example 2.18. Let R be any ring and let $A \in M_{m\times n}(R)$ be $m \times n$ matrices over R. Left multiplication by A on column vectors is a map $\varphi_A \coloneqq A\colon R^n \to R^m$ given by $v \mapsto Av$, and gives a homomorphism of abelian groups. //

Warning 2.19. Recall R (and hence R^d for all positive integers d) is naturally both a left and a right R-module. Is φ_A a homomorphism of right or left R-modules? Well, for all $r \in R$,

$$A\cdot(v\cdot r) = \varphi_A(v\cdot r) = \varphi_A(r\cdot v) = A\cdot rv \overset{\substack{\text{not}\\ \text{always!}}}{=} \varphi_A(r\cdot v) = r\cdot A\cdot v$$

but it *does* work in the reverse direction,so φ_A is always a *right* R-module but not a left R-module in general. But if R is commutative, then the above equations always hold, so φ_A is also a left R-module homomorphism. ☡

Example 2.20. If we consider the case R is a field k, then k-modules M and N are k-vector spaces and $\operatorname{Hom}_k(M, N)$ is the k-vector space of k-linear maps $M \to N$. An important case is when $N = k$, in which case $\operatorname{Hom}_k(M, k)$ is called the **dual *k*-vector space of *M***, and is often denoted M^*. //

Example 2.21. If $R = \mathbb{R}$, $M = \mathbb{R}^2$, then $\varphi\colon \mathbb{R}^2 \to \mathbb{R}^2$ given by $\left(\begin{smallmatrix} x\\ y\end{smallmatrix}\right) \longmapsto \left(\begin{smallmatrix} 3 & 1\\ 0 & 2\end{smallmatrix}\right)\left(\begin{smallmatrix} x\\ y\end{smallmatrix}\right) = \left(\begin{smallmatrix} 3x+y\\ 2y\end{smallmatrix}\right)$. is an isomorphism because $\det\left(\begin{smallmatrix} 3 & 1\\ 0 & 2\end{smallmatrix}\right) = 6 \neq 0$. Its inverse $\varphi^{-1}\colon \mathbb{R}^2 \to \mathbb{R}^2$ is given by $\left(\begin{smallmatrix} x\\ y\end{smallmatrix}\right) \longmapsto \frac{1}{6}\left(\begin{smallmatrix} 2 & -1\\ 0 & 3\end{smallmatrix}\right)\left(\begin{smallmatrix} x\\ y\end{smallmatrix}\right) = \frac{1}{6}\left(\begin{smallmatrix} 2x-y\\ 3y\end{smallmatrix}\right)$. //

Example 2.22. Let $R = \mathbb{Z}$, $M = \mathbb{Z}^2$, $\psi\colon \mathbb{Z}^2 \to \mathbb{Z}^2$ by $\left(\begin{smallmatrix} x\\ y\end{smallmatrix}\right) \longmapsto \left(\begin{smallmatrix} 3 & 1\\ 0 & 2\end{smallmatrix}\right)\left(\begin{smallmatrix} x\\ y\end{smallmatrix}\right)$. Then ψ is injective, since it is the restriction of φ to $\mathbb{Z}^2$, and φ is injective (and injectivity is preserved under restrictions). But ψ is not surjective. Intuitively, this is because the inverse of φ is not always integer-valued. More precisely, this is because $\left(\begin{smallmatrix} x'\\ y'\end{smallmatrix}\right) \in \operatorname{im}\psi$ if and only if $\left(\begin{smallmatrix} x'\\ y'\end{smallmatrix}\right) = \left(\begin{smallmatrix} 3x+y\\ 2y\end{smallmatrix}\right)$ for $x', y' \in \mathbb{Z}$. This gives us the numerical constraints $y' = 2y \iff y'$ is even and $x' = 3x + y$. This looks tricky to unravel, but we can multiply the second equation by 2 to get $2x' = 6x + y'$, that is, $2x' - y' = 6x$, or written differently, $2x' \equiv y' \pmod 6$ (or $x' \equiv \frac{y'}{2} \pmod 3$). This shows something like $\left(\begin{smallmatrix} 1\\ 0\end{smallmatrix}\right)$ is not in the image, because $2(1) \not\equiv 0 \pmod 3$. //

Example 2.23. (Modules over Group Rings and Group Representations) Let G be a group and k a field. We consider a module V over the group ring $k[G]$. Here are some properties of V:

- V is an abelian group and a module over $k[G]$. Since $k[G]$ contains k, V is also a k-vector space.
- The unit e of $k[G]$ satisfies $e \cdot v = v$ for all $v \in V$. For all $g, h \in G \subset k[G]$, we have $(gh) \cdot v = g \cdot (hv)$. This implies that G acts on V, giving a group homomorphism $G \to S_V = \mathrm{Aut}_{\mathsf{Set}}(V)$.
- For $g \in G \subset k[G]$ and $v, w \in V$, we have $g(v + w) = g(v) + g(w)$. If $\lambda \in k$, then $(\lambda g) \cdot v = g \cdot (\lambda v)$. The induced automorphism from the group action is $G \to \mathrm{Aut}_{\mathsf{Set}}(V)$, sending $g \mapsto (\varphi_g \colon v \mapsto gv)$. This map descends to a map $G \to \mathrm{GL}(V)$, called a **group representation of G over k**.

The representation theory of groups is thus subsumed by the theory of $k[G]$-modules. //

2.3 Direct Sums and Direct Products of R-Modules

Definition 2.24: Direct Sums and Direct Products of R-Modules.

Let R be any ring and let I be any set. For each $i \in I$, let M_i be a (left) R-module. Define

$$\bigoplus_{i\in I} M_i = \left\{ \{m_i\}_{i\in I} \in \prod_{i\in I} M_i \;\middle|\; m_i = 0 \text{ for all but finitely many } i \in I \right\}.$$

This is made into an R-module via

$$\{m_i\}_{i\in I} + \{m_i'\}_{i\in I} = \{m_i + m_i'\}_{i\in I} \qquad \text{and} \qquad r \cdot \{m_i\}_{i\in I} = \{rm_i\}_{i\in I}.$$

We call $\bigoplus_{i\in I} M_i$ the **direct sum** of the M_is. Here we note that the Cartesian product of the underlying sets of the M_is, $\prod_{i\in I} M_i$, is also an R-module by the same rules, called the **direct product** of the M_is.

Warning 2.25. Note that although $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$ when I is a finite set, this is *not* true in general.

Note 2.26. Note that for all $i, j \in I$, we have R-module homomorphisms

$$\begin{tikzcd}
M_i \arrow[r, hook, "\alpha_i"] & \bigoplus_{k\in I} M_k \arrow[r, hook] & \prod_{k\in I} M_k \arrow[r, two heads, "\pi_j"] & M_j \\
m \arrow[r, mapsto] & (m_k)_{k\in I}, \text{ where } m_k = m\delta_{jk} \arrow[r, mapsto] & (m_k)_{k\in I} \arrow[r, mapsto] & m_j
\end{tikzcd}$$

//

Note 2.26 suggests the possibility of isomorphisms

$$\mathrm{Hom}_R\Big(\bigoplus_{i\in I} M_i, N\Big) \xrightarrow{\cong} \prod_{i\in I} \mathrm{Hom}_R(M_i, N)$$

and

$$\mathrm{Hom}_R\Big(N, \prod_{i\in I} M_i\Big) \xrightarrow{\cong} \prod_{i\in I} \mathrm{Hom}_R(N, M_i).$$

which in turn would yield a categorical view of the direct sum and direct product. We show in the following theorem that such isomorphisms do, in fact, exist:

Theorem 2.27: Universal Mapping Property of Direct Sum and Direct Product of R-Modules.

Let $\{M_i\}_{i\in I}$ be R-modules.

(1) For all R-modules N, we have an isomorphism of abelian groups

$$\begin{aligned}\Phi\colon \operatorname{Hom}_R\Big(\bigoplus\nolimits_{i\in I} M_i, N\Big) &\xrightarrow{\cong} \prod\nolimits_{i\in I} \operatorname{Hom}_R(M_i, N),\\ \varphi &\longmapsto \{\varphi\circ\alpha_i\}_{i\in I},\\ [\{m_i\}_{i\in I}\mapsto \textstyle\sum_{i\in I} f_i(m_i)] &\longleftarrow \{f_i\}_{i\in I}.\end{aligned}$$

Moreover, if R is commutative, then this is an isomorphism of R-modules.

(2) For all R-modules M, we have an isomorphism

$$\begin{aligned}\Psi\colon \operatorname{Hom}_R\Big(M, \prod\nolimits_{i\in I} M_i\Big) &\xrightarrow{\cong} \prod\nolimits_{i\in I} \operatorname{Hom}_R(M, M_i),\\ \varphi &\longmapsto \{\pi_i\circ\varphi\}_{i\in I},\\ [m\mapsto \{f_i(m)\}_{i\in I}] &\longleftarrow \{f_i\}_{i\in I}.\end{aligned}$$

Proof. Regarding the first isomorphism, note that since $m_i = 0$ for all but finitely many $i\in I$, $f_i(m_i) = 0$ for all but finitely many $i\in I$. Thus the inverse map $\Phi((f_i)_{i\in I})$ makes sense. the maps are given in the statement, so it only remains to check these work as claimed. This is left as an exercise. □

2.4 Characterization of Exact Sequences of Modules as Direct Sums

Definition 2.28.

- A sequence $M \xrightarrow{f} N \xrightarrow{g} P$ of R-module homomorphisms is called **exact at N** if $\ker g = \operatorname{im} f$.
- A sequence $\cdots \longrightarrow M_i \xrightarrow{\varphi_i} M_{i+1} \xrightarrow{\varphi_{i+1}} M_{i+2} \longrightarrow \cdots$ of R-module homomorphisms is called a **long exact sequence**, or is simply called an **exact sequence**, if $\ker\varphi_k = \operatorname{im}\varphi_{k-1}$ for all $k\in\mathbb{Z}$.
- An exact sequence of the form $\cdots \longrightarrow 0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0 \longrightarrow \cdots$ (with zeroes extending this sequence) is called a **short exact sequence (SES) of R-modules**.

Note 2.29. Just as for groups, given a short exact sequence $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$, we must have

- f is injective,
- $\ker g = \operatorname{im} f$, and

- g is surjective. //

Definition 2.30.

- A short exact sequence $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ is **split** if g has a section, that is, if there exists an R-module homomorphism $s\colon P \to N$ such that $g \circ s = \mathrm{id}_P$.
- A short exact sequence $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ is **trivial** if there exists an isomorphism $\varphi\colon N \to M \oplus P$ such that the diagram

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, equal, "\mathrm{id}_M"'] & N \arrow[r, "g"] \arrow[d, "\varphi", "\cong"'] & P \arrow[r] \arrow[d, equal, "\mathrm{id}_P"] & 0 \\
0 \arrow[r] & M \arrow[r, hook, "i_M", "m\mapsto(m,0)"'] & M \oplus P \arrow[r, two heads, "\pi_P", "(m,p)\mapsto p"'] & P \arrow[r] & 0
\end{tikzcd}$$

commutes.

The following lemma is a useful feature of modules over rings that stands in stark contrast to the case of groups.

Theorem 2.31.

A short exact sequence $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ of R-modules is split if and only if it is trivial.

The proof of Theorem 2.31 can be found here.

Example 2.32. We can summarize Example 2.22 concisely with an exact sequence, namely $0 \to \mathbb{Z}^2 \xrightarrow{\psi} \mathbb{Z}^2 \xrightarrow{\pi} \mathbb{Z}^2/\operatorname{im}\psi \to 0$. This captures that ψ is injective, π is surjective, and $\operatorname{im}\psi = \ker\pi$. //

Example 2.33. Continuing from example Example 2.32, what is $\mathbb{Z}^2/\operatorname{im}\psi$? The given short exact sequence hints that $\mathbb{Z}^2/\operatorname{im}\psi$ is a discrete set, as since $\mathbb{Z}^2$ is two-dimensional and injectivity of ψ together imply $\mathbb{Z}^2/\operatorname{im}\psi$ is a "two-dimensional" object quotiented by a "two-dimensional" object, which leaves us with a "zero-dimensional" object.

And we can say there even more: we expect $\mathbb{Z}^2/\operatorname{im}\psi$ to be a finite abelian group of order $\det\left(\begin{smallmatrix}3&1\\0&2\end{smallmatrix}\right) = 6$. Since there is only one such group, this would imply $\mathbb{Z}^2/\operatorname{im}\psi \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

Let us make this more precise. Define $\pi'\colon \mathbb{Z}^2 \to \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ by

$$\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right) \longmapsto (2x - y \pmod 3, y \pmod 2).$$

Then $\pi'\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right) = (0,0) \iff \left(\begin{smallmatrix}x\\y\end{smallmatrix}\right) \in \operatorname{im}\psi$, $\ker\pi' = \operatorname{im}\psi$ and π' is surjective. Hence

$$0 \longrightarrow \mathbb{Z}^2 \xrightarrow{\psi} \mathbb{Z}^2 \xrightarrow{\pi'} \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

is a short exact sequence. One can check that π' is a $\mathbb{Z}$-module homomorphism (that is, a homomorphism of abelian groups). //

Example 2.34. Consider the ring $R = \mathbb{Z}$, and set $M_i = \mathbb{Z}/i\mathbb{Z}$ for each element i of the set $I = \{2, 3, 4, \dots\}$. Not only are $\prod_{i \in I} M_i = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \cdots$ and $\bigoplus_{i \in I} M_i = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \cdots$ not equal, but they are not isomorphic. Indeed, the element $(1, 1, \dots) \in \prod_{i \in I} M_i$ has infinite order, but no element of infinite order exists in $\bigoplus_{i \in I} M_i$. //

Example 2.35. Again consider the short exact sequence $0 \to \mathbb{Z}^2 \to \mathbb{Z}^2 \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to 0$, where the second arrow from the left is given by applying the linear map $\left(\begin{smallmatrix} 3 & 1 \\ 0 & 2 \end{smallmatrix}\right)$ to elements of $\mathbb{Z}^2$. This short exact sequence is *not* split, because $\mathbb{Z}^2 \not\cong \mathbb{Z}^2 \oplus \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. //

Example 2.36. The short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, "a \mapsto (a,0,0,\dots)"] & \bigoplus_{i=1}^{\infty} \mathbb{Z} \arrow[r, "(a_1, a_2, \dots) \mapsto (a_2, a_3, \dots)"'] & \bigoplus_{i=1}^{\infty} \mathbb{Z} \arrow[r] & 0
\end{tikzcd}$$

does split, because the map $\bigoplus_{i=1}^{\infty} \mathbb{Z} \to \bigoplus_{i=1}^{\infty} \mathbb{Z}$ defined by $(a_2, a_3, a_4, \dots) \mapsto (0, a_2, a_3, a_4, \dots)$ is a section. //

2.5 Homework 7

Exercise 2.37: 7.1.

Let I be an ideal of a commutative ring A. We define the **radical** of I, denoted $\sqrt{I}$, to be

$$\sqrt{I} = \{x \in A \mid x^n \in I \text{ for some } n \in \mathbb{Z}_{\geqslant 1}\}.$$

In the special case $I = (0)$, we call the radical $\sqrt{0}$ the **nilradical** of A. We call A **reduced** if nilradical of A is zero, that is, if $\sqrt{(0)} = (0)$.

(a) Show that $\sqrt{I}$ is an ideal of A for any ideal $I \subset A$.

(b) Show that $\sqrt{\sqrt{I}} = \sqrt{I}$.

(c) Show by an example that in a non-commutative ring R, the set

$$\{x \in R \mid x^n = 0 \text{ for some integer } n \in \mathbb{Z}_{\geqslant 1}\},$$

whose elements are called **nilpotent**, is not always an ideal.

A solution to Exercise 2.37 can be found here.

Exercise 2.38: 7.2.

Which of the following rings has no zero divisors? Which are reduced?

(a) $\mathbb{C}[x]/(x^2 + 1)$

(b) $\mathbb{Z}[x]/(x^2 + 1)$

(c) $\mathbb{Z}[x]/(3, x^2 + 1)$

(d) $\mathbb{Z}[x]/(2, x^2 + 1)$

A solution to Exercise 2.38 can be found here.

Exercise 2.39: 7.3.

Let I and J be ideals of a commutative ring R. Define the **ideal quotient**

$$(I : J) \coloneqq \{x \in R \mid xJ \subset I\}.$$

(a) Show that $(I : J)$ is an ideal of R.

(b) For $R = \mathbb{Z}$ and $m, n \in \mathbb{Z}$, compute $((n) : (m))$.

A solution to Exercise 2.39 can be found here.

Exercise 2.40: 7.4.

Let D be a division ring. Show that the ring $M_n(D)$ of $n \times n$ matrices over D has no (two-sided) ideals other than (0) and $M_n(D)$. We call such rings **simple**.

A solution to Exercise 2.40 can be found here.

Exercise 2.41: 7.5.

Let R be a ring, not necessarily commutative. For any abelian group M, recall that $\mathrm{End}_{\mathsf{Grp}}(M) \coloneqq \mathrm{Hom}_{\mathsf{Grp}}(M, M)$ is a ring via $(f+g)(m) = f(m) + g(m)$ and $(f \cdot g)(m) = f \circ g(m)$ for all $m \in M$.

(a) Let M be a left R-module. Show that the map

$$\lambda\colon R \to \mathrm{End}_{\mathsf{Grp}}(M)$$

given by $\lambda(r)(m) = r \cdot m$ is a ring homomorphism. Conversely, show that given any ring homomorphism $\lambda\colon R \to \mathrm{End}_{\mathsf{Grp}}(M)$, we obtain a left R-module structure on M, such that these two procedures are inverses.

(b) Define the **opposite ring** R^{op} of R to be R as additive group but with the nultiplciation

$$r \cdot_{\mathrm{op}} s \coloneqq sr,$$

where the product on the left-hand side is in R^{op}, and the product on the right-hand side is in R. Check that R^{op} is a ring.

(c) Show by analogy with part (a) that a right R-module N is "the same thing" as an abelian group N equipped with a ring homomorphism

$$\rho\colon R^{\mathrm{op}} \to \mathrm{End}_{\mathsf{Grp}}(N).$$

A solution to Exercise 2.41 can be found here.

3 Fundamentals of Ideals in Commutative Rings

Warning 3.1. Henceforth *all rings are assumed commutative*, unless specified otherwise. ☡

3.1 Chinese Remainder Theorem

$\mathbb{Z}$	rings
element n	ideal (n)
product $m \cdot n$	ideal product $(m) \cdot (n) = (mn)$
$\gcd(m, n)$	ideal sum $(m) + (n) = (m, n)$
$\operatorname{lcm}(m, n)$	ideal intersection $(m) \cap (n)$
divisibility $m \mid n$	ideal inclusion $(n) \subset (m)$

Table 3: Features of arbitrary commutative rings, as seen in $\mathbb{Z}$. (Note, however, that containment of ideals is in general weaker than divisibility.)

Definition 3.2.

Ideals I, J of a ring R are **coprime** if $I + J = R$. More generally, ideals $I_1, \ldots, I_n$ are **pairwise coprime** if $I_j + I_k = R$ for any two indices j, k such that $j \neq k$.

Proposition 3.3.

- $I + J = R$ if and only if $1 \in I + J$.
- If $I + J = R$, then $I \cdot J = I \cap J$

The proof of Proposition 3.3 can be found here.

Notation 3.4. If I is an ideal of a commutative ring R, then we write $x \equiv y \pmod{I}$ to mean $x - y \in I$, that is, that $x + I = y + I$ in R/I. #

Theorem 3.5: Chinese Remainder Theorem (CRT).

If $I_1, \ldots, I_n$ are pairwise coprime ideals of a commutative ring R, then the following hold.

(1) Given any $x_1, \ldots, x_n \in R$, there exists $x \in R$ such that

$$x \equiv x_j \pmod{I_j} \text{ for all } j \in \{1, \ldots, n\}.$$

(2) $\bigcap_{j=1}^n I_j = \prod_{j=1}^n I_j$ and the projections $\pi_j \colon R \to R/I_j$ induce an isomorphism of rings

$$R \Big/ \bigcap_{j=1}^n I_j \xrightarrow{\cong} \prod_{j=1}^n R/I_j.$$

The proof of Theorem 3.5 can be found here.

Example 3.6. $R = \mathbb{C}[x]$, $I = (x^3 - 1)$. What is R/I? We can write $(x^3 - 1) = (x - 1)(x - \omega)(x - \overline{\omega})$, where $\overline{\omega}$ is the complex conjugate of ω. So we can write I as the following product of ideals:

$$I = \underbrace{(x-1)}_{=:I_0} \cdot \underbrace{(x-\omega)}_{=:I_1} \cdot \underbrace{(x-\overline{\omega})}_{=:I_2}.$$

Let us show these ideals are pairwise coprime. To see $I_0+I_1=R$, note $I_0+I_1=(x-1,x-\omega)=\frac{1}{\omega-1}(x-\omega-(x-1))=\frac{1-\omega}{1-\omega}=1$, so $1\in I_0+I_1$, meaning $I_0+I_1=R$. Establishing the other two coprimalities is similar. By the Chinese remainder theorem, we have

$$\frac{\mathbb{C}[x]}{(x^3-1)}\cong\frac{\mathbb{C}[x]}{(x-1)}\times\frac{\mathbb{C}[x]}{(x-\omega)}\times\frac{\mathbb{C}[x]}{(x-\overline{\omega})}\cong\mathbb{C}^3,$$

where the last isomorphism is justified as follows. Consider the homomorphism $\mathbb{C}[x]\to\mathbb{C}$ via $f\to f(\omega)$. The kernel is all f such that $f(\omega)=0$, which is $(x-\omega)$. The other two isomorphisms $\mathbb{C}[x]/(x-1)$ and $\mathbb{C}[x]/(x-\omega)$ are similar. Hence $\mathbb{C}[x]/(x^3-1)\cong\mathbb{C}^3$. //

Example 3.7. $R=\mathbb{R}[x]$, and $I=(x^3-1)$. Then

$$I=\underbrace{(x-1)}_{=:I_0}\cdot\underbrace{(x^2+x+1)}_{=:I_1}.$$

What is I_0+I_1? This is $(x-1,x^2+x+1)$. Write $(x-1)^2-(x^2+x+1)=-3x$. Also $3(x-1)=3x-3+(-3)$, so $3\in I_0+I_1$. But 3 is a unit in $\mathbb{R}$, so it is a unit in $\mathbb{R}[x]$. Then

$$1=\frac{1}{3}\cdot 3\in I_0+I_1,\text{ so }I_0+I_1=\mathbb{R}[x].$$

Then by the Chinese remainder theorem,

$$\frac{\mathbb{R}[x]}{(x^3-1)}\cong\frac{\mathbb{R}[x]}{(x-1)}\times\frac{\mathbb{R}[x]}{(x^2+x+1)}.$$

The first factor is $\mathbb{R}$, and this is exactly the same proof as in Example 3.6 that $\mathbb{C}[x]/(x-1)\cong\mathbb{C}$.

Note $\mathbb{R}[z]\cong\mathbb{C}$ for any z with $\operatorname{Im}z\neq 0$. (Check!) In this setting, it is reasonable to guess $\mathbb{R}[x]/(x^2+x+1)\cong\mathbb{R}[\omega]$, where $\omega^2+\omega+1=0$, and hence that $\mathbb{R}[x]/(x^2+x+1)\cong\mathbb{C}$.

We thus consider the map $\mathbb{R}[x]\to\mathbb{C}$ given by $\mathbb{R}[x]\to\mathbb{C}$ via $f(x)\mapsto f(\omega)$. The rest is an exercise. (Use that $f(x)=0$ if and only if $f(\overline{x})=0$). //

Example 3.8. Consider $R=\mathbb{Z}[x]$ and $I=(x^3-1)$. Then

$$I=\underbrace{(x-1)}_{=:I_0}\cdot\underbrace{(x^2+x+1)}_{=:I_1}.$$

Does $I_0+I_1=\mathbb{Z}[x]$? The ideal I_0+I_1 certainly contains $3,x-1$, and x^2+x+1, and hence contains $(3,x-1,x^2+x+1)$. We claim I_0+I_1 does not contain 1. Showing this does not contain 1 directly may be difficult though. But by the contrapositive of the Chinese remainder theorem, this condition implies that I_0 and I_1 are not coprime. To that end, we claim

$$\frac{\mathbb{Z}[x]}{(x^3-1)}\ncong\frac{\mathbb{Z}[x]}{(x-1)}\times\frac{\mathbb{Z}[x]}{(x^2+x+1)}.$$

Note $\mathbb{Z}[x]/(x-1)\cong\mathbb{Z}$ and $\mathbb{Z}[x]/(x^2+x+1)\cong\mathbb{Z}[\omega]$ where ω is as in the previous examples and the reasoning for these are also as in the previous examples. Under these identifications, then $y=(1,0)$ is an element of the right-hand side. And $y^2=y$, but $y\ |(0,0)\neq(1,1)$.

But if $y'=ax^2+bx+c\pmod{x^3-1}\in\mathbb{Z}[x]/(x^3-1)$, and if $(y')^2=y'$, then $y'=0$ or 1, so the left-hand cannot possibly be isomorphic to the right-hand side. //

Note 3.9. Let R be any commutative ring and $a, b \in R$. By the second isomorphism theorem,

$$\frac{R}{(a,b)} \cong \frac{R/(a)}{(a,b)/(a)} \cong \frac{R/(a)}{(b)}. \qquad //$$

Indeed,

$$\frac{R}{(a,b)R} = \frac{R/aR}{(a,b)R/aR} \cong \frac{R/aR}{bR/aR} \cong \frac{R}{bR}$$

where we used the second isomorphism theorem for the first and last isomorphisms.

Example 3.10. Let $R = \mathbb{Z}[x]$ and $I = (2, x^3 - 1)$. What is R/I? Let us again try to factorize I as we have in the previous examples. Write

$$I_0 = (2, x-1) \supset I \text{ and } I_1 = (2, x^2 + x + 1) \supset I.$$

It would be nice if $I = I_0 \cdot I_1$. And indeed, we have

$$I_0 + I_1 = (2, x-1, x^2 + x + 1).$$

We already know from the previous example how to get a 3 from $(x-1, x^2+x+1)$ (which is in $I_0 + I_1$ above), and this time we can get 2. Thus we can get all of $\mathbb{Z}$, and hence all of $\mathbb{Z}[x]$ because then $1 + x - 1 = x$ is in the ideal as well. Thus $I_0 \cap I_1 = I_0 \cdot I_1$. Now

$$\begin{aligned} I_0 \cdot I_1 = I_0 \cap I_1 \subset (2, x^3 - 1) &= (2, x-1) \cdot (2, x^2 + x + 1) \\ &= (4, 2x - 2, 2x^2 + 2x + 2, x^3 - 1) = (2, x^3 - 1). \end{aligned}$$

So $I_0 \cdot I_1 = I$. Thus

$$\frac{\mathbb{Z}[x]}{(2, x^3 - 1)} \cong \frac{\mathbb{Z}[x]}{(2, x-1)} \times \frac{\mathbb{Z}[x]}{(2, x^2 + x + 1)}.$$

By Note 3.9,

$$\frac{\mathbb{Z}[x]}{(2, x-1)} \cong \mathbb{Z}/2\mathbb{Z} \text{ and } \frac{\mathbb{Z}[x]}{(2, x^2+x+1)} \cong \frac{\mathbb{Z}[x]/(x^2+x+1)}{(2)} \cong \frac{\mathbb{Z}[\omega]}{(2)} \cong \mathbb{F}_4,$$

so

$$\frac{\mathbb{Z}[x]}{(2, x^3 - 1)} \cong \frac{\mathbb{Z}}{2\mathbb{Z}} \times \mathbb{F}_4.$$

where $\mathbb{F}_4$ is as in Example 1.39. //

Example 3.11. If $m_1, m_2, \ldots, m_n \in \mathbb{Z}$ are pairwise coprime, then there is an isomorphism of rings

$$\frac{\mathbb{Z}}{m_1 \cdots m_n \mathbb{Z}} \xrightarrow{\cong} \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z}.$$

In particular, we obtain an isomorphism of unit groups

$$\left(\frac{\mathbb{Z}}{m_1 \cdots m_n \mathbb{Z}}\right)^{\times} \xrightarrow{\cong} (\mathbb{Z}/m_1\mathbb{Z})^{\times} \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})^{\times}.$$

Define the **Euler φ function** by

$$\varphi(m) = |\{i \in \mathbb{Z} \mid 1 \leqslant i \leqslant m \text{ and } \gcd(m, i) = 1\}| = |(\mathbb{Z}/m\mathbb{Z})^{\times}|.$$

It then follows from the above isomorphism that

$$\varphi(m_1 m_2 \cdots m_n) = \varphi(m_1)\varphi(m_2)\cdots\varphi(m_n). \qquad //$$

Exercise 3.12.

Show that if $p, r \in \mathbb{Z}$, p is prime, and $r \in \mathbb{Z}_{\geqslant 1}$, then $\varphi(p^r) = (p-1)p^{r-1}$.

3.2 Prime Ideals and Spec

Definition 3.13.

Let R be a commutative ring. A **prime ideal** of R is a proper ideal I of R such that for all $x, y \in R$, $xy \in I$ implies $x \in I$ or $y \in I$.

We often say "I is prime in R" to mean I is a prime ideal of R, or even simply "I is prime" when the ring R is understood.

Example 3.14. Let p be a prime integer. Then $p\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$, since $p \mid ab$ implies $p \mid a$ or $p \mid b$. This is what motivates the terminology "prime ideal" in the first place. Note that (0) is another prime ideal in $\mathbb{Z}$. More generally, (0) is prime in a commutative ring R if and only if R is an integral domain. //

Example 3.15. Consider $R = \mathbb{C}[x]$. Then (0) is a prime in $\mathbb{C}[x]$. All ideal of $\mathbb{C}[x]$ are principal by Exercise 8.1, so $I = (f(x))$ for some $f(x)$. Then an ideal I is prime in $\mathbb{C}[x]$ if and only if $f(x)$ is irreducible, and therefore (by the fundamental theorem of algebra) this is equivalent to $f(x) = x - a$ for some $a \in \mathbb{C}$. //

Example 3.16. Consider $R = \mathbb{Z}[x]$. Some prime ideals of $\mathbb{Z}[x]$ are

- (0),
- (p) for prime integers p,
- $(x - a)$ for any integer a,
- (p, x) for prime integers p,
- $(x^2 + 1)$, $(3, x^3 + 1)$.

Note that these are *not* all prime ideals of $\mathbb{Z}[x]$, as classifying such ideals is rather complicated. For a non-example, note that the ideal $(2, x^2 + 1)$ is *not* prime (see Exercise 7.2). //

Theorem 3.17: Criterion for Primality.

Let R be any commutative ring. Then an ideal I of R is prime if and only if R/I is an integral domain.

The proof of Theorem 3.17 can be found here.

Notation 3.18. We write $\operatorname{Spec}(R)$ for the set of all prime ideals of a ring R. #

Note 3.19. “Spec” stands for “spectrum”. For commutative rings A, we will investigate a topology for $\operatorname{Spec}(A)$ that links commutative algebra with algebraic geometry. (See Exercises 8.4 and 8.5.) //

Example 3.20. **(Functoriality of** Spec) Let A and B be commutative rings and let $\varphi\colon A \to B$ be a ring homomorphism. Define a map $f\colon \operatorname{Spec} B \to \operatorname{Spec} A$ by the preimage map $f(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$ for all $\mathfrak{p} \in \operatorname{Spec} B$. Then for all $\mathfrak{p} \in \operatorname{Spec} B$,

$$f(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p}) = \{x \in A \mid \varphi(x) \in \mathfrak{p}\}.$$

Note f is well-defined, because $\mathfrak{q} := \varphi^{-1}(\mathfrak{p})$ is indeed a prime ideal: if $x, y \in \mathfrak{q}$, so $\varphi(x), \varphi(y) \in \mathfrak{p}$, then $\varphi(x+1) = \varphi(x) + \varphi(y) \in \mathfrak{p}$, so $x + y \in \varphi^{-1}(\mathfrak{p})$; and for all $r \in A$,

$$\varphi(rx) = \varphi(r) \cdot \underbrace{\varphi(x)}_{\in\mathfrak{p}} \in \mathfrak{p},$$

so $rx \in \varphi^{-1}(\mathfrak{p})$. (This shows $\varphi^{-1}(I)$ is an ideal for any ideal I). And $\mathfrak{q}$ is prime: if $x, y \in A$ such that $xy \in \varphi^{-1}(\mathfrak{p})$, then $\varphi(x) \cdot \varphi(y) \in \mathfrak{p}$, so $\varphi(x) \in \mathfrak{p}$, so $\varphi(x) \in \mathfrak{p}$ or $\varphi(y) \in \mathfrak{p}$. Hence x or y is in $\varphi^{-1}(\mathfrak{p})$. //

Example 3.21. Consider the mapping $\varphi\colon \mathbb{Z} \to \mathbb{Z}[i]$, where $\mathfrak{p} = (2 + i)$ is prime in $\mathbb{Z}[i]$. The set $5\mathbb{Z}$, which is the principal ideal generated by 5 in $\mathbb{Z}$, is equal to the intersection $\mathbb{Z} \cap \mathfrak{p}$ and is also the preimage of $\mathfrak{p}$ under the mapping φ. //

3.3 Maximal Ideals

Definition 3.22.

An ideal I of a ring R is called **maximal** if $I \neq R$ and there are no ideals J of R such that $I \subsetneq J \subsetneq R$.

We can interpret this as a statement about the quotient rings in the following way.

Theorem 3.23: Criterion for Maximality.

An ideal I of R is maximal if and only if R/I is a field.

The proof of Theorem 3.23 can be found here.

Corollary 3.24.

Maximal ideals are prime.

The proof of Corollary 3.24 can be found here.

Warning 3.25. The converse of Corollary 3.24 is not true. Indeed, if p is a prime integer, then

$$\operatorname{Spec}\mathbb{Z} = \underbrace{\{(0)\}}_{\substack{\text{prime, but}\\ \text{not maximal,}\\ \text{since } (0)\subsetneq(p)\subsetneq\mathbb{Z}}} \cup \underbrace{\{(p)\}}_{\substack{\text{maximal,}\\ \text{since } p \text{ is prime}}}.$$ ☡

Note 3.26. Given a ring homomorphism $\varphi\colon A \to B$ and a maximal ideal $\mathfrak{m} \subset B$, we know $\varphi^{-1}(m)$ is prime, but it is *not* maximal in general. For instance, the inclusion $\varphi\colon \mathbb{Z} \to \mathbb{Q}$ $(0) \subset \mathbb{Q}$ is maximal, $\varphi^{-1}((0)) = (0)$ is not //

Theorem 3.27.

Let I be a proper ideal of a possibly noncommutative nonzero ring R. Then there exists a maximal ideal $\mathfrak{m}$ of R containing I. (In particular, by considering $I = (0)$, all rings have a maximal ideal.)

The proof of Theorem 3.27 can be found here.

Note 3.28. For "small enough" rings Zorn's Lemma is not needed to show the existence of maximal ideals. In particular, it is immediate from the definition that Noetherian rings have maximal ideals. (We will define Noetherian rings soon.) //

Note 3.29. Consider a homomorphism of the underlying groups of finitely generated $\mathbb{C}$-algebras,

$$\varphi\colon \underbrace{\mathbb{C}[x_1, \ldots, x_n]/I}_{=:A} \to \underbrace{\mathbb{C}[y_1, \ldots, y_m]/J}_{=:B}.$$

The maximal ideals $\mathfrak{m}$ of B are of the form $(y_1 - a_1), \ldots, (y_m - a_m)$ for some $a_i \in \mathbb{C}$, and likewise for A. In particular, $B/\mathfrak{m} = \mathbb{C}$. Then to see $\varphi^{-1}(\mathfrak{m})$ is maximal, we consider the following commutative diagram:

$$\begin{tikzcd}
A/\varphi^{-1}(\mathfrak{m}) \arrow[rr, hook] & & B/\mathfrak{m} \\
& \mathbb{C} \arrow[ul, "\cong"] \arrow[ur] &
\end{tikzcd}$$

Since the bottom left map is an isomorphism, the bottom right map is an isomorphism. Thus $\varphi^{-1}(\mathfrak{m})$ is maximal. This line of reasoning is called the **Hilbert Nullstellensatz**. //

3.4 Spectrum of $k[x]$

Let R be a commutative ring and let I be an ideal of R. In particular, let us consider the case k is a field and $R = k[x]$. What are the prime and maximal ideals of $k[x]$? We know from Exercise 8.1 that $k[x]$ is a PID, so all ideals of $k[x]$ take the form $(f(x))$ for some polynomial $f(x) \in k[x]$. Certainly (x) is maximal because the ring map $k[x] \to k$ via $f(x) \mapsto f(0)$ is surjective with kernel (x), so $k[x]/(x) \cong k$ is a field. But when is $(f(x))$ prime?

Proposition 3.30.

If $f(x) \neq 0$, then $(f(x))$ is prime if and only if $f(x)$ is irreducible in $k[x]$.

The proof of Proposition 3.30 can be found here.

Note 3.31. The upshot of Proposition 3.30 that if k is a field and $f(x) \in k[x]$, then

$$(f(x)) \text{ is prime} \iff (f(x)) \text{ is maximal} \iff f(x) \text{ is irreducible.}$$ //

Corollary 3.32.

If k is any field, then

$$\operatorname{Spec} k[x] = \{(0)\} \cup \{(f(x)) \mid f(x) \text{ is irreducible in } k[x]\}.$$

Example 3.33. What is $\operatorname{Spec}\mathbb{Z}[i]$?

- (0) is prime.
- (2) is not prime, since $(1+i)(1-i) = 2$. Thus $\mathbb{Z}[x]/(2, x^2+1) \cong \mathbb{Z}[i]/(2)$ is not an integral domain.
- (3) is a prime, since $\mathbb{Z}[x]/(3, x^2+1) \cong \mathbb{Z}[i]/(3)$ has no zerodivisors. (See Exercise 7.2(c)).
- When is (p) prime in $\mathbb{Z}[i]$ for prime integers p? Certainly not when $p = 1 + a^2$ for $a \in \mathbb{Z}$, since then $p = 1 + a^2 = (1+ai)(1-ai)$, and then apply the same argument from the previous point. Note
$$\frac{\mathbb{Z}[i]}{(p)} \cong \frac{\mathbb{Z}[x]}{(p, x^2+1)} \cong \frac{(\mathbb{Z}/p\mathbb{Z})[x]}{(x^2+1)}.$$
Is x^2+1 prime in $(\mathbb{Z}/p\mathbb{Z})[x]$? Well, it is if and only if x^2+1 is irreducible in $\mathbb{Z}/p\mathbb{Z}[x]$ if and only if x^2+1 has no roots modulo p if and only if -1 is not a square mod p, which turns out to be true if and only if $p \equiv 3 \pmod 4$. (You can show that if $p \equiv 1 \pmod 4$ then p is a sum of squares and therefore is not a prime.) //

The upshot of Example 3.33, modulo the final "if and only if" in the argument, is the following well-known fact:

Corollary 3.34.

If p is a prime integer, then

$$(p) \text{ is prime in } \mathbb{Z}[i] \qquad \Longleftrightarrow \qquad p \equiv 3 \pmod 4.$$

We have now done some number theoretic examples; we now turn to more geometric examples.

Example 3.35. Let $R = \mathbb{R}[x,y]$. Consider for $(a,b) \in \mathbb{R}^2$ the ideal

$$I = \{f \in R \mid f(a,b) = 0\}.$$

We will now check if I maximal or prime. Consider the evaluation map $\mathbb{R}[x,y] \to \mathbb{R}$ sending $f(x,y) \mapsto f(a,b)$. This is surjective, since $t \mapsto t$ for all $t \in \mathbb{R}$. The kernel is the set of all polynomials $f(x) \in \mathbb{R}[x,y]$ such that $f(a,b) = 0$, so its kernel is I by definition. But this shows $\mathbb{R}[x,y]/I \cong \mathbb{R}$ is a field, so I is maximal.

What are the generators of I? Certainly $(x-a, y-b) \subset I$, and the reverse inclusion is true for the following reason: $f(x,y) = f(a,b) +$ polynomials g in $x-a, y-b$ with $g(a,b) = 0$. Then $f(a,b) = 0 \implies f(x,y) \in (x-a, y-b)$. So $I \subset (x-a, y-b)$, so $I = (x-a, y-b)$.

We can interpret this geometrically as follows: the collection of polynomials I vanishing at $(a,b) \in \mathbb{R}^2$ is given by $(x-a, y-b)$. Thus, we can think of $(x-a, y-b)$ as the point (a,b) in $\mathbb{R}^2$. //

Example 3.36. Similarly, consider $I = \{f \in \mathbb{R}[x,y] \mid f(x,x^2) = 0\}$. This corresponds to the curve $y = x^2$, since I is the ideal of all polynomials that vanish on *every pont* of this parabola. We can argue this as follows.

Is I prime? Is I maximal? Consider the map R/I defined by $\mathbb{R}[x,y] \to \mathbb{R}[x]$ via $f(x,y) \mapsto (x,x^2)$. Its kernel is the set $\{f(x,y) \mid f(x,x^2) = 0\} =: I$, so

$$\mathbb{R}[x,y]/I \cong \mathbb{R}[x],$$

which is an integral domain but not a field. Thus I is prime but not maximal.

Now what are the generators of I? Certainly $y - x^2 \in I$, since the function $f(x,y) = y - x^2$ vanishes on the parabola. Thus $(x^2 - y) \subset I$. Conversely, if $f \in \mathbb{R}[x,y]$, we can Taylor expand the polynomial $f(x,y)$ in the single variable x as

$$f(x,y) = f(x,x^2) + (y - x^2)\frac{\partial f}{\partial y}(x,x^2) + \frac{(y-x^2)}{2}\frac{\partial^2 f}{\partial y^2}(x,x^2) + \cdots,$$

so in particular if $f(x,x^2) = 0$ then $f(x,y) \in (y - x^2)$. So $I = (y - x^2)$. This converse direction requires more details to be made formal, but this is the key idea.

But what maximal ideals contain I? The point $(0,0)$ corresponds to the point (x,y). And it is easy to check that $(y - x^2) \subset (x,y)$. Similarly, the point $(2,4)$ on the parabola corresponds to the point $(x-2, y-4)$, so geometrically we should believe that $(y - x^2) \subset (x-2, y-4)$. And this is true (indeed, one can check $y - x^2 = (y-4) - (x-2)^2 - 4(x-2))$, but seeing and proving this algebraically is a pain. But as we have just shown, this is not so difficult to see geometrically, so the geometric interpretation can sometimes be more useful or intuitive than the algebraic interpretation. (Bonus question: Are there any other maximal ideals that contain this point?) //

3.5 Prime Avoidance

Theorem 3.37.

Suppose $I_1, \ldots, I_n$ are ideals of a commutative ring R.

(1) (Prime Avoidance). If $J \subset \bigcup_{j=1}^n I_j$ and all but at most two among $I_1, \ldots, I_n$ are prime, then $J \subset I_j$ for some $j \in \{1, \ldots, n\}$. (The contrapositive is that if J is not contained in any of the I_js, then J is not contained in the union of the I_js).

(2) Let $\mathfrak{p}$ be a prime ideal and let $I_1, \ldots, I_n$ be ideals of a commutative ring R such that $\mathfrak{p} \supset \bigcap_{j=1}^k I_j$. Then $\mathfrak{p} \supset I_j$ for some j. In particular, if $\mathfrak{p} = \bigcap_{j=1}^n I_j$, then $\mathfrak{p} = I_j$ for some j.

The proof of Theorem 3.37 can be found here.

Corollary 3.38.

The following hold in any commutative ring A.

(1) If $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in \operatorname{Spec} A$, then $\bigcup_{j=1}^n = \mathfrak{p}_k$ for some $k \in \{1, \ldots, n\}$.

(2) If $I_1, \dots, I_n$ are ideals of A and $\bigcap_{j=1}^{n} I_j = \mathfrak{p} \in \operatorname{Spec} A$, then $I_k = \mathfrak{p}$ for some $k \in \{1, \dots, n\}$.

3.6 Homework 8

Exercise 3.39: 8.1.

Let R be an integral domain. A **Euclidean valuation** of R is a set function $d\colon R \smallsetminus \{0\} \to \mathbb{Z}_{\geqslant 0}$ such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $d(r) < d(b)$. An integral domain that has a Euclidean valuation is called a **Euclidean domain**.

(a) Let K be a field. Show that $K[x]$ has Euclidean valuation $d(f(x)) = \deg(f(x))$, the degree of $f(x)$.

(b) Show that any Euclidean domain R is a principal ideal domain.

A solution to Exercise 3.39 can be found here.

Exercise 3.40: 8.2.

Let R be a commutative ring. Prove that

$$\sqrt{(0)} = \bigcap\nolimits_{\mathfrak{p} \in \operatorname{Spec}(R)} \mathfrak{p}.$$

Hint: For the difficult direction, if $f \in R$ is not nilpotent, consider the set $\mathcal{S}$ of all ideals $I \subset R$ such that for all $n > 0$, $f^n \notin I$. Use Zorn's Lemma to show $\mathcal{S}$ has a maximal element M, and show that M is prime.

A solution to Exercise 3.40 can be found here.

Exercise 3.41: 8.3.

Let R be a commutative ring. We define the **Jacobson radical** $J(R)$ of R by

$$J(R) = \{x \in R \mid 1 - xy \in R^\times \text{ for all } y \in R\}.$$

(a) Show that $J(R)$ is an ideal of R.

(b) Show that

$$J(R) = \bigcap\nolimits_{\mathfrak{m} \in \operatorname{Max}(R)} \mathfrak{m},$$

where $\operatorname{Max}(R)$ is the set of maximal ideals of R.

A solution to Exercise 3.41 can be found here.

Exercise 3.42: 8.4.

Let R be a ring. For any subset S of R, define

$$V(S) = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid S \subset \mathfrak{p}\}.$$

(a) Let $I = (S)$, the ideal generated by S. Show that $V(S) = V(I) = V(\sqrt{I})$.

(b) Show that the sets $V(S)$ for varying subsets $S \subset R$ (or equivalently $V(I)$ for varying ideals I) satisfy the axioms needed to be the closed subsets of a topology on $\operatorname{Spec}(R)$. This is called the **Zariski topology** on $\operatorname{Spec}(R)$.

(c) Give an example showing that the Zariski topology is not always Hausdorff. (Indeed, it very rarely is.)

A solution to Exercise 3.42 can be found here.

Exercise 3.43: 8.5.

Show that if A and B are commutative rings, then any surjective ring homomorphism $\varphi \colon A \twoheadrightarrow B$ induces a homeomorphism of $\operatorname{Spec} B$ onto the closed subset $V(\ker \varphi)$ of $\operatorname{Spec} A$.

A solution to Exercise 3.43 can be found here.

4 Local Rings and Localization

Again in this section all rings are assumed commutative unless specified otherwise.

By "inverting" elements we can "destroy" certain prime ideals of our ring. For example, in $\mathbb{Z}$, if you invert a prime ideal p, then there is no prime ideal generated by p since p is now a unit, and hence generates the (non-prime) unit ideal. Informally, by inverting an element of $\mathbb{Z}$ we obtain a ring that looks a lot like $\mathbb{Z}$, but without an ideal generated by p.

4.1 Local Rings

Definition 4.1.

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

Example 4.2. Any field is a local ring, with maximal ideal (0). //

Example 4.3. If k is a field, then $R = k[x]/(x^n)$ is a local ring with maximal ideal (x). Indeed, by the correspondence theorem, the ideals of R are in correspondence with ideals I of $k[x]$ containing (x^n). Thus, if I is maximal and $x^n \in I$, then $x \in I$ (since if I is maximal then I is prime, hence radical), so it follows that $(x) \subset I$. And (x) is a *maximal* ideal in $k[x]$ because $k[x]/(x) \xrightarrow{\cong} k$ is a field. //

Note 4.4. Local rings are called "local" because they capture the local geometry of an algebraic variety. This is suggested by Example 4.3, since passing from a polynomial $f(x) \in k[x]$ to its image in $k[x]/(x^n)$ is the same as truncating $f(x)$ as to preserve only terms of degree less than n. In turn, this image contains precisely the information of the kth derivative of $f(x)$ for all $k \in \{1, \ldots, n-1\}$. Thus elements here contain "tangent information," and this is true in a formal sense. //

Example 4.5. Where p is a prime integer, the p-adic integers $\mathbb{Z}_p$ is a local ring, with maximal ideal (p). //

Theorem 4.6.

Let $\mathfrak{m}$ be an ideal of a ring R. Then R is local with maximal ideal $\mathfrak{m}$ if and only if $\mathfrak{m} = R \smallsetminus R^\times$.

The proof of Theorem 4.6 can be found here.

4.2 Spectrum of $k[[x]]$

Definition 4.7: Ring of Formal Power Series.

Let R be a commutative ring. Define the **ring of formal power series over $\boldsymbol{R}$**, denoted $R[[x]]$, as follows.

- As a set, $R[[x]] = \{\{a_n\}_{n \in \mathbb{Z}_{\geqslant 0}} \mid a_n \in R\}$,
- addition is given by $\{a_n\}_{n \in \mathbb{Z}_{\geqslant 0}} + \{b_n\}_{n \in \mathbb{Z}_{\geqslant 0}} = \{a_n + b_n\}_{n \in \mathbb{Z}_{\geqslant 0}}$,
- the additive identity is given by $0 = (0, 0, \ldots,)$,
- multiplication is given by $\{a_n\}_n \cdot \{b_n\}_n = \{\sum_{k=0}^n a_k b_{n-k}\}_{n \in \mathbb{Z}_{\geqslant 0}}$, and
- the multiplicative identity is given by $1 = (1, 0, 0, \ldots)$.

One can check that the above operations indeed make $R[[x]]$ into a ring.

Notation 4.8. In the context of Definition 4.7, we will usually write $\{a_n\}_{n \in \mathbb{Z}_{\geqslant 0}}$ as $\sum_{n=0}^\infty a_n x^n$. #

Example 4.9. In this ring, we note that

$$(1-x)^{-1} = 1 + x + x^2 + x^3 + \cdots = \sum_{n=0}^\infty x^n,$$

so $(1-x)\sum_{n=0}^\infty x^n = 1$. Thus $1 - x \in R[[x]]^\times$, which is in stark contrast to the usual polynomial ring $R[x]$, whose units are simply the units of R. //

Note 4.10. Let $f \in R[[x]]$. Then

$$(1 - xf)(1 + xf + (xf)^2 + (xf)^3 + (xf)^4 + \cdots) = 1. \tag{4.10.1}$$

For all n, the coefficient of x^n is a finite sum, and hence is well-defined in $R[[x]]$. Then we can check the coefficient of all terms x^n for $p \geqslant 0$ to conclude Equation (4.10.1) holds. //

Proposition 4.11.

Let R be a commutative ring. Then

$$\sum_{n=0}^{\infty} a_n x^n \in R[[x]]^{\times} \qquad \iff \qquad a_0 \text{ is a unit in } R.$$

The proof of Proposition 4.11 can be found here.

Now let k be a field. What are the prime ideals of $k[[x]]$? And more generally, what are the ideals of $k[[x]]$? Well, we can name some ideals right away:

- (x) is an ideal. The degree function is not well-defined on $k[[x]]$, which hints that it is easiest to consider the quotient $k[[x]]/(x)$. Consider the map $k[[x]] \to k$ given by $f(x) \mapsto f(0)$. This map makes sense since all terms of degree $\geqslant 1$ vanish. One can check its kernel is (x), so we conclude $k[[x]]/(x) \cong k$, a field, and hence (x) is maximal.
- (0) is an ideal. It is prime, since one can check that if two power series multiply to 0, then, by induction, all coefficients of one of the polynomials are zero.
- Note that if $f \in k[[x]] \setminus (x) = k$, then f is a unit (since k is a field). Thus by Theorem 4.6, (x) is the *unique* maximal ideal, which means $k[[x]]$ is a local ring.

Definition 4.12.

Let R be a commutative ring. For all elements $f(x) = \sum_{n=0}^{\infty} a_n x^n$ of $R[[x]]$, define

$$v(f) \coloneqq \min\{a_n \mid a_n \neq 0\}.$$

Similarly, for all ideals I of R, we define $v(I) \coloneqq \min\{v(f) \mid f \in I\}$.

Note 4.13. Observe for an element $f(x) \in k[[x]]$ that

$$v(f) = 0 \iff f \text{ is a unit of } k[[x]]. \qquad //$$

Proposition 4.14.

Let I be any ideal of $R[[x]]$, where R is any commutative ring. Then $I = (x^{v(I)})$. Therefore, if k is a field, then

$$\operatorname{Spec} k[[x]] = \{(0), (x)\}.$$

The proof of Proposition 4.14 can be found here.

Note 4.15. So, although $k[[x]]$ is a very large ring, its ideal structure is very simple. It is a local ring, and we can write down all its ideals very easily. On the other hand, the polynomial $k[x]$ is much smaller, but its ideal structure is much more complicated (see Corollary 3.32). //

Example 4.16. Let k be a field and let $n \in \mathbb{Z}_{\geqslant 1}$. Then $k[x]/(x^n)$ has a unique maximal ideal, (x). Indeed, by the correspondence theorem,

$$\left\{\begin{matrix}\text{ideals of } k[x] \\ \text{containing } (x^n)\end{matrix}\right\} \longleftrightarrow \left\{\begin{matrix}\text{ideals of} \\ k[x]/(x^n)\end{matrix}\right\},$$

$$\begin{aligned} I &\longmapsto \text{image of } I, \\ \text{preimage of } \overline{I} &\longleftarrow \overline{I}. \end{aligned}$$

This bijection preserves maximal ideals, since it is inclusion-preserving, and hence bijects the corresponding sets of maximal ideals. Then by Theorem 4.6, the theorem that R is local with maximal ideal $\mathfrak{m}$ if and only if $R \smallsetminus \mathfrak{m} = R^\times$ implies the element $u \coloneqq 1 + x$ is not in $\mathfrak{m}$, hence is a unit—indeed, this is because $(1+x)(1-x+x^2-\cdots+(-1)^{n-1}x^{n-1}) = 1$. More generally, the element $a + f(x)$ is not in $\mathfrak{m}$ for any $a \in k$ and $f(x) \in k[x]$, so $u \in R^\times$. //

The following is another example of the above theorem.

Example 4.17. Let p be a prime number, and define $\mathbb{Z}_{(p)} \subset \mathbb{Q}$ by

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; a, b \in \mathbb{Z}, \gcd(a,b) = 1, p \nmid b \right\}.$$

One can check $\mathbb{Z}_{(p)}$ is a subring of $\mathbb{Q}$, and that

$$\mathbb{Z}_{(p)}^\times = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; a, b \in \mathbb{Z}, \gcd(a,b) = 1 \text{ and } p \nmid a \cdot b \right\}.$$

And $\mathbb{Z}_{(p)} \smallsetminus \mathbb{Z}_{(p)}^\times = p\mathbb{Z}_{(p)}$ is an ideal, so by the lemma $\mathbb{Z}_{(p)}$ is a local ring with maximal ideal $p\mathbb{Z}_{(p)}$. //

4.3 Localization and Localization at Prime Ideals

We continue the convention that all rings used are commutative unless otherwise specified. The ideas and notation in Example 4.17 hint at a more general construction, which we now pursue.

Suppose we have an integral domain A. By "inverting" the nonzero elements of A, we form a field called the **fraction field of A**, denoted $\operatorname{Frac}(A)$. For example, $\operatorname{Frac}\mathbb{Z} = \mathbb{Q}$.

$\mathbb{Z}_{(p)}$ is an example where we invert "most" elements of $A \smallsetminus \{0\}$. Let us now formalize and vastly generalize this procedure.

First we need to know what kind of subsets of elements in A we can invert in the ring, and in doing so generalize this procedure to commutative rings that are not necessarily integral domains.

Definition 4.18.

Let A be any commutative ring. A subset S of an A is called **multiplicatively closed** if S is a submonoid of the monoid $(A, \cdot)$, or equivalently, if $1 \in S$ and S is closed under multiplication, that is, for all $a, b \in S$, $ab \in S$.

Definition 4.19: Localization.

Let A be any ring. Given a multiplicatively closed subset S of A, we define a ring called the **localization of S by A**, denoted $S^{-1}A$, by

$$S^{-1}A \coloneqq (A \times S)/\!\sim,$$

as a set where $\sim$ is the equivalence relation generated by the relations

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

over all $a, b \in A$, $s, t \in S$. We define addition by

$$(a, s) + (b, t) = (at + bs, st),$$

and $(a, s) \cdot (b, t) = (ab, st)$.

Proposition 4.20.

The localization of A by S is well-defined, and forms a commutative ring with additive identity $(0, 1)$ and multiplicative identity $(1, 1)$. Moreover, there exists a canonical ring homomorphism $j \colon A \to S^{-1}A$ given by $a \mapsto (a, 1)$.

The proof of Proposition 4.20 can be found here.

Example 4.21. If $S = A^\times$, then $A \to S^{-1}A$ by the canonical map is an isomorphism. //

Example 4.22. If $0 \in S$, then $S^{-1}A = \{0\}$. Indeed, then any two elements $(a, s), (b, t) \in S^{-1}A$ are equal, because

$$\underbrace{0}_{\in S} \cdot (at - bs) = 0.$$

Hence $S^{-1}A$ only has one element, so $A = \{0\}$. //

The following remark is very useful in many situations.

Note 4.23. If A is an integral domain S is any multiplicatively closed subset not containing 0, then

$$a/b = c/d \text{ in } S^{-1}A \qquad \iff \qquad at - bs = 0 \text{ in } S^{-1}A.$$ //

Example 4.24. For any commutative ring A, the subset $S = \{\text{non-zerodivisors in } A\}$ of A is multiplicatively closed, and we define the **total ring of fractions**, denoted $\operatorname{Frac} A$, as the ring $S^{-1}A$. //

Example 4.25. $S \coloneqq A \smallsetminus \{0\}$ is a multiplicatively closed subset of A if and only if A is an integral domain, and in this case $S^{-1}A$ is a field. We call this field the **field of fractions** of A, and again denote it by $\operatorname{Frac} A$ (but sometimes also by $\operatorname{Quot} A$ or $\operatorname{Fr} A$). //

Example 4.26. $A = \mathbb{C}[x, y]/(xy)$ is not an integral domain, since it has zerodivisors x and y. Its total ring of fractions turns out to be

$$\operatorname{Frac}\left(\frac{\mathbb{C}[x, y]}{(xy)}\right)$$

where $\mathbb{C}(x) \coloneqq \operatorname{Frac}(\mathbb{C}[x])$ is the field of rational functions in x over $\mathbb{C}$. By Exercise 9.5 its total ring of fractions is isomorphic to the product $\mathbb{C}(x) \times \mathbb{C}(y)$ of the rings $\mathbb{C}(x)$ and $\mathbb{C}(x)$ of rational functions in x and y, respectively. This suggests that geometrically this ring should be thought of as the union of the x and y axes, so the total ring of fractions is simply the product of the fraction fields. This observation can be made formal as follows. To turn this suggestion into a formal observation one can use the two natural surjective ring homomorphisms $A \twoheadrightarrow A/(y) \cong \mathbb{C}[x]$ and $A \twoheadrightarrow A/(x) \cong \mathbb{C}[y]$ together with Exercise 8.5. //

Example 4.27. For any ring A and any $f \in A$, the set $S = \{f^n\}_{n \in \mathbb{Z}_{\geqslant 0}}$ is multiplicatively closed. Intuitively, $S^{-1}A$ is "$A[1/f]$". //

Example 4.28. For any A, if $\mathfrak{p} \in \operatorname{Spec} A$, then $S = A \smallsetminus \mathfrak{p}$ is multiplicatively closed. In this case we use the notation

$$A_{\mathfrak{p}} \coloneqq S^{-1}A.$$

For example, $(\mathbb{Z} \smallsetminus p\mathbb{Z})^{-1}\mathbb{Z} = \mathbb{Z}_{(p)}$. //

Lemma 4.29.

For any multiplicatively closed subset S of A,

$$\ker(j) = \{a \in A \mid \text{there exists } s \in S \text{ such that } sa = 0\}.$$

The proof of Lemma 4.29 can be found here.

Example 4.30. The key special case of the above argument is when A is an integral domain. Then $j \colon A \to S^{-1}A$ is injective as long as $0 \notin S$. More generally, j is injective if $S \subset \{\text{nonzerodivisors}\}$. //

Where $R = \mathbb{Q}$ and $S = \mathbb{Q} \smallsetminus \{0\}$, $S^{-1}\mathbb{Q} \to \mathbb{Q}$ via $(a, b) \mapsto a/b$ is an isomorphism. Thus this process generalizes the construction of the rationals from the integers.

Example 4.31. Let $R = k[x]$ and $S \equiv k[x] \smallsetminus \{0\}$. Then

$$S^{-1}R = \{(p(x), q(x)) \mid q(x) \neq 0\} \cong k(x).$$

(The field of fractions for an integral domain is the smallest field containing the ring. Thus if we want to try to understand the ring by using field arithmetic, then we want to use the field of fractions of the ring.) //

Example 4.32. Let R be any ring, $f \in R$, $S = \{1, f, f^2, f^3, f^4, \ldots\}$. Define

$$R_f \coloneqq S^{-1}R.$$

If $R = \mathbb{Z}$ and f is a prime integer p, then

$$R_f = \mathbb{Z}_p = \{(a, p^k) \mid a \in \mathbb{Z}, k \geqslant 0\},$$

where

$$(a, p^k) \sim (b, p^\ell) \iff ap^\ell - bp^k = 0 \iff \frac{a}{p^k} = \frac{b}{p^\ell}.$$

Thus

$$\mathbb{Z}_p \cong \mathbb{Z}[1/p] = \{a \in \mathbb{Q} \mid \text{in lowest terms the denominator is a power of } p\}. \quad //$$

Example 4.33. If $R = \mathbb{Z}/p^3\mathbb{Z}$, f is a prime integer p. Then

$$R_f = \left(\frac{\mathbb{Z}}{p^3\mathbb{Z}}\right) = 0,$$

by an argument similar to that of Example 4.22, since p is a zerodivisor in R. //

Intuitively, the claimed isomorphism in the following lemma makes sense since we are just formally introducing an element $1/f$ to the ring that is the inverse of f.

Lemma 4.34.

If f is not a nilpotent element of a ring R, then

$$R_f \cong R[x]/(xf-1).$$

In other words, if $f \notin \sqrt{(0)}$ then $A_f \cong A[1/f]$. (Here we are abusing notation to write $A[1/f] \cong A_f$.)

The proof of Lemma 4.34 can be found here.

Example 4.35. Let $R = \mathbb{Z}/6\mathbb{Z}$ and $f = 2$. Then R_f is the "integers mod 6, with 2 invertible." Perhaps by intuition, one may guess $R_f \cong \mathbb{Z}/3\mathbb{Z}$. It turns out that indeed this is the case, and we prove this formally: Note

$$R_f = \{(a,1),(a,2),(a,4) \mid a \in \mathbb{Z}/6\mathbb{Z}\}.$$

If $a \equiv 0 \pmod 6$ or $a \equiv 3 \pmod 6$, then $(a, 2^k) = (0,1)$ because

$$(a \cdot 1 - 0 \cdot 2^k) \cdot \underbrace{2}_{\in S} = 0.$$

If $a \equiv 1 \pmod 6$ or $a \equiv 4 \pmod 6$ then $(a,1) = (1,1)$ because $(a \cdot 1 - 1 \cdot 1) \cdot 2 = 0$, $(a,1) = (2,1)$, $(a,2) = (1,1)$, $(a,6) = (2,1)$. Thus any given element of the ring equals some element in $\{(0,1),(1,1),(2,1)\}$ under $\sim$, and one can check none of these three elements are isomorphic to each other. Thus $R_f = \{(0,1),(1,1),(2,1)\}$. Since there is only one ring of order 3, we conclude $R \cong \mathbb{Z}/3\mathbb{Z}$. We conclude $(\mathbb{Z}/6\mathbb{Z})_2 \cong \mathbb{Z}/3\mathbb{Z}$.

Thus

$$\mathbb{Z}/6\mathbb{Z} \longrightarrow \frac{(\mathbb{Z}/6\mathbb{Z})[x]}{(2x-1)} \cong R_f \cong \mathbb{Z}/3\mathbb{Z}$$

is *not* injective, that is, the natural map $R \to S^{-1}R$ is not injective, where $S = \{1, 2, 2^2, 2^3 \ldots\}$. //

4.4 Universal Mapping Property of Localization

Proposition 4.36: Universal Mapping Property of the Localization.

If S is a multiplicatively closed subset of a commutative ring A and $\varphi\colon A \to B$ is a ring homomorphism such that $\varphi(S) \subset B^\times$, then there exists a unique ring homomorphism $\tilde{\varphi}\colon S^{-1}A \to B$ such that the diagram

$$\begin{tikzcd}
A \arrow[rr, "\varphi"] \arrow[dr, "j"'] & & B \\
& S^{-1}A \arrow[ur, "\tilde{\varphi}"'] &
\end{tikzcd}$$

commutes, where $j\colon A \to S^{-1}A$ is the natural map $a \mapsto a/1$.

The proof of Proposition 4.36 can be found here.

Example 4.37. Let A be a commutative ring, and suppose S and T are multiplicatively closed subsets of A such that $S \subset T$. Then since $j_{T,A}(S) \subset (T^{-1}A)^{\times}$, by Proposition 4.36 there exists a unique $\widetilde{j}\colon S^{-1}A \to T^{-1}A$ such that the diagram

$$\begin{tikzcd}
A \arrow[rr, "j_{T,A}"] \arrow[dr, "j_{S,A}"'] & & T^{-1}A \\
& S^{-1}A \arrow[ur, "\widetilde{j}"'] &
\end{tikzcd}$$

commutes. In fact, $\widetilde{j} = j_{\widetilde{T},S^{-1}A}$, where $\widetilde{T}$ is the image of T in $S^{-1}A$. (The details are left as an exercise.) //

Example 4.38. As a specific case of Example 4.37, let A be an integral domain, $T = A \smallsetminus \{0\}$, and S is any multiplicatively closed subsets of $A \smallsetminus \{0\}$, then we have canonical injections

$$\begin{tikzcd}
A \arrow[rr, hook] \arrow[dr, hook] & & T^{-1}A = \mathrm{Frac}(A) \\
& S^{-1}A \arrow[ur, hook] &
\end{tikzcd}$$

So, the localization is just some subring of the fraction field of A. (See the lemma about $\ker(j)$ above.) //

Example 4.39. Let $A = \mathbb{Z}$, so that $\mathrm{Frac}(A) = \mathbb{Q}$, and let $S = \mathbb{Z} \smallsetminus (p)$, where p is a prime integer. Then

$$S^{-1}A = \mathbb{Z}_{(p)} = \{x \in \mathbb{Q} \mid p \text{ is not a factor of the denominator of } x \text{ in lowest terms}\}.$$

Now consider $S_2 = \{2^n\}_{n=1}^{\infty}$. Then

$$S_2^{-1}\mathbb{Z} = \mathbb{Z}[1/p] = \{x \in \mathbb{Q} \mid p^n x \in \mathbb{Z} \text{ for some } n \in \mathbb{Z}_{\geqslant 0}\},$$

which reflects the fact from Example 4.38 that there exist canonical injections

$$\begin{tikzcd}
\mathbb{Z} \arrow[rr, hook] \arrow[dr, hook] & & \mathbb{Q} \\
& \mathbb{Z}[1/p] \arrow[ur, hook] &
\end{tikzcd}$$

//

4.5 Ideals in $S^{-1}A$

We next show that this construction does not add any new ideals, so ideals are collapsed together when we localize at some multiplicatively closed subset. First we introduce a useful piece of notation. (See also Exercise 8.2.)

Notation 4.40. Let A be a ring and S is a multiplicatively closed subset of A, then for any ideal $I \subset A$ we write $S^{-1}I$ for the ideal of $S^{-1}A$ generated by $j(I)$. #

Lemma 4.41.

If A is a commutative ring and S is a multiplicatively closed subset of A, then the assignment

$$\begin{aligned} \left\{\substack{\text{ideals}\\ \text{of } A}\right\} &\longrightarrow \left\{\substack{\text{ideals}\\ \text{of } S^{-1}A}\right\}, \\ I &\longmapsto S^{-1}I \end{aligned}$$

is surjective, and $S^{-1}I = S^{-1}A$ if and only if $I \cap S \neq \varnothing$. In other words, localization at S deletes any ideals intersecting S.

The proof of Lemma 4.41 can be found here.

The following is an important example, although it is somewhat of a "partial" example because we are restricting to prime ideals.

Proposition 4.42.

Let A be a commutative ring and let S be a multiplicatively closed subset of A. Then there is a bijective correspondence

$$\begin{aligned} \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \varnothing\} &\longleftrightarrow \operatorname{Spec}(S^{-1}A), \\ \mathfrak{p} &\longmapsto S^{-1}\mathfrak{p} \\ j^{-1}(\mathfrak{q}) &\longleftarrow\!\shortmid \mathfrak{q} \end{aligned}$$

is a bijection. In other words, localization at S deletes prime ideals intersecting S, and any prime ideal of $S^{-1}A$ are localizations of prime ideals.

The proof of Proposition 4.42 can be found here.

Proposition 4.42 is extremely important when thinking geometrically about the ring theory of a problem, and it turns out that the bijection of Proposition 4.42 is in fact a homeomorphism with respect to the Zariski topologies (when $\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \cap S = \varnothing\}$ is given the subspace topology on $\operatorname{Spec} A$). Indeed, this follows from Exercise 8.5.

Corollary 4.43.

If A is a commutative ring and $\mathfrak{p} \in \operatorname{Spec} A$, then

$$\begin{aligned} \operatorname{Spec}(A_{\mathfrak{p}}) &\xrightarrow{\cong} \{\mathfrak{q} \in \operatorname{Spec} A \mid \mathfrak{q} \subset \mathfrak{p}\} \\ S^{-1}\mathfrak{p} &\longleftarrow\!\shortmid \mathfrak{p} \\ \mathfrak{q} &\longmapsto j^{-1}(\mathfrak{q}). \end{aligned}$$

The proof of Corollary 4.43 can be found here.

Note 4.44. It follows that the ideal structure of $A_{\mathfrak{p}}$ is in bijection with the set of ideals *inside* $\mathfrak{p}$ (because anything outside $\mathfrak{p}$ becomes a unit when localizing at $\mathfrak{p}$, so any ideal not fully contained in $\mathfrak{p}$ collapses to the unit ideal). This is why this is called "localization," since we are literally throwing out all ideals except those inside $\mathfrak{p}$.

Note that, on the other hand, the prime ideals of $A/\mathfrak{p}$ are in bijection with the prime ideals of A *containing* $\mathfrak{P}$. //

Example 4.45. For prime integers p we have $\operatorname{Spec}\mathbb{Z}_{(p)} = \{(0), p\mathbb{Z}_{(p)}\}$, and as the notation suggests, this is just the example from a while ago, that is,

$$\mathbb{Z}_{(p)} = \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; a, b \in \mathbb{Z}, \gcd(a,b) = 1, p \nmid b \right\}. \qquad //$$

Example 4.46. In the case $A = \mathbb{C}[x]$, $\mathfrak{p} = (x)$, the localization of A at $\mathfrak{p}$ is the collection of prime ideals inside (x), that is,

$$\mathbb{C}[x]_{(x)} = \left\{ \frac{p(x)}{q(x)} \in \mathbb{C}(x) \;\middle|\; p(x), q(x) \in \mathbb{C}[x], \gcd(p(x), q(x)) = 1, x \nmid q(x) \right\},$$

and

$$\operatorname{Spec}(\mathbb{C}[x]_{(x)}) = \{(0), x\mathbb{C}[x]_{(x)}\}. \qquad //$$

Example 4.47. If $A = \mathbb{C}[x,y]$, $\mathfrak{p} = (x,y)$, then the localization of A at $\mathfrak{p}$ is

$$\mathbb{C}[x,y]_{(x,y)} = \left\{ \frac{f(x,y)}{g(x,y)} \in \mathbb{C}(x,y) \;\middle|\; f(x,y), g(x,y) \in \mathbb{C}[x,y] \text{ and } g(0,0) \neq 0 \right\}. \qquad //$$

(Note $g(x,y) \in \mathbb{C}[x,y]$ lies in (x,y) if and only if $g(0,0) = 0$.) Geometrically, then, $\mathbb{C}[x,y]_{(x,y)}$ is the collection of rational functions that are defined at 0. This also agrees with the general rule of thumb that geometrically the point (a,b) in the affine plane $\operatorname{Spec} k[x,y]$ is identified with the point (prime ideal) $(x-a, y-b)$ in $\operatorname{Spec} k[x,y]$. (In fact, this is already made rigorous over $\mathbb{C}$.)

Example 4.48. Let $R = \mathbb{C}[x,y]/(xy)$. What is R_x? On the other hand, what is $R_{(x)}$? Let us use all tools at our disposal to "guess" isomorphisms, with enough confidence that it is in fact an isomorphism, to the point that we would have no issue sitting down with a strong cup of coffee to prove it in full confidence. We first recall what those tools are:

- Let S be a multiplicatively closed subset of R. Then $\operatorname{Spec}(S^{-1}R)$ is in bijection with $\{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \cap S = \varnothing\}$.
- We can also use that R is a reduced ring (which can be seen by Exercise 9.5 since it is contained in a product of fields, which is reduced).
- Since R is reduced, if $\mathfrak{p}$ is a minimal prime then $R_{\mathfrak{p}}$ is a field by Exercise 9.4. bv (Check!).
- Moreover, if $S \subset T$ for another multiplicatively closed subset T of R, then by the universal mapping property of localization we get a well-defined ring homomorphism $S^{-1}R \to S^{-1}T$.
- We can also use that if $S = R \smallsetminus ((x) \cup (y))$ then $S^{-1}R \cong \mathbb{C}(x) \times \mathbb{C}(y)$. (This is Exercise 9.5)

With these points in mind, we can proceed as follows:

- *Computing* $\operatorname{Spec} R$: We first compute the spectrum of R. Recall that there is a bijection of $\operatorname{Spec} R$ onto $\{\mathfrak{p} \in \operatorname{Spec}\mathbb{C}[x,y] \mid \mathfrak{p} \supset (xy)\}$ given by sending $\mathfrak{p} \in \operatorname{Spec} R$ to its preimage

$\pi^{-1}(\mathfrak{p})$ under the quotient map $\pi\colon \mathbb{C}[x,y] \twoheadrightarrow \mathbb{C}[x,y]/(xy)$, and with inverse sending primes $\mathfrak{q} \in \operatorname{Spec}(\mathbb{C}[x,y])$ to $\pi(\mathfrak{q})$.

We can rewrite $\{\mathfrak{p} \in \operatorname{Spec}\mathbb{C}[x,y] \mid \mathfrak{p} \supset (x)\} \cup \{\mathfrak{p} \in \operatorname{Spec}\mathbb{C}[x,y] \mid \mathfrak{p} \supset (y)\}$. (This is not a *disjoint* union, since for example, the ideal (xy) is contained in both of these.) This is in bijection with

$$\begin{aligned}\operatorname{Spec}(\mathbb{C}[x,y]/(x)) \cup \operatorname{Spec}(\mathbb{C}[x,y]/(y)) &\cong \operatorname{Spec}\mathbb{C}[y] \cup \operatorname{Spec}\mathbb{C}[x]\\ &= (\{(0)\} \cup \{(y-a) \mid a \in \mathbb{C}\}) \cup (\{0\} \cup \{(x-a) \mid a \in \mathbb{C}\}).\end{aligned}$$

Now we have worked out all the ideals in the union, so we need to pull them back. Pulling back to $\mathbb{C}[x,y]$ via the aforementioned bijection, we get

$$(\{(x)\} \cup \{(x, y-a) \mid a \in \mathbb{C}\}) \cup (\{y\} \cup \{(x-a, y) \mid a \in \mathbb{C}\})$$

So the maximal ideals of $\mathbb{C}[x,y]/(xy)$ are the points on the coordinate axes of the xy-plane, and the coordinate axes themselves correspond to the (non-maximal) prime ideals (x) and (y).

- *Computing R_x*: It is straightforward to compute that $S = R \setminus (x, y-a)$ for $a \neq 0$. Given our knowledge of $\operatorname{Spec} R$ from the previous point and how the spectrum changes with localization, we can see that $\operatorname{Spec} R_x$ is the line with a point removed; indeed, in R_x the ideal (x) is no longer a prime, as x becomes a unit in R_x. (This is in contrast with the case of $\operatorname{Spec} R_{(x)}$, which is just the coordinate axes but "zoomed in" at an infinitesimal neighborhood of the y axis). Recall that when R is any commutative ring and $x \in R$ is not nilpotent, we have $R_x \cong \frac{R[t]}{tx-1}$ ="$R[1/x]$" (that is, in R_x we are defining t to be the multiplicative inverse of x, that is, $tx = 1$). Thus in our situation,

  $$R_x \cong \frac{\mathbb{C}[x,y,t]}{(xy, tx-1)}.$$

  Motivated by our intuition for how $\operatorname{Spec} R_x$ should look, we consider the localization $\mathbb{C}[x]_x$. Using the same logic as we did to obtain the above expression, we can also write

  $$\mathbb{C}[x]_x \cong \frac{\mathbb{C}[x,t]}{(tx-1)} \cong \frac{\mathbb{C}[x,y,t]}{(y, tx-1)}$$

  This hints to us that we should try to show $(xy, tx-1) = (y, tx-1)$. And indeed, $(xy, tx-1) \subset (y, tx-1)$ because $xy = y \cdot x$, and $(y, tx-1) \subset (xy, tx-1)$ because $y = -y(tx-1) + txy$. Thus points of R_x are points where you just delete the x axis

- *Computing $R_{(x)}$*: Where $R = \mathbb{C}[x,y]/(xy)$ again, what is $R_{(x)}$? By our geometric intuition we know this should be either $\mathbb{C}(x)$ or $\mathbb{C}(y)$, so we just need to determine which. This is left as an exercise. (Prove that the map $R_{(x)} = (\mathbb{C}[x,y]/(xy))_{(x)} \to \mathbb{C}(y)$ defined by

  $$\frac{f + (xy)}{g + (xy)} \longmapsto \frac{f(0,y)}{g(0,y)}$$

  is an isomorphism.) //

Example 4.49. When A is an integral domain and $\mathfrak{p} = 0$, $A_{(0)} = \operatorname{Frac} A$, and $\operatorname{Spec}(A_{(0)}) = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \subset (0)\} = \{(0)\}$. //

In these examples, we have been thinking of $A_{\mathfrak{p}}$ for an integral domain A as a subring of $\operatorname{Frac}(A)$. There is also a partial converse, which can be stated as follows.

Proposition 4.50.

If A is an integral domain, then inside $\operatorname{Frac}(A)$,

$$A = \bigcap_{\mathfrak{p}\in\operatorname{Spec} A} A_{\mathfrak{p}} = \bigcap_{\mathfrak{m}\in\operatorname{Max}(A)} A_{\mathfrak{m}}.$$

The proof of Proposition 4.50 can be found here.

Example 4.51. Inside $\mathbb{Q}$, $\mathbb{Z}_{(p)}$ is bigger than $\mathbb{Z}$, but if we start thinking about intersections over all prime ideals then we will cut out just the integers. In other words,

$$\mathbb{Z} = \bigcap_{\substack{\text{prime}\\ \text{integers } p}} \mathbb{Z}_{(p)} \quad (\text{inside } \mathbb{Q}).$$ //

4.6 Modules of Fractions

Definition 4.52.

Let A be a commutative ring, $S \subset A$ a multiplicatively closed subset, and M an A-module. Define

$$S^{-1}M \coloneqq (M \times S)/{\sim},$$

where $(m, s) \sim (n, t)$ if and only if there exists $u \in S$ such that

$$u(tm - sn) = 0.$$

We denote the equivalence class of the element $(m, s) \in M \times S$ with respect to $\sim$ by m/s, and define addition and multiplication operations on $S^{-1}M$ by

$$\frac{m}{s} + \frac{n}{t} \coloneqq \frac{tm + sn}{st}$$

and

$$\frac{a}{s} \cdot \frac{m}{t} \coloneqq \frac{am}{st},$$

respectively, for all $m, n \in M$, $s, t \in S$, $a \in A$.

Exercise 4.53.

The operations in Definition 4.52 make $S^{-1}M$ into an $S^{-1}A$-module. (See Exercise 9.1).

Theorem 4.54: Functoriality of Localization of Modules.

Let A be a commutative ring and S a multiplicative subset of A. For any A-modules M and N, and an A-module homomorphism $f\colon M \to N$, there exists a well-defined

$S^{-1}A$-module homomorphism $S^{-1}f\colon S^{-1}M \to S^{-1}N$ defined by

$$(S^{-1}f)\left(\frac{m}{s}\right) = \frac{f(m)}{s}.$$

satisfying the following properties.

- For any A-module homomorphisms $f\colon M \to N$ and $g\colon N \to P$,
$$S^{-1}(g \circ f) = S^{-1}g \circ S^{-1}f.$$
- If the sequence of A-module homomorpisms
$$M \xrightarrow{f} N \xrightarrow{g} P$$
is exact at N, then $S^{-1}M \xrightarrow{S^{-1}f} S^{-1}N \xrightarrow{S^{-1}g} S^{-1}P$ is exact at $S^{-1}N$.
- S^{-1} preserves addition of homomorphisms in the sense that S^{-1} induces a homomorphism on the hom-sets.
- In categorical terms, the above statements together are equivalent to saying S^{-1} is a covariant exact additive functor from the category of A-modules into the category of $S^{-1}A$-modules.

The proof of Theorem 4.54 can be found here.

Example 4.55. If N is an A-module and N is a submodule of N, then $S^{-1}M \subset S^{-1}N$ is an $S^{-1}A$ submodule, and quotient

$$\frac{S^{-1}N}{S^{-1}M} \cong S^{-1}(N/M).$$

This follows from applying Theorem 4.54 to the short exact sequence $0 \to M \to N \to N/M \to 0$. //

Example 4.56. Ideals of A are precisely the A-submodules of A, so as a particular case of Example 4.55 we conclude that all ideals of $S^{-1}A$ are of the form $S^{-1}I$ for ideals I of A, and

$$S^{-1}(A/I) \cong S^{-1}A/S^{-1}I.$$

Note that we have used the notation $S^{-1}I$ twice now. Both objects described are indeed the same, as will be shown in Exercise 9.2. There is a converse to Theorem 4.54 that we will soon prove, which allows us to go back and forth from local to global information. //

4.7 Annihilators and Support of Modules

Definition 4.57.

If A is a commutative ring, M is an A-module, and X is a subset of M, then we define the **annihliator** of X by

$$\operatorname{Ann}_A(X) \coloneqq \{a \in A \mid ax = 0 \text{ for all } x \in X\}.$$

Now fix a commutative ring A, a multiplicatively closed subset S of A, and a prime ideal $\mathfrak{p} \in \operatorname{Spec}(A)$.

Example 4.58. Recall that if $M \to N \to P$ is an exact sequence of modules, then so is $S^{-1}M \to S^{-1}N \to S^{-1}P$. Then in particular,

- $S^{-1}(M \times P) \cong S^{-1}M \times S^{-1}P$,
- $S^{-1}(N/M) \cong S^{-1}N/S^{-1}M$,
- if $M, P \subset N$ are submodules, then $S^{-1}(M + P) = S^{-1}M + S^{-1}P$, and $S^{-1}(M \cap P) = S^{-1}M \cap S^{-1}P$. //

The proof of Definition 4.57 can be found here.

Example 4.59. When $A = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$, we have

$$\operatorname{Ann}_A(M) = \{a \in \mathbb{Z} \mid am \equiv 0 \pmod{n} \text{ for all } m \in \mathbb{Z}/n\mathbb{Z}\} = n\mathbb{Z} = (n).$$

//

Example 4.60. Now fix a prime $p \in \mathbb{Z}$. Then $\mathbb{Z}_{(p)} = \left\{\frac{a}{b} \in \mathbb{Q}\right\}$. What is $(\mathbb{Z}/n\mathbb{Z})_{(p)}$? By definition,

$$(\mathbb{Z}/n\mathbb{Z})_{(p)} = S^{-1}(\mathbb{Z}/n\mathbb{Z}) = (\mathbb{Z} \smallsetminus (p))^{-1}(\mathbb{Z}/n\mathbb{Z}).$$

The answer will certainly depend on the relationship between p and n: if $p \nmid n$, then

$$(\mathbb{Z}/n\mathbb{Z})_{(p)} = \{(x, s) \mid x \in \mathbb{Z}/n\mathbb{Z}, s \in \mathbb{Z} \smallsetminus (p)\}.$$

And $x/s = x'/s'$ if and only if there exists $u \in \mathbb{Z} \smallsetminus (p)$ such that $u(xs' - x's) \equiv 0 \pmod{n}$. But such a u always exists, since we can just take $u = n$, which is in $S = \mathbb{Z} \smallsetminus (p)$ since $p \nmid n$. Thus any two elements are there equal, so $(\mathbb{Z}/n\mathbb{Z})_{(p)} = \{0\}$ if $p \nmid n$.

On the other hand, if $p \nmid n$, say $n = p^a n'$ where $p \nmid n'$, then by the CRT we can write

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_{n'}\mathbb{Z}$$

Since localization commutes with direct products,

$$(\mathbb{Z}/n\mathbb{Z})_{(p)} \cong (\mathbb{Z}/p^a\mathbb{Z})_{(p)} \times \cancelto{\{0\} \text{ by the previous case}}{(\mathbb{Z}/n'\mathbb{Z})_{(p)}}.$$

So it suffices to find $(\mathbb{Z}/p^a\mathbb{Z})_{(p)}$. Everything already invertible in $\mathbb{Z}/p^a\mathbb{Z}$ is invertible, since if something is not divisible by p then its inverse can be found as elements not divisible by p are made into units by the localization process.

Let us now make this intuition rigorous. We claim the map $\mathbb{Z}/p^a\mathbb{Z} \to (\mathbb{Z}/p^a\mathbb{Z})_{(p)}$ via $m \mapsto (m, 1)$ is an isomorphism.

Injective: If $(m, 1) \sim (m', 1)$ then there exists $u \in \mathbb{Z} \smallsetminus (p)$ such that $u(m - m') \equiv 0 \pmod{p}^a$. Since $p \nmid u$, there exists $t \in \mathbb{Z}$ such that $tu \equiv 1 \pmod{p}^a$, so $m - m' \equiv 0 \pmod{p}'$, so $m \equiv m' \pmod{p}'$.

Surjective: If $(m, s) \in (\mathbb{Z}/p^a\mathbb{Z})_{(p)}$, then $s \in \mathbb{Z} \smallsetminus (p)$, that is, s is coprime to p, so by elementary number theory there exists $t \in \mathbb{Z} \smallsetminus (p)$ such that $st \equiv 1 \pmod{p}^a$, so $(m, s) \sim (mt, 1)$, which is in the image because $(mts - m) \cdot 1 \equiv 0 \pmod{p}^a$. This gives the desired isomorphism. The upshot is that

$$(\mathbb{Z}/n\mathbb{Z})_{(p)} = \text{“}p\text{-part” of } \mathbb{Z}/n\mathbb{Z}.$$

Thus our map is an isomorphism. In conclusion,

$$(\mathbb{Z}/n\mathbb{Z})_{(p)} \cong \begin{cases} 0 & \text{if } p \nmid n, \\ \mathbb{Z}/p^a\mathbb{Z} & \text{if } n = p^a n' \text{ for some } a \geqslant 1, \text{ where } n' \nmid p. \end{cases} \qquad //$$

Proposition 4.61.

Let M be an A-module and let S be a multiplicatively closed subset of A, and let $j\colon M \to S^{-1}M$ be the natural map given by $j(m) = (m, 1)$. Then for all $m \in M$,

$$j(m) = 0 \qquad \Longleftrightarrow \qquad S \cap \operatorname{Ann}_A(m) \neq \varnothing.$$

The proof of Proposition 4.61 can be found here.

Definition 4.62.

Let M be an A-module. Define the **support** of M by

$$\operatorname{supp}(M) \coloneqq \{\mathfrak{p} \in \operatorname{Spec} A \mid M_{\mathfrak{p}} \neq 0\}.$$

Let M be an A-module, S a multiplicatively closed subset, and $j\colon M \to S^{-1}M$ the natural map. The **Support** of M is defined as

$$\operatorname{supp}(M) \coloneqq \{\mathfrak{p} \in \operatorname{Spec}(A) \mid M_{\mathfrak{p}} \neq 0\}.$$

Theorem 4.63.

The localization $S^{-1}M$ equals 0 if and only if for every $m \in M$, there exists $r \in S$ such that $r \cdot m = 0$ in M. Therefore, $S^{-1}M = 0$ if and only if for every $m \in M$, the set S intersects $\operatorname{Ann}_A(m)$ nontrivially.

Proof. Given any $m \in M$, if $S^{-1}M = 0$ then by definition there exists some $s \in S$ such that $s \cdot m = 0$ in M. Conversely, if for some $m \in M$, every $s \in S$ satisfies $s \cdot m \neq 0$, then $m/1 \neq 0$ in $S^{-1}M$, contradicting our assumption that $S^{-1}M = 0$. Hence, the statement holds. □

Corollary 4.64.

If $\mathfrak{p} \in \operatorname{Spec}(A)$ and $\mathfrak{p} \not\supset \operatorname{Ann}_A(M)$, then $M_{\mathfrak{p}} = 0$.

Proof. If $M_{\mathfrak{p}} \neq 0$ for some $\mathfrak{p} \in \operatorname{Spec}(A)$, then by definition, there is no $s \in A \smallsetminus \mathfrak{p}$ such that $sM = 0$. Conversely, if there exists $s \in A \smallsetminus \mathfrak{p}$ with $sM = 0$, then every element of M is annihilated by some element not in $\mathfrak{p}$, which implies that $M_{\mathfrak{p}}$ must be zero because s acts as a unit in $S^{-1}M$, annihilating M upon localization. □

Proposition 4.65.

Suppose M is finitely generated over A and $\mathfrak{p} \in \operatorname{Spec}(A)$. If $M_{\mathfrak{p}} = 0$, then $\mathfrak{p}$ contains $\operatorname{Ann}_A(M)$.

Proof. Let M be generated by elements $m_1, m_2, \ldots, m_n$. If $M_{\mathfrak{p}} = 0$, then for each i, there exists $s_i \in A \smallsetminus \mathfrak{p}$ such that $s_i m_i = 0$. Since $S = A \smallsetminus \mathfrak{p}$ is multiplicatively closed, the product $s = s_1 s_2 \cdots s_n$ is in S and annihilates each generator of M, hence annihilates M. Thus, $s \in \operatorname{Ann}_A(M)$ and $s \notin \mathfrak{p}$, which shows $\mathfrak{p}$ contains $\operatorname{Ann}_A(M)$. □

The above results then prove the following theorem:

Theorem 4.66.

if A is a commutative ring, S is a multiplicatively closed subset of A, and M is an A-module, then the following statements hold:

(i) $S^{-1}M = 0$ if and only if any $m \in M$ is annihilated by some $s \in S$.

(ii) If $\mathfrak{p} \in \operatorname{Spec}(A)$ and $M_{\mathfrak{p}} \neq 0$, then $\mathfrak{p}$ intersects $\operatorname{Ann}_A(M)$.

(iii) If M is finitely generated over A, then $\operatorname{supp}(M)$ equals the set of all prime ideals $\mathfrak{p}$ of A that contain $\operatorname{Ann}_A(M)$.

In other words, the finitely generated module over the ring A, referred to as a "function" when viewed geometrically on the affine space over A, exhibits a support set. This support set consists of the closed set of points where the module M equals zero.

For example, let's consider the module $k[x]/(f(x))$ when the ring A is K. This module is finitely generated over A because it can be generated by the set $\{1, x, x^2, \ldots, x^{n-1}\}$, where n represents the degree of the polynomial f. We interpret the module M (i.e., $k[x]/(f(x))$) as a "function" defined on a one-dimensional affine space $K[x]$. This function is defined at points, which in this context correspond to elements or prime ideals of the spectrum of $A[x]$, denoted as the spectrum of $A[x]$ or equivalently $k[x]$. The "value" of the module M at a point $\mathfrak{p}$ in the spectrum of $A[x]$ is denoted as $M_{\mathfrak{p}}$. Consequently, the support of M, denoted as $\operatorname{supp} M$, aligns with the conventional notion of support in a topological space when M is finitely generated As a result, we can establish the third point mentioned earlier, which states that the support of M is equal to $V(\operatorname{Ann}_A(M))$, where $\operatorname{Ann}_A(M)$ represents the annihilator of M. It is worth noting that this set $\operatorname{supp} M$ is closed in the spectrum of A and thus coincides with its own closure. Furthermore, $V(\operatorname{Ann}_A(M))$ is the set of points in the spectrum of A such that if a point $\mathfrak{p}$ contains the annihilator $\operatorname{Ann} A$, then the value $M_{\mathfrak{p}}$ of the "function" M at the point $\mathfrak{p}$ is equal to zero. This confirms that the support of M indeed corresponds to the support in the traditional mathematical sense of a function defined on a topological space.

As an illustrative example, if the polynomial $f(x) = x - \alpha$, resulting in the module $M = k[x]/(x - \alpha)$ over the ring K, then the support of M is equal to $V(\operatorname{Ann}_A(x)) = V((\alpha)) = \operatorname{Spec}(k[x])$. This implies that $M_{\mathfrak{p}}$ is never equal to zero. Conversely, since $M_{\mathfrak{p}} = 0$ if and only if $\mathfrak{p} = (0) \not\supset \operatorname{Ann}_A(k) = 0$, but it does.

Exercise 4.67.

In the context of the function language described, what is the meaning of $k[x]$-modules (algebras) M, N, P making a sequence $0 \to M \to N \to P \to 0$ exact?

Example 4.68. $\operatorname{supp}(\mathbb{Z}/n\mathbb{Z}) = \{(p) \mid p \text{ divides } n\}$. //

Example 4.69. Consider $A = \mathbb{C}[x, y]$ and $M = \mathbb{C}$. Fix $a, b \in \mathbb{C}$. If $f \in A$ and $x \in \mathbb{C}$, define

$$f \cdot x \coloneqq f(a, b)x.$$

One can check this gives M a module structure on A. What is the support of M?

Let us start with a more simple question: if x is a nonzero complex number (if $x = 0$ then obviously $\operatorname{Ann} x$ is everything),

$$\begin{aligned}\operatorname{Ann}_A(x) &= \{f \in \mathbb{C}[x, y] \mid f(a, b)x = 0\} \\ &= \{f \in \mathbb{C}[x, y] \mid f(a, b) = 0\} && \text{(since } x \neq 0) \\ &= (x - a, y - b).\end{aligned}$$

Now let $\mathfrak{p} \in \operatorname{Spec} \mathbb{C}[x, y]$ and let $j\colon \mathbb{C} = M \to \mathbb{C}_{\mathfrak{p}} = M_{\mathfrak{p}}$ be the natural map. Then for all $x \in \mathbb{C}$,

$$\begin{aligned}j(x) \neq 0 &\iff S \cap \operatorname{Ann}(x) = \varnothing \\ &\iff \mathbb{C}[x, y] \smallsetminus \mathfrak{p} \cap (x - a, y - b) = \varnothing \\ &\iff \mathfrak{p} \supset (x - a, y - b) \\ &\iff \mathfrak{p} = (x - a, y - b).\end{aligned}$$

Hence j is the zero map, unless, $\mathfrak{p} = (x - a, y - b)$, in which case j is an isomorphism. We conclude $\operatorname{supp}(M) = \{(x - a, y - b)\}$. //

Example 4.70. Let $A = \mathbb{C}[x, y]$, $f(x, y) = y - x^2$, and $M = \mathbb{C}[x]$. Then M is an A-module, $A \to M$ because $\mathbb{C}[x, y]/(y - x^2) \xrightarrow{\cong} \mathbb{C}[x]$ via $f \mapsto f(x, x^2)$ is an isomorphism. For each $f \in A$ and $\alpha \in M$, define $f \cdot \alpha \coloneqq f(x, x^2)\alpha$. What is $\operatorname{Ann}(M)$? Write

$$\begin{aligned}\operatorname{Ann}(M) &= \{f \in \mathbb{C}[x, y] \mid f(x, x^2)\alpha = 0 \text{ for all } \alpha \in M\} \\ &= \{f \in \mathbb{C}[x, y] \mid f(x, x^2) = 0\} = (y - x^2).\end{aligned}$$

So what is $\operatorname{supp}(M)$? Well, if $\mathfrak{p} \subset \mathbb{C}[x, y]$ is prime, then $j\colon \mathbb{C}[x] \to \mathbb{C}[x]_{\mathfrak{p}}$ has

$$\begin{aligned}j(x) \neq 0 &\iff S \cap \operatorname{Ann}(x) = \varnothing \\ &\implies S \cap \operatorname{Ann}(M) = \varnothing \\ &\iff \mathbb{C}[x, y] \smallsetminus \mathfrak{p} \cap (y - x^2) = \varnothing \\ &\iff \mathfrak{p} \supset (y - x^2).\end{aligned}$$

So, at the very least, we have $\operatorname{supp}(M) \subset \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \supset (y - x^2)\}$. In fact, one can show this is an equality, and geometrically this makes sense. In other words, $\operatorname{supp}(M)$ “equals” the points on which the polynomial $y - x^2$ vanishes. This is another example for which the concept of the support of a module tells us a lot about the structure of the module. //

Exercise 4.71.

Let A be a commutative ring and let M be an A-module.

(a) Let S be a multiplicatively closed subset of A. Show that if $S \cap \operatorname{Ann}_A(M) = \varnothing$, then $S^{-1}M = 0$. In other words, if some element of $\operatorname{Ann}_A(M)$ lives inside S, then the localization at S is zero.

(b) Moreover, if $\mathfrak{p} \in \operatorname{Spec} A$ and $\mathfrak{p} \not\supset \operatorname{Ann}_A(M)$, then $M_{\mathfrak{p}} = 0$.

(c) If M is finitely generated, then

$$M_{\mathfrak{p}} = 0 \iff \mathfrak{p} \not\supset \operatorname{Ann}_A(M),$$

that is, $\mathfrak{p} \in \operatorname{supp} M$ if and only if $\mathfrak{p} \in V(\operatorname{Ann}_A(M))$.

Proof. For (c), see Exercise F3. Points (i) and (ii) are left as exercises. □

Note 4.72. We used in disguise the result of Exercise 4.71(a) when saying that if p does not divide n, then that is just saying $n \in S$, and n is also in $\operatorname{Ann}(\mathbb{Z}/n\mathbb{Z})$, so $S^{-1}(\mathbb{Z}/n\mathbb{Z}) = 0$. //

Example 4.73.

- If M is a submodule of an A-module N, then $S^{-1}M$ is a submodule of the $S^{-1}A$-submodule $S^{-1}N$, and $S^{-1}(N/M) \cong S^{-1}N/S^{-1}M$.
- In particular, for any ideal I of A, $S^{-1}(A/I) \xleftarrow{\cong} S^{-1}N/S^{-1}M$.
- If M_1, M_2 are submodules of an A-module M, then $S^{-1}(M_1 + M_2) = S^{-1}(M_1) + S^{-1}M_2$ is a submodule of the $S^{-1}A$-module $S^{-1}M$. (This can be checked directly, or one can use $M_1 \oplus M_2 \to \underbrace{M_1 + M_2}_{\subset M} \to 0$.) //

4.8 Detecting Exactness with Localization at Prime Ideals

Lemma 4.74.

If Q is an A-module, then

$$Q = 0 \qquad \iff \qquad Q_{\mathfrak{m}} = 0 \text{ for all } \mathfrak{m} \in \operatorname{Max}(A).$$

The proof of Lemma 4.74 can be found here.

Theorem 4.75.

If $M \xrightarrow{f} N \xrightarrow{g} P$ is a sequence of A-modules, then the following are equivalent:

(1) $M \xrightarrow{f} N \xrightarrow{g} P$ is exact.

(2) $M_{\mathfrak{p}} \xrightarrow{f_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{g_{\mathfrak{p}}} P_{\mathfrak{p}}$ is exact for all prime ideals $\mathfrak{p}$ of A.

(3) $M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}} \xrightarrow{g_{\mathfrak{m}}} P_{\mathfrak{m}}$ is exact for all maximal ideals $\mathfrak{m}$ of A.

The proof of Theorem 4.75 can be found here.

4.9 Homework 9

Exercise 4.76: 9.1.

Let A be a commutative ring, and let S be a multiplicatively closed subset of A. Let M be an A-module. Define the **module of fractions** $S^{-1}M$ by

$$S^{-1}M = (M \times S)/\sim$$

where $(m, s) \sim (n, t)$ if and only if there exists some $u \in S$ such that $u(tm - sn) = 0$ (in M). As usual, we abbreviate $(m, s) = m/s$.

(a) Show that $\sim$ is an equivalence relation.

(b) Show that $S^{-1}M$ is an $S^{-1}A$-module with operations

$$\frac{m}{s} + \frac{n}{t} = \frac{tm + sn}{st} \qquad \text{and} \qquad \frac{a}{s} \cdot \frac{m}{t} = \frac{am}{st}$$

for all $m, n \in M, a \in A, s, t \in S$.

A solution to Exercise 4.76 can be found here.

Exercise 4.77: 9.2.

Continue with the setting of Exercise 9.1. When $M = I$ is an ideal of A, we have already defined the ideal $S^{-1}I$ of $S^{-1}A$ to be the ideal generated by $j(I)$, for $j\colon A \to S^{-1}A$ the canonical homomorphism. Show that this ideal can be canonically identified with the module of fractions $S^{-1}I$ defined in Exercise 9.1 (so our potentially ambiguous notation is in fact consistent).

A solution to Exercise 4.77 can be found here.

Exercise 4.78: 9.3.

Let A be a commutative ring, and let $\mathfrak{p}$ be a prime ideal of A. What is the relationship between $A/\mathfrak{p}$ and $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$? Hint: You may need to compute a couple of examples to find the answer. See Example 4.46 for a good example.

Theorem 4.79.

Let A be a commutative ring and let $\mathfrak{p} \in \operatorname{Spec} A$. Then there exists an isomorphism of rings

$$\overline{\varphi}\colon A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}} \xrightarrow{\cong} \operatorname{Frac}(A/\mathfrak{p})$$

induced by the surjective ring homomorphism

$$\varphi\colon A_{\mathfrak{p}} \longrightarrow \operatorname{Frac}(A/\mathfrak{p}),$$
$$\frac{f}{s} \longmapsto \frac{(f+\mathfrak{p})}{(s+\mathfrak{p})} =: \frac{\overline{f}}{\overline{s}}.$$

Proof.

- *φ is well-defined:* Suppose $f/s = g/t$ in $A_{\mathfrak{p}}$. Then there exists $u \in A \smallsetminus \mathfrak{p}$ such that $u(tf - sg) = 0$ (in A). Since $u \notin \mathfrak{p}$, $\overline{u}$ is nonzero in $A/\mathfrak{p}$, and
$$\overline{u}(\overline{t}\overline{f} - \overline{s}\overline{g}) = \overline{u(tf-sg)} = \overline{0} \text{ in } A/\mathfrak{p}.$$
Hence $\varphi(f/s) = \overline{f}/\overline{s} = \overline{g}/\overline{t} = \varphi(g/t)$, so φ is well-defined.
- *φ is a ring homomorphism:* Let $f/s, g/t \in A_{\mathfrak{p}}$. Then
  - $\varphi(1/1) = \overline{1}/\overline{1} = 1/1$,
  - $\varphi\big(\frac{f}{s} \cdot \frac{g}{t}\big) = \varphi\big(\frac{fg}{st}\big) = \frac{\overline{fg}}{\overline{st}} = \frac{\overline{f}}{\overline{s}} \cdot \frac{\overline{g}}{\overline{t}} = \varphi\big(\frac{f}{s}\big) \cdot \varphi\big(\frac{g}{t}\big)$, and
  - $\varphi\big(\frac{f}{s} + \frac{g}{t}\big) = \varphi\big(\frac{tf+sg}{st}\big) = \frac{\overline{ft+sg}}{\overline{st}} = \frac{\overline{t}\overline{f}}{\overline{s}\overline{t}} + \frac{\overline{s}\overline{g}}{\overline{s}\overline{t}} = \frac{\overline{f}}{\overline{s}} + \frac{\overline{g}}{\overline{t}} = \frac{\overline{f}}{\overline{s}} + \frac{\overline{g}}{\overline{t}} = \varphi\big(\frac{f}{s}\big) + \varphi\big(\frac{g}{t}\big)$,

  so φ is a ring homomorphism.
- *φ is surjective:* Any given element of $\operatorname{Frac}(A/\mathfrak{p})$ is of the form $\overline{f}/\overline{t} \in \operatorname{Frac}(A/\mathfrak{p})$ for some $f, t \in A$ such that $\overline{t} \neq 0$ in $A/\mathfrak{p}$. It follows that $t \notin \mathfrak{p}$, so f/t is an element of $A_{\mathfrak{p}}$. Then $\varphi(f/t) = \overline{f}/\overline{t}$. Thus φ is surjective.
- $\mathfrak{p}A_{\mathfrak{p}} \subset \ker\varphi$: Any element of $\mathfrak{p}A_{\mathfrak{p}}$ is of the form pf/s for some $p, f, s \in A$ such that $p \in \mathfrak{p}$ and $s \in A \smallsetminus \mathfrak{p}$, and $\varphi(pf/s) = \overline{pf}/\overline{s} = \overline{0}\overline{f}/\overline{s} = \overline{0}$. Thus $\mathfrak{p}A_{\mathfrak{p}} \subset \ker\varphi$.
- $\ker\varphi \subset \mathfrak{p}A_{\mathfrak{p}}$: Suppose $f/g \in A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is in the kernel of φ. Then $\overline{f}/\overline{s} = \overline{0}/\overline{1}$ in $\operatorname{Frac}(A/\mathfrak{p})$, so there exists some $\overline{u} \neq 0$ in $A \smallsetminus \mathfrak{p}$ such that
$$\mathfrak{p} = \overline{0} = \overline{u}(\overline{1} \cdot \overline{f} - \overline{s} \cdot \overline{0}) = \overline{u} \cdot \overline{f} = \overline{uf} = uf + \mathfrak{p} \text{ in } A/\mathfrak{p}.$$
Thus $uf \in \mathfrak{p}$. Since $u \notin \mathfrak{p}$ and $\mathfrak{p}$ is prime, we must have $f \in \mathfrak{p}$. Then because $1/s \in A_{\mathfrak{p}}$, we conclude $f/s \in \mathfrak{p}A_{\mathfrak{p}}$. Thus $\ker\varphi \subset \mathfrak{p}A_{\mathfrak{p}}$. □

Exercise 4.80: 9.4.

Let A be a commutative ring, and let $\mathfrak{p}$ be a **minimal prime ideal** of A, that is, there are no prime ideals strictly contained in $\mathfrak{p}$.

(a) Show that all elements of the (maximal) ideal $\mathfrak{p}A_{\mathfrak{p}}$ of $A_{\mathfrak{p}}$ are nilpotent. If A is moreover reduced, show that $A_{\mathfrak{p}}$ is a field.

(b) Deduce that if A is reduced, there is an injective ring homomorphism
$$A \longrightarrow \prod_{\substack{\text{minimal} \\ \mathfrak{p} \in \operatorname{Spec} A}} A_{\mathfrak{p}}.$$

A solution to Exercise 4.80 can be found here.

Exercise 4.81: 9.5.

Show that there exists an isomorphism of rings
$$\operatorname{Frac}(\mathbb{C}[x,y]/(xy)) \cong \mathbb{C}(x) \times \mathbb{C}(y).$$

A solution to Exercise 4.81 can be found here.

5 Finiteness Conditions on Rings and Modules

5.1 Noetherian Modules

In this section we continue the convention that all rings are commutative unless stated otherwise.

Definition 5.1.

Let A be a ring and let M be an A-module. We say M is **Noetherian** (as an A-module) if every ascending chain of A-submodules

$$M_0 \subset M_1 \subset M_2 \subset \cdots$$

stabilizes, that is, if there exists $r > 0$ such that $M_r = M_{r+s}$ for all $s \geqslant 0$. This condition is known as the **ascending chain condition (ACC)** on submodules.

Example 5.2. A ring A is called **Noetherian** if A is a Noetherian module over itself with respect to the natural module structure. Since A submodules of A are ideals of A, this means every ascending chain of ideals

$$I_0 \subset I_1 \subset I_2 \subset \cdots$$

stabilizes. //

Example 5.3.

- $\mathbb{Z}$ is a Noetherian ring. Any field is a Noetherian ring.
- If A is Noetherian and $\pi\colon A \twoheadrightarrow B$ is a surjective ring homomorphism, then B is Noetherian. Indeed, for any chain $I_0 \subset I_1 \subset \cdots \subset B$, $\pi^{-1}(I_0) \subset \pi^{-1}(I_1) \subset \cdots \subset A$ stabilizes, and for all j we have $\pi(\pi^{-1}(I_j)) = I_j$ since π is surjective, so $I_0 \subset I_1 \cdots$ stabilizes.
- If A is Noetherian, then $A[x]$ is Noetherian. This result, which we will soon prove, is called **Hilbert's basis theorem** (Theorem 5.24).
- If A is Noetherian, then $S^{-1}A$ is Noetherian for all multiplicatively closed subsets S of A. Indeed, we have seen that every ideal J of $S^{-1}A$ is of the form $S^{-1}(j^{-1}I)$ for some ideal I of A, where $j\colon S \to S^{-1}A$ is the natural map. For any chain $J_0 \subset J_1, \cdots \subset S^{-1}A$, the chain $j^{-1}J_0 \subset j^{-1}J_1 \subset \cdots$ in A stabilizes, so the original chain must stabilize in $S^{-1}A$. //

Proposition 5.4.

Let A be a ring and let M be an A-module. Then the following are equivalent:

(1) M is a Noetherian A-module.

(2) Every nonempty subset Σ of submodules of M has a maximal element (with respect to inclusion).

(3) Every submodule of M is finitely generated as an A-module.

The proof of Proposition 5.4 can be found here.

Corollary 5.5.

A ring A is Noetherian if and only if every ideal I of A is finitely generated.

Lemma 5.6.

Let A be a ring. Then in a short exact sequence $0 \to M_1 \xrightarrow{i} M \xrightarrow{\pi} M_2 \to 0$ of A-modules,

$$M \text{ is Noetherian} \iff M_1 \text{ and } M_2 \text{ are Noetherian.}$$

The proof of Lemma 5.6 can be found here.

Warning 5.7. A subring of Noetherian rings need not be a Noetherian ring. For example, consider the subring $A = \mathbb{C}[x_1, x_2, x_3, \dots]$ of the ring $B = \text{Frac}(A)$. Then A is not Noetherian because $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$ gives an ascending chain of ideals that does not stabilize, whereas B is a field and hence Noetherian. In fact, the situation is even more complicated, since $\text{Frac}(\mathbb{C}[x_1, x_2, x_3, \dots]) = \mathbb{C}(x_1, \dots, x_n)$ is a field, and hence is Noetherian, so we have a tower of rings

$$\mathbb{C} \subset \mathbb{C}[x_1, x_2, x_3, \dots] \subset \mathbb{C}(x_1, x_2, x_3, \dots)$$

where a non-Noetherian ring is an intermediate ring of two Noetherian rings.

Although all Noetherian modules are finitely generated by the previous proposition, it is not true in general that finitely generated modules are Noetherian. However, the following result shows that if A is a Noetherian *ring*, then finitely generated A-modules are precisely Noetherian A-modules:

Proposition 5.8.

Let A be a Noetherian ring and let M be an A-module. Then the following are equivalent:

(1) M is a Noetherian A-module.

(2) M is a finitely generated A-module.

The proof of Proposition 5.8 can be found here.

5.2 Noetherian Rings

Recall that if V is a finite-dimensional vector space and W is a subspace of V then W is also finite-dimensional. Unfortunately, this nice fact completely breaks down in the setting of modules, and this failure is demonstrated by the following example.

Example 5.9. Let $R = \mathbb{C}[x_1, x_2, x_3, \dots]$ and consider R as a module over itself. Then M is finitely generated, namely by the element 1, but the submodule $I \subset M = (x_1, x_2, x_3, \dots,)$ is *not* finitely generated. //

Definition 5.10.

Let R be a ring and let M be an R-module. Then M is Noetherian if every R-submodule is finitely generated. We say R is a **Noetherian ring** if every ideal is finitely generated.

The above definition is not very useful though, since it does not give us much of a way to show a ring is Noetherian. However, an equivalent definition that *can* be used to identify rings with this property is the following:

Example 5.11. $\mathbb{Z}$ is a PID, so every ideal is generated by a single element, and in particular by finitely many elements. Thus $\mathbb{Z}$ is Noetherian.

Alternatively, we could use the ACC to show $\mathbb{Z}$ is Noetherian: we can write any ascending chain of ideals of $\mathbb{Z}$ as

$$(n_0) \subset (n_1) \subset (n_2) \subset, \cdots$$

which is the same thing as saying n_0 is divisible by n_1, and n_1 is divided by n_2, and n_2 is divided by n_3 //

Warning 5.12. A theorem of Motzkin from the 1940s is that there exist PIDs that are not Euclidean domains (for instance, $\mathbb{Z}[(1+\sqrt{-19})/2]$). However, since Euclidean domains are PIDs, they too are Noetherian by Example 5.11. ☡

Example 5.13. $\mathbb{Z}[x]$ is Noetherian, and more generally by Hilbert's basis theorem (Theorem 5.24 below), which states that if R is Noetherian then so is $R[x]$. //

Example 5.14. $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ is Noetherian: We can write $\mathbb{Z}[\sqrt{-5}] \cong \mathbb{Z}[x]/(x^2+5)$, which is a quotient of the Noetherian ring $\mathbb{Z}[x]$, and hence is Noetherian.

Alternatively, we can say that if I is any ideal of $\mathbb{Z}[\sqrt{-5}]$ and $a \in I$, then $(a) \subset I$, and one can show $\mathbb{Z}[\sqrt{-5}]/(a)$ is finite. Then in particular it has only finitely many ideals (namely because any ideal is in the power set and the power set of a finite set is finite). (Although $\mathbb{Z}[\sqrt{-5}]/(a)$ is finite, it is of course not true in general that if R is Noetherian and $a \in R$ then $R/(a)$ is finite.) //

Example 5.15. Consider the ring $C[0,1] = \{f \colon [0,1] \to \mathbb{R} \mid f \text{ is continuous}\}$. We claim $C[0,1]$ is *not* Noetherian. To show this, we can find an ascending chain that never stabilizes.

Note that f is a unit in $C[0,1]$ if and only if f is nowhere vanishing. Since any proper ideal cannot contain units, we know any element of a proper ideal I vanishes somewhere. To that end, consider the infinite subset $\{1/2^n \mid n \in \mathbb{Z}_{\geqslant 1}\}$ of $[0,1]$, and define

$$I_n \coloneqq \{f \in C[0,1] \mid f(1/2^m) = 0 \text{ for all } m \geqslant n\}.$$

Then $I_0 \subset I_1 \subset I_2 \subset \cdots$, is an infinite chain. But each containment is proper, since it is straightforward to construct a function in I_k but not in I_{k+1}. //

Example 5.16. To show $\mathbb{Q}[x]$ is Noetherian, we can either use Exercise 8.1 that $\mathbb{Q}[x]$ is a PID (and hence has finitely generated ideals) or use Hilbert's basis theorem.

Now consider the set

$$R = \{f \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\}.$$

Then R is a ring, since $0, 1 \in R$ and if $f(0), g(0)$ is an integer, then so is $(f+g)(0)$ and $(fg)(0)$. Now consider the subset $I = \{f \in R \mid f(0) = 0\}$. Then I is an ideal of R. It is not ideal, since if $x \in I$ then $(x) \subset I$ but $(x) \subsetneq (x/2) \subsetneq (x/4) \subsetneq (x/8) \subsetneq \cdots$, so I is not finitely generated. Thus R is not Noetherian. //

Example 5.17. Let $R = \mathbb{Z}[\sqrt[n]{2}]$ for some $n \in \mathbb{Z}_{\geqslant 1}$. Then R is Noetherian, since it is a quotient of the Noetherian ring $\mathbb{Z}[x]$, namely $R \cong \mathbb{Z}[x]/(x^n - 2)$. //

Example 5.18. Now consider the ring $R = \mathbb{Z}[\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \sqrt[5]{2}, \ldots]$. Then $(2) \subsetneq (\sqrt{2})$ is a *proper* containment, since if $\sqrt{2} = 2a$ for some $a \in R$ then $a = \sqrt{2}/2$, which is not an element of R. Continuing this chain, we get an ascending chain of proper ideals of the form

$$(2) \subsetneq (\sqrt{2}) \subsetneq (\sqrt[4]{2}) \subsetneq (\sqrt[8]{2}) \subsetneq \cdots$$

is an ascending chain of ideals of proper ideals in R that does not stabilize. Hence R is not a Noetherian ring. //

5.3 Factorization in Noetherian Integral Domains

We now exhibit another nice property of Noetherian rings.

Definition 5.19.

Let R be any (possibly noncommutative) ring, let $a \in R$ be nonzero and suppose $a \notin R^\times$. We say a is **irreducible** if whenever $a = bc$ for some $b, c \in R$, then either $a \in R^\times$ or $b \in R^\times$. We call a **reducible** if a is not irreducible.

Recall the proof of the fundamental theorem of arithmetic, that is, that any $n \in \mathbb{Z}$ can be factored into a product of prime integers (up to a unit, that is, up to a multiple of ± 1): If n is prime then we are done, so suppose n is not prime. Then $n = n_1 a_1$ for some integers $a_1, n_1 \neq \pm 1$. Then do the same for n_2, and repeat this process until we get a product of primes, which we must do in finitely many steps since n_j strictly decreases after every step.

We will now work to generalize this argument for Noetherian rings.

Definition 5.20.

An **atomic domain** (or **factorization domain**) is an integral domain A in which every nonzero non-unit $a \in A$ can be written in at least one way as a finite product of irreducible elements, up to a unit. Any such expression of a is called a **factorization** of a, and we say a **factors**.

Proposition 5.21: Factorization into Irreducible Elements in Noetherian Domains.

Let R be a commutative Noetherian integral domain. Then if $x \in R$ is nonzero and $x \notin R^\times$, then x can be written as a product of irreducible elements of R.

The proof of Proposition 5.21 can be found here.

Another slightly different way to reformulate Proposition 5.21 this is the following.

Theorem 5.22.

If R is a Noetherian integral domain and $x \in R$ is nonzero, then there exist $u \in R^\times$ and irreducible elements $x_1, \dots, x_n \in R$ such that $x = ux_1 \cdots x_n$.

Warning 5.23. The converse to Theorem 5.22 is *false* (consider $\mathbb{Z}/6\mathbb{Z}$).

5.4 Hilbert's Basis Theorem

Theorem 5.24: Hilbert's Basis Theorem.

Let A be a Noetherian ring. Then $A[x]$ is a Noetherian ring.

The proof of Theorem 5.24 can be found here.

Recall that an A-algebra is a ring B equipped with a ring homomorphism $\varphi\colon A \to B$. We call B a finitely generated A-algebra if there exist $b_1, \dots, b_n \in B$ such that $B = \varphi(A)[b_1, \dots, b_n]$. In this situation, we get a surjective ring homomorphism (the top arrow) such that the diagram

$$\begin{tikzcd}
A[x_1, \dots, x_n] \arrow[rr, two heads, "x_i \mapsto b_i"] & & B \\
& A \arrow[ul] \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

commutes. Any A-algebra is an A-module, since if we have a ring isomorphism from A to B then B is an A-module with multiplication by the map $\varphi : A \to B$ (from the definition of B being an A-algebra) and defining the ring action on B to make B an A-module by $a \cdot b \coloneqq \varphi(a)b$.

Corollary 5.25.

If A is Noetherian, then any finitely generated A-algebra is Noetherian as an A-module.

The proof of Corollary 5.25 can be found here.

Note 5.26. Just as in Corollary 5.25, one could theoretically run the above proof on an infinite collection of, say, polynomials in $\mathbb{Z}[x]$, to iteratively obtain a finite collection of generators. //

5.5 Homework 10

Exercise 5.27: 10.1.

Let I and J be ideals of a commutative ring A.

(a) Show that

$$\sqrt{I+J} = \sqrt{\sqrt{I}+\sqrt{J}}$$

(b) Deduce that if $\sqrt{I}+\sqrt{J} = A$, then $I+J = A$.

(c) Show that for any prime ideal $\mathfrak{p}$ of A, $\sqrt{\mathfrak{p}^n} = \mathfrak{p}$ for all $n \in \mathbb{Z}_{\geqslant 1}$, and thus by part (b), for any distinct maximal ideal $\mathfrak{m}_1$ and $\mathfrak{m}_2$ of A, $\mathfrak{m}_1^k$, and $\mathfrak{m}_2^\ell$ are coprime for any $k, \ell \geqslant 1$.

A solution to Exercise 5.27 can be found here.

Exercise 5.28: 10.2.

(a) Show that in a commutative Noetherian ring A, every ideal contains some power of its radical.

(b) We say an ideal I of a commutative ring A is **nilpotent** if $I^n = 0$ for some $n \in \mathbb{Z}_{\geqslant 1}$. Prove that in a commutative Noetherian ring A, the nilradical $\sqrt{0}$ is nilpotent.

(c) Give an example of a non-Noetherian commutative ring whose nilradical is not nilpotent.

A solution to Exercise 5.28 can be found here.

Exercise 5.29: 10.3: Nakayama's Lemma.

Let A be a commutative ring with Jacobson radical $J(A)$, and let M be a finitely generated A-module. Show that if $J(A)M = M$, then $M = 0$.[a] Hint: if $M \neq 0$, choose a set of generators $m_1, \ldots, m_n$ of M with minimal size; contemplate the fact that m_n lies in $J(A)M$.

[a] For an ideal I of A, we write IM for the submodule of M generated by the subset $\{xm \mid x \in I, m \in M\}$.

A solution to Exercise 5.29 can be found here.

Exercise 5.30: 10.4.

Let A be a commutative Noetherian local ring with maximal ideal $\mathfrak{m}$. Use Nakayama's lemma (Exercise 10.3) to show that exactly one of the following two statements is true for all $n \in \mathbb{Z}_{\geqslant 1}$:

(a) $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$.

(b) $\mathfrak{m}^n = 0$.

Note that this shows that a local ring A is Artinian (defined in Definition 6.1) if and only if the chain $\mathfrak{m} \supset \mathfrak{m}^2 \supset \mathfrak{m}^3 \supset \cdots$ stabilizes.

A solution to Exercise 5.30 can be found here.

Exercise 5.31: 10.5.

Let A be a commutative ring, and let M be a Noetherian A-module. Let $f\colon M \to M$ be a surjective A-module homomorphism. Show that f is an isomorphism. Hint: Consider the chain of submodules $\{\ker(f^{\circ n})\}_{n \in \mathbb{Z}_{\geqslant 1}}$, where $f^{\circ n}$ is $f \circ f \circ \cdots \circ f$ is he n-fold composition of f with itself (for example, $f^{\circ 2} = f \circ f$).

A solution to Exercise 5.31 can be found here.

Note that there is a version of Exercise 10.5 for Artinian rings.

Lemma 5.32.

Let $f\colon M \to M$ be an injective module homomorphism where M is a module over an Artinian ring. Then f is an isomorphism.

Proof. Since f is injective and M is Artinian, any descending chain of submodules of M stabilizes. Therefore, for the chain

$$\mathrm{im}(f) \supset \mathrm{im}(f \circ f) \supset \mathrm{im}(f \circ f \circ f) \supset \cdots,$$

there exists $k \in \mathbb{Z}_{\geqslant 1}$ such that $\mathrm{im}(f^{\circ k}) = \mathrm{im}(f^{\circ (k+1)}) = \cdots$. For any $x \in M$, since $f^{\circ k}(x) \in \mathrm{im}(f^{\circ k}) = \mathrm{im}(f^{\circ (k+1)})$, there exists $x' \in M$ such that $f^{\circ k}(x) = f^{\circ (k+1)}(x')$. This implies $f(f^{\circ k}(x') - f^{\circ (k-1)}(x)) = 0$, and since f is injective, $f^{\circ k}(x') - f^{\circ (k-1)}(x) = 0$. Then, similarly, $f^{\circ (k-1)}(x') - f^{\circ (k-2)}(x) = 0$, $f^{\circ (k-2)}(x') - f^{\circ (k-3)}(x) = 0$, and so on, until we reach $f(x') - x = 0$. Thus $f(x') = x$, showing that f is surjective. Hence, f is an isomorphism. □

Corollary 5.33.

An Artinian integral domain A is a field.

Proof. Let $x \in A \setminus \{0\}$. It suffices to show that multiplication by x is a ring isomorphism. So let $f\colon A \to A$ be the ring homomorphism given by $f(b) = xb$. The function f is injective, since

$$b \in \ker(f) \implies xb = 0 \implies b = 0,$$

where we used the fact that A is an integral domain. By Lemma 5.32, an injective module homomorphism from an Artinian ring is an isomorphism. Since A is Artinian and f is injective, it follows that f is an isomorphism. Thus, x has a multiplicative inverse in A, implying that A is a field. □

6 Artinian Rings and Primary Decompositions

All rings are still to be assumed commutative unless otherwise stated.

6.1 The Descending Chain Condition

What would things look like with a descending chain condition on modules?

Definition 6.1.

A ring A is **Artinian** if every descending chain of ideals $I_0 \supset I_1 \supset \cdots$ stabilizes, that is, there exists $\ell_0 \geqslant 0$ such that for all $\ell \geqslant \ell_0$, $I_\ell = I_{\ell_0}$.

Similarly, define **Artinian** modules over a ring A as those such for which any descending chain of submodules stabilizes.

Example 6.2. (1) $\mathbb{Z}$ is Noetherian but *not* Artinian: $(2) \supset (2^2) \supset (2^3) \supset \cdots$ is an infinite strictly descending ideals, and hence does not stabilize.

(2) If k is a field, then $k[x]$ is Noetherian but *not* Artinian for essentially the same reason, as we may consider the chain

$$(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \cdots .$$

(3) If k is a field, the quotient ring $k[x]/(x^n)$ for any $n \in \mathbb{Z}_{\geqslant 1}$ *is* Artinian. Note that for $n = 1$ this ring is just k, so fields are Artinian.

(4) $\mathbb{Z}/2^n\mathbb{Z}$ is Artinian, since it is a finite ring.

Just as it was for the Noetherian case, the fact a ring is Artinian depends not on the cardinality, but the ideal structure. //

Note 6.3. We now make some formal remarks about Artinian modules analogous to those made in the case of Noetherian modules. To that end, let A be a commutative ring.

(1) An A-module is Artinian if and only if any nonempty set of submodules of M has a *minimal* element; the argument is similar to the analogous statement in the Noetherian case (but instead with *maximal*). (And that result was just a consequence of set-theoretic properties of ordering.)

(2) For any short exact sequence of A-modules $0 \to M_1 \to M \to M_2 \to 0$, M is Artinian if and only if M_1 *and* M_2 are Artinian; again, the argument is the same as the argument for the analogous statement in the case of modules.

(3) If A is Artinian, then A/I is Artinian for any ideal I and $S^{-1}A$ is Artinian for any multiplicatively closed subset S of A.

//

We will see that it turns out that Artinian rings are a *very* special kind of Noetherian rings. Before arguing why this is the case, we will take the first step in exploring the special properties of Artinian rings with the following remarkable fact which shows that being Artinian is a very strong condition:

Proposition 6.4.

If A is an Artinian commutative ring, then *every* prime ideal of A is maximal.

Proposition 6.4 is in notable contrast to the situation of even $k[x]$, where (0) is prime but not maximal.

The proof of Proposition 6.4 can be found here.

The following definition should suggest how we should be interpreting Proposition 6.4.

Definition 6.5.

Suppose A is a commutative ring and

$$\mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \mathfrak{p}_2 \supsetneq \cdots \supsetneq \mathfrak{p}_n$$

is a strictly increasing chain of prime ideals of A. We say this chain has **length** n, and we define the **dimension** of A, denoted $\dim A$, to be the supremum of the lengths over all such chains in A.

Note that the dimension of A is sometimes called the **Krull dimension** of A.

Example 6.6. (1) By Proposition 6.4, any Artinian ring A has dimension 0.

(2) In contrast, $\dim \mathbb{Z} = 1$, since any strictly increasing chain of prime ideals of $\mathbb{Z}$ is of the form $\mathbb{Z}$ is $(0) \subsetneq (p)$ for a prime integer p.

(3) If k is a field, $\dim k[x] = 1$. //

Note 6.7. The intuition behind Definition 6.5 is that we want that the polynomial ring $\mathbb{C}[x_1, \ldots, x_n]$ over $\mathbb{C}$ is the algebro-geometric analog of the n-dimensional complex manifold $\mathbb{C}^n$. This is because it turns out the maximal ideals $\mathrm{Max}(\mathbb{C}[x_1, \ldots, x_n])$, which are of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n \in \mathbb{C}$, turn out to be in bijection with the points $(a_1, \ldots, a_n) \in \mathbb{C}^n$ (we will not show this in these notes, but it is true), so it is reasonable that the dimension of the collection of maximal ideals should be n. The dimension as defined in Definition 6.5 has this property, which is suggested by the fact that the strictly increasing sequence of prime ideals of

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \cdots \subsetneq (x_1, \ldots, x_n),$$

has length n. All of this can be made rigorous, but we will not do so here. But it is important and useful to keep this intuition in mind when working with any rings or modules, let alone those that are Artinian or Noetherian. //

We will show that, in fact, the Artinian rings are precisely the 0-dimensional Noetherian rings.

Proposition 6.8.

An Artinian ring A has only finitely many maximal (equivalently by Proposition 6.4, prime) ideals.

The proof of Proposition 6.8 can be found here.

Note 6.9. The geometric picture of Proposition 6.8 is that if A is Artinian then $\operatorname{Spec} A$ is a finite discrete space.

Indeed, any finite topological space that is T_1 (that is, such that all singletons are closed sets) has the discrete topology, since any subset of a finite space is closed (as a finite union of the closed singletons), which implies the topology on the set is the discrete topology. This is the situation with an Artinian ring A, since by Proposition 6.4 every point in $\operatorname{Spec} A$ is a maximal ideal, which is closed because $V(\mathfrak{m})$ is the set of prime ideals containing $\mathfrak{m}$, which by maximality of $\mathfrak{m}$ is the singleton $\{\mathfrak{m}\}$. And by Proposition 6.8 $\operatorname{Spec} A$ only has finitely many points, so $\operatorname{Spec} A$ is finite with the discrete topology. //

Note 6.10. However, if A is required to be Noetherian, then it *is* true that A is Artinian if and only if $\operatorname{Spec} R$ is finite with the discrete topology, as we shall see. //

Proposition 6.11.

If A is an Artinian ring, then $\sqrt{(0)} = J(A) =: J$, and this ideal is **nilpotent**, that is, $J^n = 0$ for some n.

The proof of Proposition 6.11 can be found here.

6.2 Artinian Modules and Composition Series

Let k be a field and let V be a finite-dimensional vector space over k, say of dimension d. Let $\{x_1, \dots, x_d\}$ be a basis for V. Now define

$$V_i = \operatorname{span}\{x_1, \dots, x_i\}.$$

Then

$$0 \subsetneq V_1 \subsetneq V_2 \subsetneq \cdots \subsetneq V_d = V.$$

Then each quotient V_{i+1}/V_i is 1-dimensional. Here the "length" of this chain is d, which agrees with the notion of dimension. Given what we know about chains of modules (with respect to inclusion), we will now work to generalize the notion "dimension" to modules:

Definition 6.12.

Let R be a commutative ring and let M be an R-module. We say a chain

$$0 \subsetneq M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \cdots \subsetneq M_d = M$$

is a **composition series** if M_{i+1}/M_i is a simple R-module. We call the integer d the **length** of this composition series.

Given the similarity to the definition of composition for series, many proofs regarding composition series that we have already proven for groups can be slightly altered to apply to the situation of modules.

Note that, in the case $R = \mathbb{Z}$ above, the notion of composition series of $\mathbb{Z}$-modules is the same as a composition series of abelian groups.

Proposition 6.13.

If M has a composition series of length d, then

(1) every composition series has length d, and

(2) every chain extends to a composition series.

Proposition 6.14.

Let M be a module over a commutative ring. Then

$$M \text{ has a composition series } \iff M \text{ is Noetherian } \textit{and} \text{ Artinian.}$$

The proof of Proposition 6.14 can be found here.

Example 6.15. Consider $R = M = k[x]/(x^3)$. Then

$$0 = (x^3) \subset (x^2) \subset (x) \subset M$$

For each $i \in \{0, 1, 2\}$, one can show $x^i k[x]/(x^3) \to k$ via $x^i f \mapsto f(0)$ is an R-module homomorphism with kernel $x^{i+1}k[x]/(x^3) = (x^{i+1})$. Thus $k[x]/(x^3)$ has length 3. //

Warning 6.16. We will soon show that if R is an Artinian ring then R is Noetherian ring. However, this is *not* true for modules in general! Indeed, consider Example 6.17 below.

Example 6.17. Consider $R = \mathbb{Z}$ and let M be the $\mathbb{Z}$-module $\mathbb{Z}[1/p]/\mathbb{Z}$. We claim this is an Artinian module that is *not* a Noetherian module. To prove this, let us first classify the submodules of M. Let us start by considering all subgroups of M when viewed as an abelian group: For each $n \in \mathbb{Z}_{\geqslant 0}$, let

$$M_n = \frac{\left\{ \frac{a}{p^n} \;\middle|\; a \in \mathbb{Z} \right\}}{\mathbb{Z}}.$$

We claim $\{M_n\}_{n=1}^{\infty}$ is all the subgroups of the abelian group M. To show this, let N be a proper subgroup of M. Then there exists $n \in \mathbb{Z}_{\geqslant 0}$ such that for some $a \in \mathbb{Z}$, $a/p^n \in N$ but $a/p^{n+i} \notin N$. Now

$$n = \min\{m \in \mathbb{Z}_{\geqslant 0} \mid p^m N = 0\}.$$

Then $N \subset M_n$ by definition of M_n, so we need to show $M_n \subset N$. We may assume a and p are coprime so that a/p^n is written in lowest terms. Since a and p are coprime, there exists $b \in \mathbb{Z}$ such that

$$N \ni 1/p^n = (1 + p^n \cdot (\text{some integer}))/p^n = ab \equiv 1 \pmod{p^n},$$

so $ab/p^n = b(a/p^n) \in N$. Thus $1/p^n$ generates N. This gives us an infinite strictly increasing ascending chain

$$0 = M_0 \subsetneq M_1 \subsetneq M_2 \subsetneq M_3 \subsetneq \cdots,$$

so M is not Noetherian.

But every *descending* chain is of this form since we just showed the M_js are *all* the submodules of M, so any descending chain is of the form $M_j \supsetneq M_{j+1} \supsetneq \cdots \supsetneq 0$, which stabilizes at 0. Thus M is Artinian. //

6.3 Artinian Rings

In this section, we lay much of the groundwork to prove the remarkable fact that Artinian rings are precisely the zero-dimensional Noetherian rings. One inclusion follows quickly, and can be seen as follows:

Corollary 6.18.

Artinian rings are 0-dimensional Noetherian rings.

The proof of Corollary 6.18 can be found here.

We now aim to prove the converse of Corollary 6.18, but there is some theory we must develop first. The full proof (Theorem 6.52 below) will not be until the next section.

Lemma 6.19.

Let R be a commutative ring and suppose some finite product $\mathfrak{n}_1 \cdots \mathfrak{n}_r$ of (not necessarily distinct) maximal ideals in R is zero. Then

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

The proof of Lemma 6.19 can be found here.

We now deduce another consequence of our work.

Corollary 6.20.

Any Artinian ring A is isomorphic to a finite direct product of local Artinian rings.

The proof of Corollary 6.20 can be found here.

Corollary 6.18 then proves the forward implication of the following theorem:

A ring A is Artinian if and only if A is Noetherian and $\dim A = 0$.

To prove the converse of Theorem 6.51, we will use the following theorem:

Any Noetherian ring A has only finitely many *minimal* prime ideals.

Proposition 6.21.

Theorem 6.52 implies Theorem 6.51.

The proof of Proposition 6.21 can be found here.

Example 6.22. Consider $A = \mathbb{C}[x,y]/(xy)$. Then A is Noetherian but not Artinian: its minimal primes are (x) and (y), but A has infinitely many maximal ideals, for example, $(x-a,y)$ or $(x,y-b)$ for $a,b \in \mathbb{C}$. (Note that $(x-a,y-b)$ for general $a,b \in \mathbb{C}$ is not necessarily even an ideal of A, since by the correspondence theorem ideals of $\mathbb{C}[x,y]$ must pull back to ideals of A containing (xy), but for instance $xy \notin (x-1,y-1)$.) And its spectrum $\operatorname{Spec} A$ is the union of coordinate axes, as elaborated upon by Note 6.23 below. //

Note 6.23. Why are minimal primes significant? If A is any commutative ring, then

$$\operatorname{Spec} A = V((0)) = V(\sqrt{(0)}) = V\Big(\bigcap_{\mathfrak{p}\in\operatorname{Spec} A} \mathfrak{p}\Big) \overset{(Corollary\ 11.9)}{=} V\Big(\bigcap_{\substack{\text{minimal}\\ \mathfrak{p}\in\operatorname{Spec} A}} \mathfrak{p}\Big) = \bigcup_{\substack{\text{minimal}\\ \mathfrak{p}\in\operatorname{Spec} A}} V(\mathfrak{p}),$$

where the last inequality holds at least if the collection of minimal prime ideals of A is finite.

We say the $V(\mathfrak{p})$ for minimal primes $\mathfrak{p}$ of A are the **irreducible components** of (the variety) $\operatorname{Spec} A$, to reflect the fact that these are the maximal irreducible subsets of the topological space $\operatorname{Spec} A$. By an **irreducible set** of a topological space we mean a set irreducible if it cannot be written as a union of two proper closed subsets. //

Let R be a commutative ring. In the previous section, we have shown the following facts about R.

- R is Artinian $\iff$ R is Noetherian and $\dim R = 0$ $\iff$ $\operatorname{Spec} R = \operatorname{Max} R$.
- R is Artinian $\implies$ $\operatorname{Max} R < \infty$.
- R is Artinian $\implies$ $|\operatorname{Spec} R| < \infty$. By the previous points, this is equivalent to $\operatorname{Spec} R = \operatorname{Max} R = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$.

Is $\operatorname{Spec} R$ then Hausdorff? Yes, because $\mathfrak{m}_i = V(\mathfrak{m}_i)$. This forces the topology on $\operatorname{Spec} R$ to be the discrete topology. (Also, it turns out that if R is Noetherian then $\operatorname{Spec} R$ is Hausdorff. This is left as an exercise.)

Example 6.24. This example shows that although all Artinian rings have finitely many maximal ideals, the converse is not true.

Let $R = \mathbb{C}[x]_{(x)}$. Then R is not Artinian, since the chain of strictly descending ideals $(x) \supsetneq (x^2) \supsetneq (x^3) \supsetneq \cdots$ does not stabilize in R.

What is $\operatorname{Spec} R$? Since (x) is prime in $\mathbb{C}[x]$, so by Corollary 4.43 there is a bijection

$$\operatorname{Spec} R \longleftrightarrow \{\mathfrak{p} \in R \mid \mathfrak{p} \subset (x)\} = \{(0),(x)\}.$$

What are the closed sets of $\operatorname{Spec} R$? There are only four subsets to consider, and two of them—$\operatorname{Spec} R$ and $\varnothing$—are always closed. Also $\{(x)\}$ is closed, since $\{(x)\} = V((x))$ (since the only elements of $\{(0),(x)\}$ containing (x) is (x)). On the other hand, $\{(0)\}$ is *not* closed, since (0) is contained in (x), hence any ideal containing (0) must be contained in (x) (since any ideal is contained in a maximal ideal, and (x) is the only maximal ideal!).

Thus, the finiteness of $\operatorname{Spec} R$ does *not* imply R is Artinian for general commutative rings R. //

Let R be a non-Noetherian ring. We can choose an ideal I inside R such that I is the only ideal of R/I. (Indeed, So I should not be a prime ideal because then R/I is a field, which does not give a counterexample.) Consider $I = (x_1^2, x_2^2, x_3^2, \dots)$. Then a prime ideal containing I is $\mathfrak{m} = (x_1, x_2, x_3, \dots,)$, which is the kernel of the map $R \to \mathbb{C}$ evaluating at the point $\{x_i\}_{i=1}^{\infty}$ at $\{0\}_{i=1}^{\infty}$. Then if $\mathfrak{q}$ is any other ideal containing I then $\mathfrak{q}$ is a maximal ideal, meaning $\mathfrak{q} = \mathfrak{p}$ because $\mathfrak{p}$ is maximal and I is the only ideal so that $\mathfrak{p}$ contains I.

This ring is then Noetherian but not Artinian because its spectrum is finite and discrete.

Proposition 6.25.

R is Artinian if and only if R is Noetherian and $\operatorname{Spec} R$ is finite with the discrete topology.

The proof of Proposition 6.25 can be found here.

Example 6.26. $\operatorname{Spec} \mathbb{Q} \cong \operatorname{Spec} \mathbb{C}$, $\operatorname{Spec}(\mathbb{C}[x]/(x)) = \operatorname{Spec}(\mathbb{C}[x])/(x^n)$. But $\mathbb{C}[x]/(x)$ is a field whereas $\mathbb{C}[x]/(x^n)$ is not even an integral domain, so the notion of a ring's spectrum is not refined enough to recover the underlying ring.

Algebraic geometry adds more structure to the topological space $\operatorname{Spec} A$ for a commutative ring A that *does* capture these differences, namely by making $\operatorname{Spec} A$ into a locally ringed space. //

6.4 Irreducible and Primary Ideals, and Primary Decompositions

The following definitions were historically motivated by attempts to generalize prime factorization in rings other than the integers. And there is a more modern motivation that is more geometric in nature, namely that these ideas provide a way to take an algebraic variety, which could have several intersecting components, and to recover what those components are.

Definition 6.27.

An ideal I of a ring A is **irreducible** if whenever there exists ideals $J_1, J_2 \subset A$ such that $I = J_1 \cap J_2$, either $I = J_1$ or $I = J_2$.

Example 6.28. In the case $A = \mathbb{Z}$ we have $I = (n) = (m_1) \cap (m_2) = \operatorname{lcm}(m_1, m_2)$ forces $(n) = (m_1)$ or $n = (m_2)$, n must be some prime power (up to sign) or $n = 0$ (Check!). If $I = J_1 \cap J_2$, then $V(I) = V(J_1) \cup V(J_2)$, and irreducibility forces $V(I) = V(J_1)$ or $V(I) = V(J_2)$. (That is, irreducibility of I implies $V(I)$ is irreducible as a topological space.) //

Irreducibility is especially useful in the case of Noetherian rings, as the following result shows.

Lemma 6.29.

In a Noetherian ring A, any ideal is a finite intersection of irreducible ideals.

The proof of Lemma 6.29 can be found here.

We now introduce primary ideals, which, like irreducibility, is another generalization of prime powers of the integers, but is a distinct generalization, as we will see. (And in fact, we will show that in general irreducible implies primary, but not conversely.)

Definition 6.30.

An ideal $\mathfrak{q}$ of A is called **primary** if $\mathfrak{q}$ is proper and for all $a, b \in A$, if $ab \in \mathfrak{q}$ and $a \notin \mathfrak{q}$, then $b \in \sqrt{\mathfrak{q}}$.

Equivalently, $\mathfrak{q}$ is primary if and only if any zerodivisor in $A/\mathfrak{q}$ is nilpotent.

The above definitions are indeed equivalent, as the following proposition shows.

Proposition 6.31.

The following are equivalent:

(1) $\mathfrak{p}$ is primary.

(2) If $y \in R/\mathfrak{p}$ is a zerodivisor, then y is nilpotent.

The proof of Proposition 6.31 can be found here.

Example 6.32. Again taking $A = \mathbb{Z}$, the primary ideals are precisely those generated by the prime powers or (0), that is, is the same as the irreducible ideals. //

Example 6.33. Likewise, if k is a field, then in $k[x]$ one can show for all ideals I that

$$I \text{ is primary } \iff I \text{ is irreducible } \iff I = (0) \text{ or } (p(x)^k) \text{ for some irreducible } p(x) \in k[x].$$

//

The following lemma should not be so surprising after glancing at the definition of a primary ideal, and indeed its proof is an argument by "following your nose":

Lemma 6.34.

If $\mathfrak{q}$ is a proper primary ideal of A, then $\mathfrak{p} = \sqrt{\mathfrak{q}}$ is prime. We say $\mathfrak{q}$ is **$\mathfrak{p}$-primary**, that is $\mathfrak{q}$ is primary and $\mathfrak{p}$ is the prime ideal that is its radical.

The proof of Lemma 6.34 can be found here.

Thus every primary ideal has canonically attached to it a prime ideal given by its radical. And in $\mathbb{Z}$ this just reflects the process of passing from a prime power to a prime itself.

Example 6.35. In contrast to the examples with $\mathbb{Z}$ or $k[x]$ for a field k, we have the following:

(1) A primary ideal is *not* necessarily a power of a prime ideal. For example, where k is a field we can take $A = k[x, y]$ and consider $\mathfrak{q} = (x^2, y)$. Then $A/\mathfrak{q} = k[x, y]/(x^2, y) \cong k[x]/(x^2)$, which has all zerodivisors as nilpotent elements. Thus $\mathfrak{q}$ is primary. Since $\sqrt{\mathfrak{q}} = (x, y)$, we conclude $\mathfrak{q}$ is (x, y)-primary. But one can check that $\mathfrak{p}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$, and that the only prime powers that are options for $\mathfrak{q}$ are $\mathfrak{p}^k$. (For a similar example, see Exercise 11.1)

(2) A power of a prime is not even necessarily primary. Let $A = k[x, y, z]/(xy - z^2)$ and $\mathfrak{p} = (x, z)$. Then $\mathfrak{p}$ is prime (since the quotient $A/(x, z) \cong k[y]$, which is an integral

domain). But $\mathfrak{p}^2 = (x^2, xz, z^2)$ (where $z^2 = xy$) is not primary, since $xy \in \mathfrak{p}^2$ but $x \notin \mathfrak{p}^2$ and $y^n \notin \mathfrak{p}^2$ (that is, $y \notin \sqrt{\mathfrak{p}^2}$) for any $n \in \mathbb{Z}_{\geqslant 1}$. //

Unfortunately, Example 6.35 shows that the primary-to-prime matchup we saw in the ring $\mathbb{Z}$ does not hold in general.

Warning 6.36. Note that we are beginning to blur the distinction between ideals of A and ideals in A/I for some ideal I, and any true mastery of the material should allow one to understand from context which one we are referring to. We will try to be precise, but sometimes with too much precision means not enough intuition. ☡

Example 6.37. If $\mathfrak{q} \subset A$ is an ideal such that $\sqrt{\mathfrak{q}}$ is maximal, then $\mathfrak{q}$ is primary. To see this, note that the nilradical of $A/\mathfrak{q}$ is (the image of) $\sqrt{\mathfrak{q}}$, which is maximal. But the nilradical of the ring is the intersection of all prime ideals of $A/\mathfrak{q}$. But we just said this is maximal, so $\operatorname{Spec}(A/\mathfrak{q}) = \{\mathfrak{q}\}$. So, all elements of $A/\mathfrak{q}$ lying in its unique maximal ideal $\sqrt{\mathfrak{q}}$ are nilpotent (because $\sqrt{\mathfrak{q}}$ is the nilradical of $A/\mathfrak{q}$) and elements not in $\sqrt{\mathfrak{q}}$ are units (because $\sqrt{\mathfrak{q}}$ is the unique maximal ideal of $A/\mathfrak{q}$, so any zerodivisor in $A/\mathfrak{q}$ is nilpotent). //

Example 6.38. We will show that all irreducible proper ideals are primary in Noetherian rings, but the converse is not true in general. To see this, let k be a field and consider the Noetherian ring $k[x, y]$. The ideal $(x, y)^2$ is primary, but $(x^2, xy, y^2) = (x, y)^2 = (x^2, y) \cap (x, y^2)$ is not irreducible. To see $(x, y)^2$ is primary, we can check directly or use Example 6.37 above. //

Definition 6.39.

A **primary decomposition** of an ideal I in a commutative ring A is an expression of I as a finite intersection of primary ideals of A, that is, an expression of the form

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n,$$

where $\mathfrak{q}_j$ is primary for each $j \in \{1, \ldots, n\}$.

We will soon show that they exist for Noetherian rings, and then talk about the extent to which they are unique. We will also use this fact to finally prove that Artinian rings are exactly the Noetherian rings of dimension 0.

6.4.1 Motivation for Primary Ideals

Let I be an ideal of a commutative ring R. It would be nice to build I out of other ideals. If we are motivated by geometry, this would mean writing I as an intersection. If R is Noetherian, we can always write I as a finite intersection of the form $I = \bigcap_{j=1}^n I_j$ (Why?), hence

$$V(I) = V\left(\bigcap\nolimits_{j=1}^n I_j\right) = \bigcup\nolimits_{j=1}^n V(I_j) = \bigcup\nolimits_{j=1} V(\sqrt{I_j}),$$

and the last equality motivates the following intuition: $\mathfrak{p}$ is prime if and only if zerodivisors of $R/\mathfrak{p}$ are contained in (0).

But using prime ideals to decompose our ideal I via intersections would not good enough to think about intersections, since an intersection of a prime ideal with another prime ideal is prime, so we do not recover non-prime ideals.

But motivated by the last equality above, we can consider ideals $\mathfrak{p}$, which we will call primary ideals, which are characterized as ideals $\mathfrak{q}$ such that zerodivisors of $R/\mathfrak{q}$ are contained in $\sqrt{(0)}$.

Warning 6.40. Note that Definition 6.30 is *not* equivalent to the statement that for all $x, y \in \mathfrak{p}$, if $xy \in \mathfrak{p}$ then *both*

(1) if $x \notin \mathfrak{p}$, then $y^n \in \mathfrak{p}$ for some n.

(2) if $y \notin \mathfrak{p}$, then $x^n \in \mathfrak{p}$ for some n.

In other words, definition of a primary ideal is *not* symmetric in x and y. ☡

Example 6.41. Let k be a field and consider $R = k[x,y]$. Then the ideal $I = (x^2, xy)$ is not primary.

In order to understand the importance of computing the quotient, we consider the generator x^2 of I, since it's not immediately clear how quotienting by x^2 affects the structure. Furthermore, we only need to find one example of elements $a, b \in R$ where $ab \in I$, $a \notin I$, and $b^n \notin I$ for any positive integer n.

To that end, consider $a = x$, $b = y$. In this case $xy \in I$, $x \notin I$, and $y^2 \in I$ for all $n \in \mathbb{Z}_{\geqslant 1}$.

Note that this proves an example showing why Warning 6.40 is true, since $yx \in I$, $y \notin I$, and $x^2 \in I$, which would mean I is primary in the weaker definition.

Note that $k[x,y]$ is an example of when a radical of an ideal is a prime ideal: indeed, $\sqrt{I} \supset (x)$ (since $xy \in (x)$). To see $(x) \subset \sqrt{I}$, if $f \in \sqrt{I}$ then $f^n \in I = (x^2, xy)$, so $f^n = xx^2 + \beta xy$, hence $f^n(0,y) = 0$. Thus $f(0,y) = 0$, hence $f \in (x)$, so $(x) = \sqrt{I}$, hence $\sqrt{I}$ is prime. More generally, we can consider Exercise 6.42. //

Exercise 6.42.

Is the weaker condition given in Warning 6.40 equivalent to the condition that the radical of I is prime?

If $\mathfrak{p}$ is primary, then $\mathfrak{P} := \sqrt{\mathfrak{p}}$ is prime. We say that $\mathfrak{p}$ is $\mathfrak{P}$-primary.

Example 6.43. We continue with the notation of Example 6.41. We have $I = (x^2, xy) \subset (x) \cap (x^2, y)$, and if $f \in (x)$ then $f = \alpha x = \beta x^2 + \gamma y$, so $x \mid \gamma = \beta x^2 + \gamma' xy$, which gives the reverse inclusion. Hence $I = (x^2, xy) = (x) \cap (x^2, y)$. And $k[x,y]/(x^2,y) \cong k[x]/(x^2)$, so $f \in k[x]/(x^2)$ is a divisor of $x^2 \iff f \in (x) \iff f^2 = 0$. //

Warning 6.44. We show in Exercise 11.3 that $(x) \cap (x,y)^2 = (x^2, xy, y^2)^n$, so Example 6.43 is an example that the primary decomposition is not unique. (However, some terms of the intersection are the same, and in fact we will soon see a uniqueness statement for primary decompositions that makes this precise.) ☡

Lemma 6.45.

Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal and let $x \in A$.

(1) If $x \in \mathfrak{q}$, then $(\mathfrak{q} : x) = A$.

(2) If $x \notin \mathfrak{q}$, then $(\mathfrak{q} : x)$ is also a $\mathfrak{p}$-primary ideal, hence $\sqrt{(\mathfrak{q} : x)} = \mathfrak{p}$.

The proof of Lemma 6.45 can be found here.

6.5 Primary Ideals of a Localization

Let A be a commutative ring. We saw a way of transferring from prime ideals of A to prime ideals of $S^{-1}A$ in Proposition 4.42. There is a useful analog of this result for primary ideals:

Proposition 6.46.

Let S be a multiplicatively closed subset of a commutative ring A and let $\mathfrak{p}$ be a prime ideal of A.

(1) If $S \cap \mathfrak{p} = \varnothing$, there is a bijection

$$\{\mathfrak{p} \subset S^{-1}A \text{ that are } S^{-1}\mathfrak{p}\text{-primary}\} \longleftrightarrow \{\mathfrak{p}\text{-primary ideals of } A\}.$$

In other words, the bijection is the same to that of Proposition 4.42: the primary ideals of $S^{-1}A$ are in bijective correspondence (via the natural map $j \colon A \twoheadrightarrow S^{-1}A$) with primary ideals of A disjoint from S.

(2) If $S \cap \mathfrak{p} = \varnothing$ and $\mathfrak{q}$ is $\mathfrak{p}$-primary, then $S^{-1}\mathfrak{q} = S^{-1}A$.

The proof of Proposition 6.46 can be found here.

Proposition 6.47.

Let S be a multiplicatively closed subset of A and let $I = \bigcap_{t=1}^{n} \mathfrak{q}_t$ be a minimal primary decomposition of I. Let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ for each $i \in \{1, \ldots, m\}$ and suppose the $\mathfrak{q}_i$ are indexed such that S intersects $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_n$ but not $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Then

$$S^{-1}I = \bigcap_{i=1}^{m} S^{-1}\mathfrak{q}_i \text{ and } j^{-1}(I) = \bigcap_{i=1}^{m} \mathfrak{q}_i,$$

are minimal primary decompositions, where $j \colon A \to S^{-1}A$ is the natural map.

The proof of Proposition 6.47 can be found here.

6.6 Existence of Primary Decompositions in Noetherian Rings

We continue working with a fixed commutative ring A. Just like factorization into prime powers in the case of $A = \mathbb{Z}$, we can ask about the existence and uniqueness of primary decompositions. We have already shown that in a Noetherian ring, any ideal is a finite intersection of irreducible ideals, so if we can show that irreducible ideals are primary then we get primary decompositions in Noetherian rings for free.

Lemma 6.48.

If A is Noetherian, then any irreducible ideal is primary.

By our above comment, we get the following corollary for free.

The proof of Lemma 6.48 can be found here.

Corollary 6.49.

Any ideal in a Noetherian ring has a primary decomposition.

In this section we continue to work with a fixed commutative ring A, and we consider a given ideal I that admits a primary decomposition

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

for some $n \in \mathbb{Z}_{\geqslant 1}$. Recall that for all $j \in \{1, \ldots, n\}$, $\mathfrak{p}_j \coloneqq \sqrt{\mathfrak{q}_j}$ is a prime ideal of A (containing $\mathfrak{q}_j$, hence containing I).

This first feature is common to *any* choice of primary decomposition:

Lemma 6.50.

For any prime $\mathfrak{p} \supset I$ that is minimal (with respect to inclusion) among primes containing I, we have $\mathfrak{p} \in \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.

The proof of Lemma 6.50 can be found here.

We can now finally prove Theorem 6.51 which we restate for convenience:

A ring A is Artinian if and only if A is Noetherian and $\dim A = 0$.

As we mentioned when we first stated this theorem, the forward direction is just Corollary 6.18, so it suffices to show the reverse implication. By Theorem 6.52, it suffices to show A has finitely many minimal prime ideals, which amounts to proving the following theorem:

Any Noetherian ring A has only finitely many *minimal* prime ideals.

Proof of 6.51. By Corollary 6.49, (0) has a primary decomposition, say $(0) = \mathfrak{q}_1 \cap \cdots \mathfrak{q}_n$. By Lemma 6.50, any minimal prime $\mathfrak{p} \subset A$ belongs to $\{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}$ which is a finite set. □

This completes the proof that a commutative ring A is Artinian if and only if A is a 0-dimensional Noetherian ring.

6.7 Uniqueness of Primary Decompositions

To formulate general uniqueness statements, we use the following definition:

Definition 6.53.

A primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ is **reduced** (or **minimal**) if

(1) For all $i \neq j$, $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$. (For example $(12) = (2) \cap (3) \cap (4) = (3) \cap (4)$, but only the last expression satisfies this condition, since $\sqrt{(2)} = \sqrt{(2)} = (2)$.)

(2) For all i, $\mathfrak{q}_i \not\supset \bigcap_{j \neq i} \mathfrak{q}_j$. (The example in the previous point works here too, since $(2) \supset (3) \cap (4) = (12)$ because 2 divides 12.)

Lemma 6.54.

If an ideal I has a primary decomposition, then I has a minimal primary decomposition.

The proof of Lemma 6.54 can be found here.

The above proof is constructive, meaning that if we are given some primary decomposition then we can apply the algorithm described in the proof to obtain a reduced primary decomposition from it.

Definition 6.55.

Suppose I has a reduced primary decomposition $I = \mathfrak{q}_1 \cap \mathfrak{q}$. Define the **associated primes** of I by

$$\operatorname{Ass}(I) \coloneqq \{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}.$$

We denote by $\operatorname{Min}(I)$ the set of minimal primes of R/I viewed in A, and call $\operatorname{Min}(I)$ the **isolated primes** of A. (That is, by the correspondence theorem, $\operatorname{Min}(I)$ is the set of primes in A containing I that are minimal with respect to inclusion.) We have seen $\operatorname{Min}(I) \subset \operatorname{Ass}(I)$ for any choice of primary decomposition. We call $\operatorname{Ass}(I) \smallsetminus \operatorname{Min}(I)$ the **embedded primes** of A.

Note 6.56. There are very good geometric reasons for the above terminology.

- We say "isolated" since the minimal primes $\mathfrak{p}_0$ are such that $V(\mathfrak{p}_0)$ is an irreducible component of the algebraic set $V(I)$, hence is "isolated" from the other irreducible components $V(\mathfrak{p}_0')$ for $\mathfrak{p}_0' \in \operatorname{Min}(I)$. Indeed, by definition of an irreducible set in a topological space, the intersection $V(\mathfrak{p}_0) \cap V(\mathfrak{p}_0')$ must be one of $\varnothing$, $V(\mathfrak{p}_0)$, or $V(\mathfrak{p}_0')$; after thinking about this for a moment, it should become evident that the only possibility is $\varnothing$. Hence $\mathfrak{p}_0$ is indeed "isolated" in the sense that $V(\mathfrak{p}_0)$ is disjoint from every other irreducible component $V(\mathfrak{p}_0)$ of the algebraic set $V(I)$.
- We say "embedded" because the embedded primes are "inside" the isolated primes, since to say $\mathfrak{p} \in \operatorname{Ass}(I) \smallsetminus \operatorname{Min}(I)$ means that there exists $\mathfrak{p}_0 \in \operatorname{Ass}(I)$ such that $\mathfrak{p}$ contains $\mathfrak{p}_0$, hence $\mathfrak{p} \in V(\mathfrak{p}_0)$. Geometrically, this means $\mathfrak{p}$ lives in the component $V(\mathfrak{p}_0)$ of the variety $\operatorname{Spec} A$. //

Warning 6.57. In commutative algebra, we say these are the associated primes of I. But in algebraic geometry, we instead call these the associated primes of R/I.

Definition 6.55 is justified by part (1) of the following theorem.

Theorem 6.58: Uniqueness of Primary Decompositions up to Associated Primes.

Suppose an ideal I of a commutative ring A has a primary decomposition (or equivalently by Lemma 6.54, a minimal primary decomposition), and let

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

be the corresponding minimal primary decomposition. Then:

(1) $\operatorname{Ass}(I)$ is independent of the choice of minimal primary decomposition of I.

(2) For any reduced primary decomposition of I, the $\mathfrak{q}_i$s for which $\sqrt{\mathfrak{q}_i} \in \operatorname{Min}(I)$ are independent of the choice of primary decomposition. (But the other components are not, and by Exercise 11.3 we get infinitely many reduced different ones, but each has the same $\mathfrak{q}$s.)

The proof of Theorem 6.58 can be found here.

Note 6.59. Let A be a commutative ring and I an ideal of A. Suppose I has a primary (hence, a reduced primary) decomposition, say $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$. We defined $\operatorname{Ass} I = \left\{\sqrt{\mathfrak{q}_i}\right\}_{i=1}^{n}$. At first glance, this depends on the choice of primary decomposition, but by Theorem 6.58(1) this set is independent of the choice of reduced primary decomposition of I. In addition, Theorem 6.58(2) states that for those i such that $\sqrt{\mathfrak{q}_i}$ are minimal primes containing I, then not only does $\sqrt{\mathfrak{q}_i}$ appear but also the full primary component $\mathfrak{q}_i$ itself appears in any primary decomposition of I. (So it is canonically associated with I, since it is in all reduced decompositions, hence is independent of choice.) This means there are two types of elements in the $\operatorname{Ass}(I)$, namely

$$\operatorname{Ass} I = \left\{\substack{\text{minimal primes}\\ \text{containing } I}\right\} \amalg \left\{\substack{\text{“embedded”}\\ \text{primes}}\right\}. \qquad //$$

Example 6.60. Let $\overline{k}$ be any algebraically closed field, $A = \overline{k}[x, y]$, and $I = (y^2, xy)$. We picture $\operatorname{Spec}(A/I)$ as the “x-axis with fuzzy origin.” To see this, we ask the following question: Given a polynomial $f(x, y) \in A$, what can we recover about $f(x, y)$ when passing to $f(x, y) \pmod I$? Recall $f(x, y) \pmod I$ is of the form $f(x, y) \pmod I = a_0 + a_1x + \cdots + a_nx^n + b_1y$ (since all other terms are in I). Note that this expression for $f(x, y)$ precisely gives the full behavior of f along the x-axis, but also the behavior of $f(x, y)$ along the y axis *only* at the origin $(0, 0)$ (more precisely, it tells us the first derivative of f in the y direction at the point $(0, 0)$). So, the fuzzy point is pointing “vertically” in the plane. But we can get any directional derivative at the origin by taking linear combinations of the partial derivatives, which means we can recover the information of f on the x-axis, together with derivatives in all directions at $(0, 0)$. This is why we put a fuzzy point at the origin, to indicate that the local behavior is known. (If we know the behavior of the second derivative too, the fuzzy point would be “bigger,” since we know more information.) //

Example 6.61. Consider the following two primary decompositions of I:

$$I = (y) \cap (x, y^2) = (y) \cap (x, y)^2.$$

Then we have the following:

- The associated primes are in both cases $\{(y), (xy)\}$; compare part (1) of the theorem.
- $g_1 \coloneqq (y)$ is a minimal prime containing I ($(x, y) \eqqcolon \mathfrak{p}_2$ is *not*), and the primary component $\mathfrak{q}_1 = (y)$ corresponding to g_1 is the same in both decompositions (the $\mathfrak{q}_2$s are different); compare part (2) of the theorem.
- The associated point $(x, y) \longleftrightarrow$ origin, which is “embedded“” in the x-axis, whereas $(y) \leftrightarrow$ the x-axis. //

The following corollary is then an application of point (1) of the above theorem.

Corollary 6.62.

Let A be any ring where (0) has a primary decomposition (for example, any Noetherian ring). Then

$$ZD = \{0\} \cup \{\text{zerodivisors of } A\} = \bigcup\nolimits_{\mathfrak{p}\in\operatorname{Ass}(0)} \mathfrak{p}.$$

In particular, if $(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ is a reduced primary decomposition, then $ZD = \bigcup_{j=1}^n \mathfrak{p}_j$, where $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$.

The proof of Corollary 6.62 can be found here.

The following corollary then follows, and is helpful to keep in mind.

Corollary 6.63.

If A is any reduced Noetherian ring,

$$ZD = \bigcup\nolimits_{\substack{\text{minimal} \\ \mathfrak{p}\,\in\,\operatorname{Spec} A}} \mathfrak{p}.$$

The proof of Corollary 6.63 can be found here.

6.8 Homework 11

Exercise 6.64: 11.1.

In the polynomial ring $\mathbb{Z}[x]$, show that $\mathfrak{m} = (2, x)$ is a maximal ideal, and $(4, x)$ is $\mathfrak{m}$-primary but is not a power of $\mathfrak{m}$.

A solution to Exercise 6.64 can be found here.

Exercise 6.65: 11.2.

Let A be a commutative ring, and let $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ be $\mathfrak{p}$-primary ideals for a prime ideal $\mathfrak{p}$. Show that $\bigcap_{j=1}^n \mathfrak{q}_j$ is also a $\mathfrak{p}$-primary ideal.

A solution to Exercise 6.65 can be found here.

Exercise 6.66: 11.3.

Let $A = k[x, y]$ for a field k. Consider the ideal $I = (x^2, xy)$ of A. Set $\mathfrak{p} = (x)$ and for all $n \in \mathbb{Z}_{\geqslant 2}$ set $\mathfrak{q}_n = (x^2, xy, y^n)$.

(a) Show that $\mathfrak{p}$ and $\mathfrak{q}_n$ are primary, and $I = \mathfrak{p} \cap \mathfrak{q}_n$ is for each n a primary decomposition of I.

(b) Determine the associated primes of I, and check directly that the (infinitely many) primary decompositions exhibited in part (a) all yield the same set of associated primes.

A solution to Exercise 6.66 can be found here.

Exercise 6.67: 11.4.

Let A be a commutative ring and let M be an A-module. We say M is **free** if there exists an A-module isomorphism of M onto the direct sum $\bigoplus_I A$ for some set I. In this case, we call the cardinality of I the **rank** of M (over A). Show that the rank is well-defined. That is, prove that if M is a free module $M \cong \bigoplus_J A$ for some other set J as well, then I and J have the same cardinality. Hint: Reduce to the corresponding statement (which you may assume) for bases of a vector space by reducing modulo a maximal ideal of A.

A solution to Exercise 6.67 can be found here.

Exercise 6.68: 11.5.

(a) Let A be a ring, and let $P \cong \bigoplus_I A$ be a free A-module on a set I. Show that for any A-module surjection $\pi\colon M \to P$, there is an (injective) A-module section $s\colon P \to M$, and that $M = \ker(\pi) \oplus s(P)$.

(b) Show that if A is a PID and M is a free module of finite rank d over A, then any A-submodule $N \subset M$ is a free module over A of some rank $d' \leqslant d$. Hint: Induct on d; for the induction step, consider a projection $\pi\colon M \to A^{\oplus(d-1)}$ and apply part (a) to the restriction $\pi|_N\colon N \to \pi(N)$.

A solution to Exercise 6.68 can be found here.

7 Factorization

7.1 Irreducible and Prime Elements

Definition 7.1.

Let R be a ring, let $x \in R \smallsetminus R^\times$ be nonzero.

(1) We say x is **irreducible** in R if for all $y, z \in R$, if $x = yz$ then $y \in R^\times$ or $z \in R^\times$.

(2) We say x is **prime** in R if (x) is a prime ideal. Equivalently, if $x \mid yz$, then $x \mid y$ or

$x \mid z$.

Example 7.2. (1) If $R = \mathbb{Z}$, then

$$x \text{ is irreducible in } \mathbb{Z} \iff x \text{ is prime in } \mathbb{Z} \iff x \in \{\pm p \mid p \text{ is a prime integer}\}.$$

(2) If $R = \mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$, then the primes are $2, 3, 4$. But $4 = 2 \times 2$, $3 = 3 \times 3$, and $2 = 4 \times 2$, hence are not irreducible.

(3) If $R = \mathbb{Z}[\sqrt{-5}]$ and $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$, then $4 = (a^2 + 5)(c + d\sqrt{-5})$, so $4 = (a^2 + \cancel{5b^2})(c + \cancel{5d^2})$, forcing $2 = ac$, so 2 is irreducible. And $2 \mid 6 = (1+\sqrt{-5})(1-\sqrt{-5})$, so 2 is not prime. //

Lemma 7.3.

If R is an integral domain, then every prime is irreducible.

The proof of Lemma 7.3 can be found here.

7.2 Unique Factorization Domains (UFDs)

Let R be an integral domain. Suppose x is irreducible but not prime. Then there exist y, z such that $x \mid yz$. So there exists w such that $xw = yz$. Now suppose we can factor y and z as products of irreducible elements as $y_1 \cdots y_n$ and $z = z_1 \cdots z_m$, respectively. Then $xw_1 \cdots w_n = y_1 \cdots y_n z_1 \cdots z_n$. So, if x is irreducible but not prime, then x has some factor that can be factored in more than one way up to multiplication by units.

Using Theorem 5.22 as inspiration, consider the following definition.

Definition 7.4.

Let R be an integral domain. We say R is a **unique factorization domain (UFD)** (or less commonly, R is **factorial**) if

(1) If $x \neq 0$, then there exists $u \in R^\times$ and irreducible elements $x_1, \ldots, x_n \in R$ such that

$$x = ux_1 \cdots x_n.$$

(For example, we can factor 6 as 3×2. Or we can factor 6 as $(-2) \times (-3)$).

(2) If $x = ux_1 \cdots x_n = xu'x'_1 \cdots x'_m$, then

- $m = n$, and
- there exists $\sigma \in S_n$ and units $w_1, \ldots, w_n$ such that for all i, $x_i = w_i x'_{\sigma(i)}$.

Warning 7.5. There are rings, however, where you can have an irreducible element that has no factorization, but such that for which all elements that do have factorizations have unique factorizations. Although any factorization in these rings is unique, they are technically not UFDs by definition. The ring $\mathbb{Z}[\{x^r \mid r \in \mathbb{Q}_{\geqslant 0}\}]$ is an example of such a ring.

Example 7.6.

- $\mathbb{Z}$ is a UFD.
- PIDs are UFDs (the proof is similar to that of $\mathbb{Z}$).

- If R is a UFD, then so is $R[x]$, and thus so is $R[x_1, \dots, x_n]$ for any $n \in \mathbb{Z}_{\geqslant 1}$.
- Since $\mathbb{Z}$ is a UFD and $\mathbb{Z}[x_{i_1}, \dots, x_{i_n}]$ embeds in $\mathbb{Z}[x_1, x_2, \dots]$, because any $f \in \mathbb{Z}[x_1, x_2, \dots]$ is a finite sum we know $f \in \mathbb{Z}[x_{i_1}, \dots, x_{i_n}]$ for some choice of indices, so f can be factored uniquely.
- $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[\sqrt{-2}]$, $\mathbb{Z}[e^{2\pi i/3}]$, $\mathbb{Z}[\varphi]$ where $\varphi = (1+\sqrt{5})/2$. More generally, $\mathbb{Z}[(1+\sqrt{-n})/2]$ or $\mathbb{Z}[\sqrt{-n}]$ is a UFD when $n = 7, 11, 19, 43, 67, 163$. (Interesting historical note: this was proven by a high school teacher in the 1950s, but his proof was not universally accepted until after his death.) //

We can also give several non-examples.

Example 7.7.

- $\mathbb{Z}[\sqrt{-5}]$ is not a UFD, since $1 \pm \sqrt{-5}, 2, 3$ are irreducible but $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$.
- $\mathbb{C}[x, y, z, w]/(xy - zw)$ is not a UFD. Indeed, in this ring we have $xy = zw$ but $x \neq y, z$ and $y \neq z, w$ (and none are units), so the element $xy = zw$ has non-unique factorization into irreducible up to a unit.
- $\mathbb{R}[x^2, x^3]$, the polynomial ring whose elements have no terms of degree 1, is not a UFD, since $x^6 = x^2x^2x^2 = x^3x^3$. //

Although the following statement is conjectured to be in the affirmative, it still remains an open question:

Conjecture 7.8. There are infinitely many square-free integer n such that $\mathcal{O}_n$ is a UFD, where

$$\mathcal{O}_n = \begin{cases} \mathbb{Z}[\sqrt{n}] & \text{if } n \not\equiv 1 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{n}}{2}\right] & \text{if } n \equiv 1 \pmod 4. \end{cases}$$

For n negative in the above conjecture, there are only finitely many integers such that $\mathbb{Z}[\sqrt{-n}]$ is a UFD; such an integer n is called a **Heegner number**, and the set of Heegner numbers is precisely $\{1, 2, 3, 6, 11, 19, 43, 67, 163\}$. (See also the example with the historical note.)

Theorem 7.9.

Let R be an integral domain. Then R is a UFD if and only if both

(1) any nonzero element of R has a factorization, and

(2) irreducible elements are prime elements (that is, generate prime ideals).

The proof of Theorem 7.9 can be found here.

Example 7.10. Suppose $x, y, z \in \mathbb{Z}$ satisfy $x^2 + y^2 = z^2$ in $\mathbb{Z}$. Then in $\mathbb{Z}[i]$, $(x+iy)(x-iy) = (\pi_1 \cdots \pi_n)^2$, hence $(x+iy) = \beta^2 = (a+bi) = (a^2 - b^2) + i(2ab)$. This therefore gives us a parameterization of the Pythagorean triples. (Historical note: a mathematician in 1847 posted an erroneous "proof" of Fermat's last theorem, as it assumed all rings are UFDs.) //

7.3 Factoring Polynomials

We now discuss how unique factorization passes from a ring A to a polynomial ring $A[x]$.

Let A be a UFD. We claim that $A[x]$ is also a UFD, and this will increase our stock of established UFDs. Our current stock includes

- Any PID is a UFD (see Exercise 12.2). Thus $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}[x]$, $k[x]$ for any field k, are all UFDs.
- A polynomial ring over a PID is typically not a PID, but is a UFD (see Exercise 12.2). For example, $\mathbb{Z}[x]$ has non-principal ideal $(2, x)$, but is a UFD. So, this source of UFDs will not get us to an example like $\mathbb{Z}[x]$.

Note that any PID is a UFD, but not conversely. For example, $\mathbb{Z}[x]$ is a UFD, but not a PID, for example by considering the ideal $(2, x)$.

The following is the UFD analog of Hilbert's basis theorem:

Theorem 7.11.

If A is a UFD, then so is $A[x]$, and hence so is $A[x_1, \ldots, x_n]$ for any $n \in \mathbb{Z}_{\geqslant 1}$. In particular, $k[x_1, \ldots, x_n]$ and $\mathbb{Z}[x_1, \ldots, x_n]$ are UFDs for any field k.

To prove Theorem 7.11, we will argue that since A is an integral domain, and thus has a fraction field $\operatorname{Frac}(A[x])$ (by Exercise 12.2) is a UFD, and then pull unique factorizations from the fraction field back to a unique factorization in $A[x]$.

Before giving the proof, we first give some useful definitions.

Definition 7.12.

Let A be a UFD.

(1) For any prime (equivalently by Theorem 7.9, irreducible) element p of A and $a \in \operatorname{Frac}(A) \smallsetminus \{0\}$, we can write $a = p^r \cdot \frac{b}{c}$, where $r \in \mathbb{Z}$, $b, c \in A$, and $p \nmid bc$. Then r is uniquely determined by a, and we define the **valuation** of a with respect to p to be r, and denote it

$$\operatorname{ord}_p(a) \coloneqq r,$$

and by convention we set $\operatorname{ord}_p(0) \coloneqq \infty$. In particular, ord_p defines a group homomorphism $\operatorname{ord}_p\colon \operatorname{Frac}(A)^\times \to \mathbb{Z}$.

(2) Set $k \coloneqq \operatorname{Frac} A$. For any $f \in k[x] \smallsetminus \{0\}$, set $\operatorname{ord}_p f = \min_i(\operatorname{ord}_p(a_i))$, where $f(x) = a_n x^n + \cdots + a_0$. For example, in the case $f(x) = x + 1/p$, we have $\operatorname{ord}_p(x + 1/p) = -1$, and if $f(x) = px^2 + p^3$, then $\operatorname{ord}_p(px^2 + p^3) = 1$.

(3) Fix a choice p of prime element generating each principal prime ideal of A. For any $f \in k[x] \smallsetminus \{0\}$, we define the **content** of f, denoted $c(f)$, as

$$c(f) \coloneqq \prod_{\substack{\text{prime elements} \\ p \in A, \text{ up to units}}} p^{\operatorname{ord}_p(f)}.$$

For example if $A = \mathbb{Z}$ and $f(x) \in \mathbb{Z}[x]$ is given by $f(x) = 30x^2 + 45x + 125$, then since $\mathrm{ord}_p(f) = 0$ for all $p \neq 5$ and $\mathrm{ord}_5(f) = 1$, so

$$c(f) = 5^{\mathrm{ord}_5(f)} = 5^1 = 5.$$

Observe that for any f we can write

$$f = f(c) \cdot f_1,$$

where $c(f_1) = 1$. That is, $f_1(x) \in A[x]$ (that is, there are no negative powers of primes in the coefficients of f_1), and the coefficients have no common prime factors. We say that any polynomial satisfying the same conditions as f_1 are **primitive**. For example, the polynomial $f(x) = 30x^2 + 45x + 125$ is not primitive, but $f_1(x) = 6x^2 + 9x + 25$ is primitive, and $f(x) = 5f_1(x) = c(f)f_1(x)$.

Proposition 7.13: Gauss's Lemma.

If $f, g \in k[x] \smallsetminus \{0\}$, then $c(fg) = c(f)c(g)$.

The proof of Proposition 7.13 can be found here.

(The less formal way of stating the above argument is that if you start with the highest order terms, first find terms in each that are not divisible by p, then the terms corresponding to the sum of those degrees in the product will not be divisible by p, then you can repeat this process for the next highest degree terms, and so on.)

To show $A[x]$ is a UFD, we will combine Proposition 7.13 with the fact that $k[x]$ is a UFD.

Corollary 7.14.

For $f \in A[x]$, if f factors over k, then f factors over A. That is, if f is reducible in $k[x]$, then f is reducible in $A[x]$.

The proof of Corollary 7.14 can be found here.

Note 7.15. For primitive polynomials $f_1 \in A[x]$, then the converse is certainly true. (The reason we are not saying for any polynomial f is because f may be a unit in $k[x]$, that is, f may be some element of A). //

We can now prove Theorem 7.11, which we restate for convenience:

Theorem 7.16: Gauss's Lemma.

If A is a UFD then $A[x]$ is a UFD, and moreover the prime elements of $A[x]$ are the prime (equivalently, irreducible) elements of A together with the primitive polynomials in $A[x]$ that are irreducible in $k[x]$.

The proof of Theorem 7.16 can be found here.

7.4 Strategies for Proving Irreduciblity

The following is an easy-to-prove fact in $\mathbb{Z}[x]$ whose generalization is pretty much the same.

Theorem 7.17.

Let $f \in \mathbb{Z}[x]$ and $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, and let p be a prime. Assume

- $p \nmid a_n$, and
- $f \pmod p$ is irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$.

Then f is irreducible in $\mathbb{Q}[x]$.

The proof easily generalizes to the following.

Theorem 7.18.

Let A be an integral domain and $f \in A[x]$. Let I be any ideal of A and assume

- leading coefficient of $f \notin I$, and
- $f \pmod I$ is irreducible in $(A/I)[x]$.

Then f is irreducible in $(\operatorname{Frac} A)[x]$.

The proof of Theorem 7.18 can be found here.

We also have the following.

Theorem 7.19: Rational root test for $\mathbb{Z}$.

Let $f \in \mathbb{Z}[x]$, $f = a_n x^n + \cdots + a_0$ and let a/b be a root in $\mathbb{Q}$. Then if $f(a/b) = 0$ and $(a, b) = 1$, then $a \mid a_0$ and $b \mid a_n$.

Theorem 7.20: Eisenstein's Criterion for $\mathbb{Z}$.

Let $f \in \mathbb{Z}[x]$, $f = a_n x^n + \cdots + a_0$ and let p be a prime. Assume

(1) $p \nmid a_n$,

(2) $p \mid a_0, a_1, \ldots, a_{n-1}$, and

(3) $p^2 \nmid a_0$.

Then f is irreducible in $\mathbb{Q}[x]$.

Example 7.21.

- $x^n - p$ is irreducible.
- $px^2 - p = p(x-1)(x+1)$.
- $x^2 - p^2$ is reducible
- So (1) of Eisenstein's Criterion is necessary. (Why?).
- And $f(x) = 1 + x + x^2 + \cdots + x^{p+1} = \frac{x^p - 1}{x-1}$.

- Now consider $f(x+1)$. We have
$$f(x+1) = \frac{(x+1)^? - 1}{(x+1)-1} = \frac{\sum_{i=0}^{p} x^i - 1}{x} = \sum_{i=0}^{p-1} \binom{p}{x+1} x^i = x^{p-1} + \binom{p}{1} x^{p-2} + \binom{p}{2} x^{p-3} + \cdots + p,$$
so $p \mid \binom{p}{i}$ for all $i \in \{0, \ldots, p-1\}$. Thus by Eisenstein's Criterion, $f(x+1)$ is irreducible, hence $f(x)$ is too.
- Let $f_1(x) = x^2 + 2x + 6$ (so $p = 2$). And $f_2(x) = x^2 + 3x + 6$ (so $p = 3$). What about over $R = \mathbb{Z}[\sqrt{-5}]$. Then f_1 is irreducible since $f_1(x) = (x + (1 + \sqrt{-5}))x + (1 - \sqrt{-5})$. So the current state of Eisenstein's Criterion does not work for general rings. //

We can generalize Eisenstein's Criterion via prime ideals to integral domains as follows:

Theorem 7.22: Eisenstein's Criterion for Integral Domains.

Let A be an integral domain and $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$. Suppose there exists a prime ideal $\mathfrak{p}$ in A such that:

- $a_n \notin \mathfrak{p}$,
- $a_0, \ldots, a_{n-1} \in \mathfrak{p}$,
- $a_0 \notin \mathfrak{p}^2$.

Then $f(x)$ cannot be written as a product of two positive degree polynomials in $A[x]$. If in addition to (1-3) above, $f(x)$ satisfies

(4) $f(x)$ is primitive in $A[x]$,

then $f(x)$ is irreducible in $A[x]$.

The proof of Theorem 7.22 can be found here.

Theorem 7.22 allows us to factorize polynomials over rings like $\mathbb{Z}[\sqrt{-5}]$, which before this point we were unable to do. For example, if $x^2 + 2x + 6 = (x + (1 + \sqrt{-5}))(x + (1 - \sqrt{-5}))$, and $\mathfrak{p} = (2, 1 + \sqrt{-5})$, $\mathfrak{p}^2 = (4, 2 + 2\sqrt{-5}, -4 + 2\sqrt{-5}) = (2)$, so $x^2 + 2x + 6$ is irreducible over $\mathbb{Z}[\sqrt{-5}]$.

For another example in $\mathbb{Z}[1 + \sqrt{-5}]$, consider $f = x^2 + 3x + 6$. Then $\mathfrak{p} = (3, 1 + \sqrt{-5})$, and we can compute $\mathfrak{p}^2 = (-2 + \sqrt{-5})$. (Alternatively, we can check $6 \notin \mathfrak{p}^2$). Then by Eisenstein's Criterion, f is irreducible over $\mathbb{Z}[1 + \sqrt{-5}]$.

The utility of Eisenstein's criterion in the case of UFDs is strengthened by Gauss's lemma, which allows us to drop the primitive hypothesis:

Theorem 7.23: Eisenstein's Criterion for UFDs.

Let A be a UFD and let$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in A[x]$. If there exists a prime ideal $\mathfrak{p}$ in A such that

(1) $a_n \notin \mathfrak{p}$,

(2) $a_0, \ldots, a_{n-1} \in \mathfrak{p}$, and

(3) $a_0 \notin \mathfrak{p}^2$,

then $f(x)$ is irreducible in $\operatorname{Frac}(A)[x]$ (hence $f(x)$ is also irreducible in $A[x]$).

These two theorems clearly delineate the criteria and conclusions for Eisenstein's Criterion in the contexts of integral domains and UFDs separately. This separation helps avoid confusion and makes the conditions and implications in each case more apparent.

The following theorem then proves the rational root theorem for $\mathbb{Z}$, and generalizes it to arbitrary integral domains:

Theorem 7.24: Rational Root Test for UFDs.

Let R be a UFD, let $k = \operatorname{Frac}(R)$, and let $f \in R[x]$. Then if $f(a/b) = 0$ for some coprime $a, b \in k$, then $b \mid a_n$ and $a \mid a_0$.

The proof of Theorem 7.24 can be found here.

7.5 Hensel's Lemma Over the Integers

We now discuss Hensel's lemma. Hensel's lemma is a generalization of Newton's Method (also called the Newton-Raphson Method), which is a classical method for approximating roots of polynomials. The algorithm is as follows:

- Start with an initial guess x_0 for the root of the equation.
- For each $n \in \mathbb{Z}_{\geqslant 1}$, let $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$, where f' is the formal derivative of f (that is, f' is obtained from f by applying the power rule for each term of f).
- Then $x \coloneqq \lim_{n\to\infty} x_n$ is a root of f.
- Output the final value of x as the approximate root of the equation.

Example 7.25. Consider $f(x) = x^2 - 7$, $x_0 = 1$, $f(x_0) = -2 \times 3$, then $x_1 = 1 - \frac{-6}{4} = 4$, and $f(x_1) = 9$. One can check $x_2 = 23/8$, $f(x_2) = 81/64$ and $f(x_2) = \frac{81}{64} = \frac{3^4}{64}$, $x_3 = \frac{977}{360}$, and $f(x_3) = \frac{6561}{135424} = \frac{3^8}{135424}$. So we seem to be getting higher and higher powers of 3 in the numerator of $f(x_3)$, as n increases.

Let us now make this observation formal with Hensel's Lemma. Note that we say a polynomial f is **monic** if its leading coefficient (the coefficient on the monomial term of f of the highest degree) is 1. //

Theorem 7.26: Hensel's Lemma.

Let $f \in \mathbb{Z}[x]$ be a monic polynomial and let $a \in \mathbb{Z}$. Then if p is a prime integer such that

(1) $f(a) \equiv 0 \pmod{p}$ and

(2) $f'(a) \not\equiv 0 \pmod{p}$,

then for all $n \in \mathbb{Z}_{\geqslant 1}$, there exists a unique $a_n \in \mathbb{Z}/(p^{n+1})$ such that $f(a_n) \equiv 0 \pmod{p^{n+1}}$

and $a_n \equiv a_{n-1} \pmod{p^n}$.

The proof of Theorem 7.26 can be found here.

In other words, Hensel's lemma says that if you have a *simple root*, that is, a root of multiplicity/order 1, then you can lift that root to a root of f modulo p, modulo p^2, modulo p^3, and to a root modulo p^n for any $n \in \mathbb{Z}_{\geqslant 1}$.

Example 7.27. Consider $R[x, \varepsilon]/(\varepsilon^2)$, where $f(x) = \sum a_n x^n$

$$f(x+\varepsilon) = \sum a_n (x+\varepsilon)^n = \sum a_n (x^n + n\varepsilon x^{n-1}) \quad \frac{1}{\varepsilon}(f(x+\varepsilon) - f(x)) = \sum a_n n x^{n-1},$$

so the derivative $\lim_{t \to 0} \frac{1}{t}(f(x+t) - f(t))$ equals $\frac{1}{\varepsilon}(f(x+\varepsilon) - f(\varepsilon))$. Thus we can think of ε as "infinitely small". //

7.6 Homework 12

All rings are still commutative in this problem set. You often see the following definition of associated prime.

Definition 7.28.

Let A be any commutative ring, and let M be an A-module. A prime ideal $\mathfrak{p}$ of A is **associated with** M if it is the annihilator of one of its elements, that is, if for some $x \in M$ we have

$$\mathfrak{p} = \operatorname{Ann}_A(x) = \{a \in A \mid ax = 0\}.$$

Exercise 7.29: 12.1.

Let A be a nonzero commutative Noetherian ring, let

$$(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$$

be a reduced primary decomposition of (0), and let $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ for each i.

(a) Show that for any nonzero $x_i \in \bigcap_{j \neq i} \mathfrak{q}_j$, $\operatorname{Ann}_A(x_i) \subset \mathfrak{p}_i$.

(b) We showed in Exercise 10.2(a) that there exists $m \in \mathbb{Z}_{\geqslant 1}$ such that $\mathfrak{p}_i^m \subset \mathfrak{q}_i$. Deduce that $(\bigcap_{j \neq i} \mathfrak{q}_j) \cdot \mathfrak{p}_i^m = 0$. Replacing m with the least integer such that $(\bigcap_{j \neq i} \mathfrak{q}_j) \cdot \mathfrak{p}_i^m = 0$, verify that for any $x_i \in (\bigcap_{j \neq i} \mathfrak{q}_j) \cdot \mathfrak{p}_i^{m-1}$, $\operatorname{Ann}_A(x_i) \supset \mathfrak{p}_i$.

(c) Conclude that

$$\begin{aligned} \operatorname{Ass}((0)) &= \{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} = \operatorname{Ann}_A(x) \text{ for some } x \in A\} \\ &=: \{\text{prime ideals of } A \text{ associated with } M\} \end{aligned}$$

In other words, for $M = A$, the associated primes of M are what we have previously written as $\operatorname{Ass}((0))$, that is, the associated primes of the zero ideal in A.

A solution to Exercise 7.29 can be found here.

Exercise 7.30: 12.2.

Show that any PID is a UFD.

A solution to Exercise 7.30 can be found here.

Exercise 7.31: 12.3: Hensel's Lemma Over the Integers.

Let $f(x) \in \mathbb{Z}[x]$ be a nonzero monic polynomial and let p be a prime integer. Suppose f has a **simple root** at some $a_0 \in \mathbb{Z}/(p)$, which means

- $f(a_0) = 0$ in $\mathbb{Z}/(p)$ and
- $f'(a_0) \neq 0$ in $\mathbb{Z}/(p)$.

Show that for any $n \in \mathbb{Z}_{\geqslant 1}$ there is a unique $a_n \in \mathbb{Z}/(p^{n+1})$ satisfying

- $f(a_n) = 0$ in $\mathbb{Z}/(p^{n+1})$ and
- $a_n = a_{n-1}$ in $\mathbb{Z}/(p^n)$.

We say a_n is a **lift** of a_0 to a solution over $\mathbb{Z}/(p^{n+1})$. Hint: Use "Newton's method," inductively defining $a_n = a_{n-1} - f(a_{n-1}) \cdot (f'(a_{n-1}))^{-1}$ in $\mathbb{Z}/p^{n+1}\mathbb{Z}$.

A solution to Exercise 7.31 can be found here.

Exercise 7.32: 12.4.

Use Hensel's lemma to calculate all solutions in $\mathbb{Z}/(125)$ to the equation $x^3 + 3x + 1 = 0$.

A solution to Exercise 7.32 can be found here.

Exercise 7.33: 12.5.

(a) Show that the polynomials $x^4 + 1$ and $x^6 + x^3 + 1$ are irreducible in $\mathbb{Q}[x]$.

(b) Is the polynomial $x^2 + y^2 - 1$ irreducible in $\mathbb{Q}[x, y]$? In $\mathbb{C}[x, y]$?

A solution to Exercise 7.33 can be found here.

8 Modules Over PIDs

8.1 Structure Theorem for Finitely Generated Modules Over a PID

Let A be a fixed PID. Recall from Exercise 11.4 that the rank of a free module M, which we will denote $\operatorname{rk} M$, is well-defined. Moreover we showed that if F is a free A-module and $\pi \colon M \twoheadrightarrow F$ is a surjective A-module homomorphism, then π has a section (so $M \cong F \oplus \ker \pi$). If A is a PID and F is a free A-module of rank d, then any A-submodule $F' \subset F$ is also free of some rank $d' \leqslant d$.

Definition 8.1.

Let M be an A-module. We define the **torsion submodule** of M, denoted $\operatorname{Tor}(M)$, by

$$\operatorname{Tor}(M) = \{m \in M \smallsetminus \{0\} \mid am = 0 \text{ for some } a \in A \smallsetminus \{0\}\}.$$

Note that we require elements of $\operatorname{Tor}(M)$ to be nonzero, since otherwise $\operatorname{Tor}(M) = M$. We say M is **torsion-free** if $\operatorname{Tor}(M) = 0$.

Lemma 8.2.

Let A be an integral domain. Then for any A-module M, $M/\operatorname{Tor}(M)$ is torsion-free.

The proof of Lemma 8.2 can be found here.

Proposition 8.3.

If M is torsion-free, then M is free.

The proof of Proposition 8.3 can be found here.

Warning 8.4. The following fact is completely false if M is not finitely generated or if A is not a PID; there are counterexamples in either case!

Corollary 8.5.

M is isomorphic to a direct sum $F \oplus T$, where F is a free module and T is the torsion submodule of M. In particular, the quotient module $M/\operatorname{Tor}(M)$ is free.

The proof of Corollary 8.5 can be found here.

Definition 8.6.

Let I be any ideal of A. Define the ***I*-torsion submodule** of M, denoted by $M[I]$, as the set of elements of M that are annihilated by some nonzero element of I. Formally,

$$M[I] \coloneqq \{m \in M \mid am = 0 \text{ for some nonzero } a \in I\}.$$

Warning 8.7. Although they may seem similar at first, $M[I]$ is very different from $\operatorname{Ann}_I(M)$!

Note that the I-torsion is a submodule of M: If $m \in M$, $a \in A$, and $a' \in A \smallsetminus \{0\}$ kills m, then $aa' \in I$ and is nonzero (since A is an integral domain), and $a'(am) = a(a'm) = a \cdot 0 = 0$, hence $am \in M[I]$. Additionally, if $m, m' \in M[I]$ and $a, a' \in I \smallsetminus \{0\}$ such that $am = 0, a'm' = 0$, then $aa' \in I$ is nonzero and $aa'(m + m') = a'(am) + a(a'm') = 0$, so $m + m' \in M[I]$.

Definition 8.8.

Let p be a prime element of A (that is, $(p) \in \operatorname{Spec} A$), and define the ***p*-infinity torsion**

submodule of M to be

$$M_{p^\infty} := \bigcup_{n=1}^{\infty} M[(p^n)] = \{m \in M \mid p^n m = 0 \text{ for some } n \in \mathbb{Z}_{\geqslant 0}\}.$$

Note that M_{p^∞} is also a submodule of M, by the same argument for $M[I]$.

Note 8.9. If $A = \mathbb{Z}$, then M is an abelian group, and M_{p^∞} is the Sylow p-subgroup of M. Note that showing the Sylow subgroup is actually a subgroup and in this case it is two lines (that is, the proof that I-torsion is a submodule, or in this case a subgroup). This tells us that the above definitions are reasonable notions for us to use when further developing theory, since it allows us to recover other known results. //

Lemma 8.10.

$M_{p^\infty} = 0$ for all but finitely many $(p) \in \operatorname{Spec} A$.

Proof of 8.10. See here.

We now present the main structure theorem for finitely generated modules over a PID, and we will follow it up with several of its variants, consequences, and applications:

Theorem 8.11: Structure Theorem for Finitely Generated Modules over a PID.

Let M be a finitely generated module over a PID A.

(1) There exist unique $r, s \in \mathbb{Z}_{\geqslant 0}$, $q_1, \ldots, q_s \in A$ such that $q_1 \mid q_2 \mid \cdots \mid q_s$ and
$$M \cong A^{\oplus r} \oplus \bigoplus_{i=1}^{s} A/(q_i).$$
The sequence $q_1 \mid q_2 \mid \cdots \mid q_s$ is called the **invariant factor sequence** of M, and the q_i are called the **invariant factors** of M.

(2) If N is a submodule of $A^{\oplus r}$, then there exists a basis $\{e_1, \ldots, e_r\}$ for $A^{\oplus r}$ such that there exist unique $q_1, \ldots, q_r \in A$ satisfying $q_1 \mid q_2 \mid \cdots \mid q_r$, and the nonzero elements of $\{q_1 e_1, \ldots, q_r e_r\}$ form a basis for N.

Proof of 8.11. See here.

Example 8.12. Let $A = \mathbb{Z}$. We can apply the theorem to the following $\mathbb{Z}$-modules as follows. (Note that it helps to keep the CRT in mind here.)

- $M = \mathbb{Z}/16\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. The decomposition of M according to the theorem is $\cong \mathbb{Z}/48\mathbb{Z}$.
- $M = \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. The decomposition of M according to the theorem is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$. But a more intuitive decomposition would be $(\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z}$.
- $M = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The decomposition of M according to the theorem is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. But a more intuitive decomposition would be $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \times \mathbb{Z}/3\mathbb{Z}$. //

The following corollaries show that the "more intuitive" decompositions from Example 8.12 above can be obtained from the structure theorem in a precise way:

Corollary 8.13.

M is isomorphic to $A^{\oplus r} \oplus \bigoplus_{(p)\in \operatorname{Spec} A} M_{p^\infty}$, and for each $(p) \in \operatorname{Spec} A$, there exist unique $t, r_1, \dots, r_t \in \mathbb{Z}_{\geqslant 0}$ such that $r_1 \geqslant r_2 \geqslant \cdots \geqslant r_t$ and

$$M_{p^\infty} \cong A/(p^{r_1}) \oplus \cdots \oplus A/(p^{r_t}).$$

The proof of Corollary 8.13 can be found here.

Corollary 8.14.

There exist unique $r, k \in \mathbb{Z}_{\geqslant 0}$, prime ideals $(p_1), \dots, (p_k) \in \operatorname{Spec} A$, and integers $r_{i,1} \geqslant r_{i,2} \geqslant \cdots \geqslant r_{i,t_i} \geqslant 1$ for each $i \in \{1, \dots, k\}$, such that

$$M \cong A^{\oplus r} \oplus \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{t_i} A/(p_i^{r_{i,j}}).$$

Proof that 8.13 and 8.11 together imply 8.14. See here.

The following is just a more readable version of Corollary 8.14 resulting from a re-indexing:

Corollary 8.15.

If M is a finitely generated module over a PID A, then there exists unique $k, t \in \mathbb{Z}_{\geqslant 0}$, prime ideals $(p_1), \dots, (p_k) \in \operatorname{Spec} A$, $d_1, \dots, d_t \in \mathbb{Z}_{\geqslant 1}$, and $i_1, \dots, i_t \in \{1, \dots, k\}$ such that

$$M \cong A^{\oplus r} \oplus \bigoplus_{j=1}^{t} A/(p_{i_j}^{d_j}).$$

8.2 Applications of the Structure Theorem in Linear Algebra

Fix a field k. We first recall many concepts from linear algebra:

- On a k-vector space V, the data of the following constructions are equivalent:
  (i) $T \in \operatorname{Hom}_k(V, V)$
  (ii) $k[x]$-module structure on V
- For the data (V, T) and (V', T') as in (i), the diagram

$$\begin{tikzcd} V \arrow[r, "T"] \arrow[d, "\varphi"'] & V \arrow[d, "\varphi"] \\ V' \arrow[r, "T'"'] & V' \end{tikzcd}$$

commutes. Equivalently,

$$\left\{ \substack{\varphi\in\operatorname{Hom}_k(V,V') \\ \text{such that } \varphi\circ T=T'\circ\varphi} \right\} \xrightarrow{\cong} \operatorname{Hom}_{k[x]}(V, V')\varphi$$
$$\varphi \longmapsto \varphi.$$

(And this is an equivalence of categories). This condition says that precisely multiplication by x commutes with the action of φ.

- To give an isomorphism $\varphi\colon V \xrightarrow{\cong} V'$ is equivalent to giving a $k[x]$-module isomorphism $\varphi\colon V \xrightarrow{\cong} V'$ such that $T = \varphi^{-1} \circ T' \circ \varphi$. Let (V, T) be as above. Then
  (1) We obtain a k-algebra homomorphism
  $$\begin{aligned} \mathrm{ev}_T\colon k[x] &\longrightarrow \mathrm{End}_k(V), \\ f(x) &\longmapsto f(T), \end{aligned}$$
  whose image is the k-subalgebra $k[T] \subset \mathrm{End}_k(V)$ generated by T.
  (2) When $\dim_k V < \infty$, $\ker(\mathrm{ev}_T) \neq 0$: indeed, $\mathrm{im}(\mathrm{ev}_T) = k[T]$ has $\dim_k k[T] \leqslant \dim_k \mathrm{End}_k(V) = (\dim_k(V))^2 < \infty$.
  Since $\dim_k k[x] = \infty$, $\ker(\mathrm{ev}_T) \neq 0$, hence there exists a unique monic nonzero polynomial $m_T(x)$ such that $\ker(\mathrm{ev}_T) = (m_T(x))$. We call $m_T(x)$ the **minimal polyomial** of T.

  As a consequence, we obtain
  $$\left\{\begin{smallmatrix} (V,T) \text{ such that} \\ \dim_k(V)<\infty \end{smallmatrix}\right\} \longleftrightarrow \left\{\begin{smallmatrix} \text{finitely-generated} \\ \text{torsion } k[x]\text{-modules} \end{smallmatrix}\right\},$$
  via the previous correspondence. (Indeed, we have just seen that when $\dim_k(V) < \infty$, there exists a nonzero $m_T(x)$ annihilating the $k[x]$-module V, which is therefore torsion, and it is finitely generated because it is already finitely generated as a k-module.) The reverse direction of the correspondence (that is, finitely generated torsion implies finite-dimensional and a choice of a linear endomorphism) is left as an exercise.
- Let $\dim_k V < \infty$. For $T \in \mathrm{End}_k(V)$, let A be a matrix of T in some basis $e_1, \ldots, e_n$ (that is, $T(e_j) = \sum_{i=1}^n a_{ij} e_i$, or $(T(e_1) \cdots T(e_n)) = (e_1 \cdots e_n) \cdot A$).
  Now set $p_A(x) \coloneqq \det(x \cdot I_n - A) \in k[x]$, where I_n denotes the $n \times n$ identity matrix over k. We call $p_n(x)$ the **characteristic polynomial** of A. Since the determinant is invariant under conjugation, we are entitled to write $p_T(x) \coloneqq p_A(x)$ and call $p_T(x)$ the **characteristic polynomial of *T***.

8.3 Applications of the Structure Theorem for $k[x]$-Modules

Let (V, T) be as before, but now we impose the condition $\dim_k(V) < \infty$. Then as $k[x]$-modules, we have an isomorphism
$$V \cong \bigoplus\nolimits_{j=1}^{s} k[x]/(q_j)$$
for uniquely determined monic polynomials $q_1, \ldots, q_s$ such that $q_1 \mid q_2 \mid \cdots \mid q_s$. For any $q(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0 \in k[x]$ of degree $d \in \mathbb{Z}_{\geqslant 1}$, with respect to the ordered basis $(1, x, x^2, \ldots, x^{d-1})$ of $k[x]/(q)$, the matrix of multiplication by x is
$$\mathscr{C}_q \coloneqq \begin{pmatrix} 0 & \cdots & \cdots & \cdots & -a_0 \\ 1 & 0 & \cdots & \cdots & -a_1 \\ 0 & 1 & 0 & \cdots & -a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{pmatrix},$$

since $x \cdot x^{d-1} = x^d = -a_0 - a_1 x - \cdots - a_{d-1}x^{d-1}$. We call $\mathscr{C}_q$ the **companion matrix** of q.

8.3.1 Rational Canonical Form

Definition 8.16.

A **rational canonical form** of a linear transformation $T\colon V \to V$ (or of a matrix $A \in M_n(k)$ representing T) is a matrix representation of T in some basis of the form

$$\begin{pmatrix} \mathscr{C}_{q_1} & 0 & \cdots & 0 \\ 0 & \mathscr{C}_{q_2} & \ddots & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \mathscr{C}_{q_s} \end{pmatrix},$$

where the q_j are as in the main structure theorem.

The word "rational" stems from the fact that this is valid in the field k, that is, you do not have to pass to an algebraically closed field containing k.

Theorem 8.17.

Let V be a finite-dimensional k-vector space, with $\dim_k V = n$, and let $T \in \operatorname{End}_k(V)$. Then $V_T \cong \bigoplus_{i=1}^s k[x]/(q_i(x))$ is the unique decomposition by the structure theorem, where $q_1 \mid q_2 \mid \cdots \mid q_s$ and each q_i is monic. Then:

(1) $m_T(x) = q_s(x)$. (Recall $m_T(x)$ is defined as the monic generator of $\ker \mathrm{ev}_T = \operatorname{Ann}_{k[x]}(V_T)$.)

(2) There exists a basis of V in which T has rational canonical form (RCF) and is unique.

(3) $A, B \in M_n(k)$ are conjugate over a field L containing k if and only if they are conjugate over k.

(4) $p_T(x) = \prod_{j=1}^s q_j(x)$, hence $m_T(x) \mid p_T(x) \mid m_T(x)^s$ and $p_T(x)$ and $m_T(x)$ have the same roots. Finally, $p_T(T) = 0$. (This last result is sometimes known as the **Cayley-Hamilton theorem**.)

The proof of Theorem 8.17 can be found here.

8.3.2 Prime Canonical Form

Instead of using invariant factors from the main structure theorem, Corollary 8.14 gives a decomposition

$$V \cong \bigoplus_{i=1}^t k[x]/(p_i(x)^{e_i}),$$

where the p_i are irreducible (not necessarily distinct) in $k[x]$. This resulting canonical form could be called **prime canonical form (PCF)**. (Note that this terminology does not seem to be standard; many opt for the term "Jordan canonical form" in this setting, but any use of the latter term usually implies that we are working over a more special setting that we explore next section, namely over an algebraically closed field.)

8.3.3 Jordan Canonical Form

If a polynomial $p_i \in k[x]$ **splits completely**, that is, if p_i factors into a product of $\deg p_i$ linear polynomials in $k[x]$, then the structure theorem gives us a very special result. For example, if k is any algebraically closed field, then each p_i splits completely over k.

Definition 8.18.

Let $\lambda \in k$. A **Jordan block** of size d and eigenvalue λ is a matrix $J_{\lambda,d} \in M_d(k)$ of the form

$$J_{\lambda,d} \coloneqq \begin{pmatrix} \lambda & 1 & & & \\ & \lambda & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda & 1 \\ & & & & \lambda \end{pmatrix}.$$

Theorem 8.19.

Let k be a field, $T \in \operatorname{End}_k(V)$ for $\dim_k V < \infty$. Assume $p_T(x)$ factors into linear polynomials in $k[x]$ (for example, when k is algebraically closed). Then there exists a basis of V in which T has a matrix

$$\begin{pmatrix} J_{\lambda_1,d_1} & & \\ & \ddots & \\ & & J_{\lambda_r,d_r} \end{pmatrix}$$

for some $d_1, \ldots, d_r \in \mathbb{Z}_{\geqslant 1}, \lambda_1, \ldots, \lambda_r \in k$. We call this the **Jordan canonical form** of T.

The proof of Theorem 8.19 can be found here.

Corollary 8.20.

Let k be any field. Let $A \in M_n(k)$ where $p_A(x)$ has all its roots in k (that is, splits completely in k). Then A is $\mathrm{GL}_n(k)$-conjugate to a diagonal matrix if and only if its minimal polynomial has distinct roots.

The proof of Corollary 8.20 can be found here.

Now fix a field k and consider a pair (V, T), where V is a finite-dimensional k-vector space and $T \in \operatorname{End}_k(V)$.

Exercise 8.21.

Show that isomorphism classes (V, T), where V is a finite-dimensional k-vector space and $T\colon V \to V$ is a linear transformation, are precisely conjugacy classes of $M_n(k)$.

8.4 Classification Problems Using the Structure Theorem for $k[x]$-Modules

Let $n \in \mathbb{Z}_{\geqslant 1}$. By Exercise 8.21, conjugacy classes of $M_n(k)$ are in bijective correspondence with isomorphism classes of pairs (k^n, T) for $T \in \operatorname{End}_k(k^2)$, and these pairs are themselves in bijective correspondence with $k[x]$-modules M such that M is an n-dimensional vector space over k. Thus it suffices to compute the last of these.

By the structure theorem for finitely generated modules over a PID, there exists a unique $r \in \mathbb{Z}_{\geqslant 0}$, $s \in \mathbb{Z}_{\geqslant 1}$, together with unique ideals $(q_1(q)), \ldots, (q_s(x))$ of $k[x]$, such that $(q_s(x)) \subset \cdots \subset (q_1(x))$ and

$$M \cong A^{\oplus r} \oplus \bigoplus_{i=1}^{s} \frac{k[x]}{(q_i(x))}. \tag{8.21.1}$$

Since $(q_j(x)) = (uq_j(x))$ for any unit $u \in k[x]^\times = k \smallsetminus \{0\}$, by choosing u appropriately the uniqueness condition on the chain $(q_1(x)) \subset \cdots (q_s(x))$ is equivalent to when we have that both

(1) $q_i(x)$ is monic for each i, and

(2) $q_1(x) \mid q_2(x) \mid \cdots \mid q_s(x)$.

Note that M must be a torsion module: if not, then M has a direct summand $k[x]^{\oplus r}$ for some $r \in \mathbb{Z}_{\geqslant 1}$, which is infinite-dimensional as a k-vector space. Thus Equation (8.21.1) simplifies as

$$M \cong \bigoplus_{i=1}^{s} k[x]/(q_i(x)).$$

And for each $i \in \{1, \ldots, s\}$ the direct summand $k[x]/(q_i)$ has basis $(1, x, \ldots, x^{\deg q_i - 1})$ as a k-vector space, so

(3) $\dim_k M = \sum_{i=1}^{s} \deg(q_i)$.

The restraints (1), (2), and (3) above therefore uniquely determine the $k[x]$-module structure of the n-dimensional k-vector space M (or equivalently by previous remarks, the conjugacy classes of $M_n(k)$).

Moreover, since the conjugacy classes of $M_n(k)$ are in bijective correspondence with the k-linear transformations and two matrices are conjugate if and only if they have the same rational canonical form, it follows that given $s \in \mathbb{Z}_{\geqslant 1}$ and monic $q_1(x), \ldots, q_s(x)$ satisfying the above conditions, a representative for the corresponding conjugacy class is

$$\begin{pmatrix} \mathscr{C}_{q_1} & & \\ & \ddots & \\ & & \mathscr{C}_{q_s} \end{pmatrix}$$

Our above discussion thus proves the following corollary.

Corollary 8.22.

For any $n \in \mathbb{Z}_{\geqslant 1}$ and any field k, the conjugacy classes of $M_n(k)$ are in bijective correspondence with integers $s \in \mathbb{Z}_{\geqslant 1}$ together with monic polynomials $q_1(x), \dots, q_s(x)$ satisfying

- $q_1(x) \mid q_2(x) \mid \cdots \mid q_s(x)$ and
- $\sum_{i=1}^{s} \deg(q_i) = n$.

Moreover, for any such $s \in \mathbb{Z}_{\geqslant 1}$ and $q_1(x), \dots, q_s(x)$, a representative for the corresponding conjugacy class is the block matrix

$$\begin{pmatrix} \mathscr{C}_{q_1} & & \\ & \ddots & \\ & & \mathscr{C}_{q_s} \end{pmatrix}$$

Example 8.23. (Classification of Conjugacy Classes of $M_2(k)$ with RCF) Let k be a field. To classify the conjugacy classes of $M_2(k)$, by Corollary 8.22 it suffices to determine all possible integers $s \in \mathbb{Z}_{\geqslant 1}$ together with monic polynomials $q_1(x), \dots, q_s(x)$ satisfying

- $q_1(x) \mid q_2(x) \mid \cdots \mid q_s(x)$ and
- $\sum_{i=1}^{s} \deg(q_i) = 2$.

We then have the following two cases:

- If $s = 1$ then $\deg q_1(x) = 2$, so $q_1(x) = x^2 + ax + b$ for some $a, b \in k$. The divisibility condition is trivially satisfied, so this case corresponds to the conjugacy class of $M_2(k)$ with representative
$$\mathscr{C}_{q_1} = \begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}.$$
- If $s = 2$ then $\deg q_1(x) = \deg q_2(x) = 1$, so $q_1(x) = x - a$ and $q_2(x) = x - b$ for some $a, b \in k$. But $q_1(x) \mid q_2(x)$, and $(x - a) \mid (x - b)$ if and only if $a = b$. Thus $q_1(x) = q_2(x) = x + a$, so this case corresponds to the conjugacy class of $M_2(k)$ with representative
$$\begin{pmatrix} \mathscr{C}_{q_1} & \\ & \mathscr{C}_{q_2} \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$ //

Thus the conjugacy classes of $M_2(k)$ for a field k come in two families; an arbitrary matrix $A \in M_n(k)$ is conjugate (that is, represents the same linear transformation) to a matrix of exactly one of the following forms: either

- $\begin{pmatrix} 0 & -b \\ 1 & -a \end{pmatrix}$ for some $a, b \in k$, or
- $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ for some $a \in k$.

Warning 8.24. Although $k[x]/(x) \cong k \cong k[x]/(x-1)$ are isomorphic as rings, it is *not* true that $k[x]/(x) \cong k[x]/(x-1)$ as $k[x]$-module!

Instead of the RCF in the above example, we could have opted to use the PCF. In short, we can obtain the PCF by first decomposing our module into prime components and applying the RCF to the resulting direct summands. The PCF decomposition takes the form

$$M \cong \bigoplus_{i=1}^{t} k[x]/(p_i(x)^{e_i}),$$

where the p_is are irreducible and need not be distinct (but the collection of p_i and the powers e_i that do appear are unique).

Example 8.25. (Classification of Conjugacy Classes of $M_2(k)$ with PCF) By Corollary 8.14, there exist unique $k \in \mathbb{Z}_{\geqslant 0}$, prime ideals $(p_1), \ldots, (p_k) \in \operatorname{Spec} A$, and integers $r_{i,1} \geqslant r_{i,2} \geqslant \cdots \geqslant r_{i,t_i} \geqslant 1$ for each $i \in \{1, \ldots, k\}$, such that

$$M \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{t_i} \mathbb{F}_2[x]/(p_i^{r_{i,j}}).$$

- **Case 1.** $k = 1$.
  - **Case 1(a).** $k = 1$, $t_1 = 1$. Then $M \cong \bigoplus_{i=1}^{1} \bigoplus_{j=1}^{1} \mathbb{F}_2[x]/(p_i^{r_{i,j}}) = \mathbb{F}_2[x]/(p_i^{r_{i,j}})$. This means either $\deg(p_i) = 1$ and $r_{1,1} = 2$, or $\deg(p_i) = 2$ and $r_{1,1} = 1$. In the former case we have $p_i(x) = (x - a)$ for some $a \in \mathbb{F}_2$, in which case

    $$M \cong \frac{\mathbb{F}_2[x]}{((x-a)^2)}.$$

    This gives us two conjugacy classes.

    In the latter case, since the only irreducible polynomial of degree 2 in $\mathbb{F}_2[x]$ is $x^2 + x + 1$, we know $p_1(x) = x^2 + x + 1$ and

    $$M \cong \frac{\mathbb{F}_2[x]}{(x^2 + x + 1)}$$

  - **Case 1(b).** $k = 1, t_1 = 2$. Then $M \cong \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{2} \mathbb{F}_2[x]/(p_i^{i_{i,j}})$, so the only possibility is $p_1(x) = x - a$ for some $a \in \mathbb{F}_2$ and

    $$M \cong \frac{\mathbb{F}_2[x]}{(x-a)} \oplus \frac{\mathbb{F}_2[x]}{(x-a)}.$$

  Then $\deg p_i = 2$, and in fact this forces $t_1 = 2$, since the sum of the dimension of the $k[x]/(p_i^{r_{i,j}})$ as k-vector spaces must coincide with that of M, which is 2.
- **Case 2.** $k = 2$. This case is left as an exercise; similar logic as in the previous case should be used here. In the end, we will recover of course the same conjugacy classes as we did in Example 8.23.

The takeaway from the above two examples is that the RCF is much easier to compute, but PCF is much easier in every other way: we can read off information such as the eigenvalues, the determinant, and the trace, whereas this is not the case for the RCF. //

Example 8.26. Let k be a field. We now classify all matrices up to conjugation with characteristic polynomial $f = x^2(x-1)^3$. By our previous discussions, it suffices to classify finitely generated torsion $k[x]$-modules M such that

- $\dim_k M = 5$,
- $M \cong \bigoplus_{p_i} \frac{k[x]}{(p_i)}$, and

- $\prod_i p_i = f$.

We know $M \cong \bigoplus_p M_{p^\infty}$, where $M_{p^\infty} = \{m \in M \mid p^r m = 0 \text{ for some } r \in \mathbb{Z}_{\geqslant 1}\}$. Now, if g is irreducible and $g \nmid f$, then the r_is in the decomposition of M_{g^∞} as in the first corollary to the structure theorem are all 0.

$$M_{g^\infty} = \begin{cases} 0 & \text{if } g \mid f, \\ 0 & \text{otherwise.} \end{cases}$$

Thus

$$M \cong \underbrace{M_{x^\infty}}_{\dim_k = 2} \oplus \underbrace{M_{(x-1)^\infty}}_{\dim_k = 3}$$

The r_is corresponding to M_{x^∞} thus satisfy $\sum_i r_i = 2$, which gives two possibilities

$$M_{x^\infty} \cong \frac{k[x]}{(x^2)} \xleftrightarrow[\text{with basis } (1,0)]{} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

or

$$M_{x^\infty} \cong \frac{k[x]}{(x)} \oplus \frac{k[x]}{(x)} \xleftrightarrow{\text{with basis } ((1,0),(0,1))} \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

On the other hand, the r_is corresponding to $M_{(x-1)^\infty}$ satisfy $\sum_i r_i = 3$, which gives two possibilities

$$M_{(x-1)^\infty} \cong \frac{k[x]}{(x-1)^3} \longleftrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

or

$$M_{(x-1)^\infty} \cong \frac{k[x]}{(x-1)^2} \oplus \frac{k[x]}{(x-1)} \longleftrightarrow \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 1 & 1 & 0 \\ \hline 0 & 0 & 1 \end{array}\right)$$

or

$$M_{(x-1)^\infty} \cong \frac{k[x]}{(x-1)} \oplus \frac{k[x]}{(x-1)} \oplus \frac{k[x]}{(x-1)} \longleftrightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \qquad /\!/$$

In each way to direct sum any of the two 2×2 matrices above with any of the three 3×3 matrices above gives us a set of non-repeating representatives, thus completing the classification.

Example 8.27. In general, if R is a PID and M is a finitely generated torsion R-module, then we can choose generators for the prime ideals (p) with

$$M \cong \bigoplus_p M_{p^\infty},$$

where

$$M_{p^\infty} = \{m \in M \mid p^r m = 0 \text{ for some } r \in \mathbb{Z}_{\geqslant 1}\}.$$

When $R = \mathbb{Z}$, the M_{p^∞} are precisely the Sylow p-subgroups of M. When $R = \mathbb{C}[x]$, we can take as the ps the monomials $x - \lambda$ for $\lambda \in \mathbb{C}$, and

$$M_{(x-\lambda)^\infty} = \{m \in M \mid (x-\lambda)^n m = 0\},$$

which of course is just the generalized eigenspace for the eigenvalue λ. //

8.5 Review of Decomposing Vector Spaces into (Generalized) Eigenspaces

Definition 8.28.

Let V be a $\mathbb{C}$-vector space, $\lambda \in \mathbb{C}$, and $T \in \mathrm{End}_{\mathbb{C}}(V)$. The **$\boldsymbol{\lambda}$-eigenspace** V_λ is the set

$$V_\lambda \coloneqq \{v \in V \mid Tv = \lambda v\}.$$

Note 8.29. If $v \in V_\lambda$, then $Tv \in V_x$ because $T(Tx) = \lambda(\lambda x) = \lambda(Tv)$, so $Tv \in V_\lambda$.

For instance, if $N = \mathbb{C}^2$ and $T = \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)$, $V_\lambda = 0$ unless $\lambda = 1$. But $\dim_{\mathbb{C}} V_\lambda = 1$, $(0,1) \in V_\lambda$, and $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)^2 = 0$. //

Definition 8.30.

The λ-**generalized eigenspace** is defined by

$$E_\lambda \coloneqq \{v \in V \mid (T - \lambda I)^n v = 0 \text{ for some } n \in \mathbb{Z}_{\geqslant 1}\}.$$

If $v \in E_\lambda$, then $Tv \in E_\lambda$ because

$$(T - \lambda I)^n Tv = T(T - \lambda I)^n v = T(0) = 0.$$

Proposition 8.31.

Under the equivalence of pairs (V, T) with $k[x]$-modules M, the pairs $(E_\lambda, T|_{E_\lambda})$ are in bijection with $M_{(x-\lambda)^\infty}$.

The proof of Proposition 8.31 can be found here.

Corollary 8.32.

Let V be a vector space over $\mathbb{C}$ and $T \in \mathrm{End}_{\mathbb{C}}(V)$. Then

$$V \cong \bigoplus\nolimits_{\lambda \in \mathbb{C}} E_\lambda$$

(and this corresponds to the Jordan form of T).

8.6 Homework 13

Exercise 8.33: 13.1.

(a) Give a complete and non-redundant list of isomorphism classes of $\mathbb{F}_2[x]$-modules of order 8. ($\mathbb{F}_p$ is alternative notation for the field $\mathbb{Z}/p\mathbb{Z}$, when p is prime.)

(b) Give a complete and non-redundant list of conjugacy classes in $\mathrm{GL}_3(\mathbb{F}_2)$.

A solution to Exercise 8.33 can be found here.

Exercise 8.34: 13.2.

Let $m, n \in \mathbb{Z}_{\geqslant 1}$, and let $f\colon \mathbb{Z}^n \to \mathbb{Z}^m$ be a homomorphism of abelian groups.

(a) Show that there are bases of $\mathbb{Z}^n$ and $\mathbb{Z}^m$ in which the matrix of f has the form $\{a_{ij}\}_{1\leqslant i\leqslant m, 1\leqslant j\leqslant n}$ where
  - $a_{ij} = 0$ for all $i \neq j$.
  - For all $i \geqslant 1, a_{ii}$ divides $a_{i+1,i+1}$. (Eventually some of the a_{ii} may all be zero.)

(b) When $m = n$, suppose that in the standard basis f is left multiplication (on column vectors) by a matrix $A \in M_n(\mathbb{Z})$. Show that the image of f is finite index in $\mathbb{Z}^n$ if and only if A is nonsingular, and in that case

$$[\mathbb{Z}^n : \operatorname{im}(f)] = \det(A).$$

A solution to Exercise 8.34 can be found here.

Exercise 8.35: 13.3.

Continuing with the setup of Exercise 13.2, let $m = n = 3$, and suppose that in the standard basis f is left multiplication by the matrix

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Find explicit bases of the source and target in which the matrix of f has the form described in Exercise 13.2. Equivalently, find elements P and Q of $\mathrm{GL}_3(\mathbb{Z})$ such that $Q^{-1}AP$ has the form in Exercise 13.2. Hint: Use elementary row and column operations that are invertible over $\mathbb{Z}$ in combination with the Euclidean algorithm.

A solution to Exercise 8.35 can be found here.

Exercise 8.36: 13.4.

Let V be a finite-dimensional vector space over a field K, and let $\{T_i\}_{i\in I} \subset \operatorname{Hom}_K(V, V)$ be a set of linear maps such that

- Each T_i is diagonalizable over K (i.e. V has a basis of eigenvectors for T_i).
- The T_i all commute with one another: for all $i, j \in I, T_iT_j = T_jT_i$.

Show that there is a basis of V that **simultaneously diagonalizes** all $T_i, i \in I$, that is, such that there is a basis of simultaneous eigenvectors.

Hint: First treat by induction the case where I is finite: to formulate an inductive argument, you will use and should check that if $W \subset V$ is a λ-eigenspace for T_i, some $\lambda \in K$, then every T_j preserves W. For the case where I is infinite, use that the span of all the T_i inside $\operatorname{Hom}_K(V, V)$ is a finite-dimensional K-vector space.

A solution to Exercise 8.36 can be found here.

Exercise 8.37: 13.5.

(a) Let K be a field, and let V and W be finite-dimensional K-vector spaces with given bases $\{v_i\}_{i=1,\dots,n}$ and $\{w_j\}_{j=1,\dots,m}$, and let $T\colon V \to W$ be a K-linear map. As usual, the matrix of T in the given bases is defined to be the $A = (a_{ij}) \in M_{m\times n}(K)$ with $T(v_j) = \sum_{i=1}^{m} a_{ij} w_i$ for all j. Compute the matrix of the dual map $T^*\colon W^* \to V^*$ with respect to the dual bases $\{w_j^*\}$ and $\{v_i^*\}$.

(b) Let V be any K-vector space. Show the canonical K-linear map $\mathrm{ev}\colon V \to (V^*)^*$ is injective in general and is an isomorphism when $\dim_K(V) < \infty$. (Recall $\mathrm{ev}(v)(\lambda) = \lambda(v)$ for $v \in V$ and $\lambda \in V^*$.)

A solution to Exercise 8.37 can be found here.

9 Some Multilinear Algebra

9.1 Dual Space and Tensor Products of Vector Spaces

Fix a field k. In a more general context of modules over a commutative ring A, we have seen:

(i) The direct sum $\bigoplus_{i\in I} M_i$ of any A-modules M_i, for I some index set, is an A-module.

(ii) For any A-modules M and N, $\mathrm{Hom}_A(M,N)$ is an A-module (recall that the A-module structure of $\mathrm{Hom}_A(M,N)$ requires A to be commutative).

We have used these notions for $A = k$, a field. Taking $N = A$ in (ii), we get the dual A-module to M; this is subtle for general A, but we will look at its simple behavior for $A = k$. For any commutative A-modules M and N, we can define a new A-module $M \otimes_A N$, the tensor product of M and N, such that for any A-module P,

$$\left\{ \begin{array}{c} A\text{-bilinear maps} \\ M \times N \to P \end{array} \right\} \cong \left\{ \begin{array}{c} A\text{-module homomorphisms} \\ M \otimes_A N \to P \end{array} \right\}.$$

Again, this is simpler when $A = k$, and we'll introduce this case first, then the general case (including noncommutative A) later.

9.2 Dual Vector Spaces

Let V be a k-vector space. Define the **dual** of V by $V^* := \mathrm{Hom}_k(V,k)$. The k-vector space structure of V^* is the natural vector space structure of $\mathrm{Hom}_k(V,k)$, that is, for all $\lambda, \mu \in V^*$ and all $v \in V$, we have $(\lambda + \mu)(v) = \lambda(v) + \mu(v)$ and $(c \cdot \lambda)(v) = c \cdot \lambda(v)$ for $c \in k$.

Lemma 9.1.

Let V be a k-vector space with basis $(v_i)_{i\in I}$, so that the map $v_i \mapsto e_i = (\delta_{ij})_{j\in I}$ gives an isomorphism $V \cong \bigoplus_{i\in I} k$. Then

$$V^* \cong \prod_{i\in I} k$$

as k-vector spaces, but not naturally.

The proof of Lemma 9.1 can be found here.

Corollary 9.2.

When $\dim_k(V) < \infty$, there is a non-canonical isomorphism $V \xrightarrow{\cong} V^*$ sending the basis $(v_i)_{i\in I}$ to the **dual basis** (v_i^*), which is characterized by the property that for all $i, j \in I$,

$$v_i^*(v_j) = \delta_{ij} = \begin{cases} 1 & \text{if } i = j, \\ 0 & \text{if } i \neq j. \end{cases}$$

When $|I| = \infty$, V and V^* are not isomorphic.

The proof of Corollary 9.2 can be found here.

Note 9.3. (Naturality of Dual Maps) For any k-linear map $\rho\colon V \to W$ (where V, W are k-vector spaces), the dual k-linear map $\rho^*\colon W^* \to V^*$ is defined by $\rho^*(\lambda)(v) = \lambda(\rho(v))$ for all $\lambda \in W^*$. (See also Exercise 13.5.) //

Exercise 9.4.

For finite-dimensional vector spaces V with bases $\{v_i\}$, W with bases $\{w_j\}$, relate the matrix of ρ in these bases to the matrix of ρ^* in the dual bases $\{v_i^*\}$, $\{w_j^*\}$.

Note 9.5. Categorically, V^* is contravariantly functorial in V: for all homomorphisms $T\colon V \to W$ of k-vector spaces, there exists a **dual map** $T^*\colon W^* \to V^*$ given by $T^*(\lambda)(v) \coloneqq \lambda(T(v))$. //

Note 9.6. (Double Dual) In contrast to the basis-dependent isomorphism $V \xrightarrow{\cong} V^*$ in the case $\dim_k V < \infty$, there is a canonical isomorophism $\mathrm{ev}\colon V \to (V^*)^*$. //

In Exercise 13.5 we show that ev is always injective, and is an isomorphism when $\dim_k(V)$ is finite.

9.3 Bilinear Maps and Tensor Products

Let V_1, V_2, and W be k-vector spaces. (Note that we will soon provide a generalization of the following constructions to modules over possibly noncommutative rings, though in that case we need to be a bit more careful.)

Definition 9.7.

A ***k*-bilinear map** is a set map $f\colon V_1 \times V_2 \to W$ such that for all $v_1, v_1' \in V_1$, $v_2, v_2' \in V_2$, and $c \in k$, $v_2 \in V_2$, $f(-, v_2) \in \mathrm{Hom}_k(V_1, W)$, and for each $v_1 \in V_1$ and each $f(v_1, -) \in \mathrm{Hom}_k(V_2, W)$, and

$$\begin{aligned} f(v_1 + v_1', v_2) &= f(v_1, v_2) + f(v_1', v_2), \\ f(v_1, v_2 + v_2') &= f(v_1, v_2) + f(v_1, v_2'), \\ f(cv_1, v_2) &= f(v_1, cv_2) = cf(v_1, v_2). \end{aligned}$$

Example 9.8. Let $A \in M_{m\times n}(k)$. The function $k^m \times k^n \to k$ given by $(x, y) \mapsto x^t A y$ is a k-bilinear map. In terms of matrices, this map is given by

$$\begin{aligned} f\colon k^m \times k^n &\longrightarrow k, \\ (v, w) &\longmapsto v^t A w, \end{aligned}$$

that is,

$$f\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}\right) = \begin{pmatrix} x_1 & \cdots\cdots & x_m \end{pmatrix} \begin{pmatrix} a_{1,1} & \cdots\cdots & a_{1,n} \\ \vdots & \ddots & \vdots \\ a_{m,1} & \cdots\cdots & a_{m,n} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

For instance, in the case $m = n$ and A is the identity matrix I_n, then f is just the dot product of two vectors. //

Notation 9.9. Write $\mathrm{Bilin}_k(V_1 \times V_2, W)$ for the k-vector space of k-bilinear maps $V_1 \times V_2 \to W$. #

Theorem 9.10: Universal Mapping Property of the Tensor Product Space.

There exists a k-vector space $V_1 \otimes_k V_2$, together with a k-bilinear map $\otimes\colon V_1 \times V_2 \to V_1 \otimes_k V_2$ such that for any k-vector space W, the map

$$\begin{aligned} \mathrm{Hom}_k(V_1 \otimes_k V_2, W) &\longrightarrow \mathrm{Bilin}_k(V_1 \times V_2, W) \\ \varphi &\longmapsto \varphi \circ \otimes \end{aligned}$$

is an isomorphism of k-vector spaces.

Definition 9.11.

The pair $(V_1 \otimes V_2, \otimes)$ is called the **tensor product** of V_1 and V_2 over k.

The proof of Definition 9.11 can be found here.

Note 9.12. We use the definite article "the" in the above definition, since it turns out that the tensor product of V_1 and V_2 over k is unique up to a unique isomorphism. The details are left as an exercise. (More generally, uniqueness up to a unique isomorphism is an aspect of the categorical result we will see called Yoneda's lemma.) //

Notation 9.13. We typically write $v_1 \otimes v_2$ for $\otimes(v_1, v_2)$ for any vectors $v_1 \in V_1$, $v_2 \in V_2$. #

Lemma 9.14.

We have $\dim_k(V \otimes_k W) = \dim_k V \cdot \dim_k W$, and this is a cardinality statement in the sense that it is true even when V or W are infinite-dimensional.

The proof of Lemma 9.14 can be found here.

9.4 Functoriality of ⊗ and the ⊗-Hom Adjunction

The following result follows immediately from Theorem 9.10.

Theorem 9.15: Functoriality of Tensoring.

Let $T_1 \colon V_1 \to W_1$ and $T_2 \colon V_2 \to W_2$ be k-linear maps. These induce a unique k-linear map $T_1 \otimes T_2 \colon V_1 \otimes_k V_2 \to W_1 \otimes_k W_2$ making the diagram

$$\begin{tikzcd}
V_1 \times V_2 \arrow[r, "T_1 \times T_2"] \arrow[d, "\otimes"'] \arrow[dr, "k\text{-bilinear}"] & W_1 \times W_2 \arrow[d, "\otimes"'] \\
V_1 \otimes_k V_2 \arrow[r, dashed, "T_1 \otimes T_2"'] & W_1 \otimes_k W_2
\end{tikzcd}$$

commute. Moreover, for all simple tensors $v_1 \otimes v_2$, the resulting map $T_1 \otimes T_2$ satisfies

$$(T_1 \otimes T_2)(v_1 \otimes v_2) = T_1(v_1) \otimes T_2(v_2).$$

Exercise 9.16.

When the spaces are finite-dimensional and we choose bases of V_1, V_2, W_1, W_2, compare the matrix of $T_1 \times T_2$ (with respect to the induced basis on $T_1 \otimes T_2$ on the corresponding tensor spaces) to the matrices of T_1 and T_2. The resulting operation on pairs of matrices is called the **Kronecker product**.

Theorem 9.17: Tensor-Hom Adjunction.

For any k-vector spaces V, W, U, there exists a natural isomorphism of k-vector spaces

$$\operatorname{Hom}_k(V \otimes W, U) \xrightarrow{\cong} \operatorname{Hom}_k(V, \operatorname{Hom}_k(W, U)).$$

The proof of Theorem 9.17 can be found here.

9.5 More Tensor Algebra: Symmetric and Alternating Products

Let V be a k-vector space. Iteratively tensoring V with itself, we define a k-vector space

$$V^{\otimes n} \coloneqq \underbrace{V \otimes_k V \otimes_k \cdots \otimes_k V}_{n \text{ copies of } V},$$

where it is left as an exercise to show that the order in which we tensor is irrelevant (that is, that tensoring vector spaces is associative). This satisfies the universal mapping property

$$\operatorname{Hom}_k(V^{\otimes n}, W) \cong \operatorname{Multilin}_k(V^{\times n}, W), \tag{9.17.1}$$

where $\operatorname{Multilin}_k(V^{\times n}, W)$ denotes the collection of functions that are linear in each variable when fixing the other $n-1$ variables.

Definition 9.18.

Define the **tensor algebra** of V by

$$T(V) \coloneqq \bigoplus_{n=0}^{\infty} V^{\otimes n}.$$

Note 9.19. The tensor algebra is indeed a k-algebra, but it is noncommutative. The product in this algebra is characterized by its behavior on simple tensors: the map V for all $m, n \in \mathbb{Z}_{\geqslant 0}$, the multiplication on $V^{\otimes m} \times V^{\otimes n} \to V^{\otimes(m+n)}$ is given by

$$(v_1 \otimes \cdots \otimes v_m) \cdot (w_1 \otimes \cdots \otimes w_n) = v_1 \otimes \cdots \otimes v_m \otimes w_1 \otimes \cdots \otimes w_n. \qquad //$$

Exercise 9.20.

Use the universal property to define the algebra structure:

$$\begin{tikzcd}
V^{\times(n+m)} \arrow[r, phantom, "="] & V^{\times m} \times V^{\times n} \arrow[r] \arrow[d] & V^{\otimes(m+n)} \arrow[d, equal] \\
& V^{\otimes m} \times V^{\otimes n} \arrow[r] \arrow[ur, dashed, "m"] & V^{\otimes m} \otimes V^{\otimes n}
\end{tikzcd}$$

The product is the arrow m.

9.5.1 Special Kinds of Multilinear Maps

For all $n \in \mathbb{Z}_{\geqslant 0}$, define

$$\mathrm{Sym}_k(V^{\times n}, W) \coloneqq \{f \in \mathrm{Multilin}_k(V^{\times n}, W) \mid f(v_{\sigma(1)}, \ldots, v_{\sigma(n)}) = f(v_1, \ldots, v_n) \text{ for all } \sigma \in S_n\},$$
$$\mathrm{Alt}_k(V^{\times n}, W) \coloneqq \{f \in \mathrm{Multilin}_k(V^{\times n}, W) \mid f(v_1, \ldots, v_n) = 0 \text{ whenever } v_i = v_j \text{ for some } i \neq j\}.$$

Also for all $n \in \mathbb{Z}_{\geqslant 0}$, set

$$S^n(V) \coloneqq V^{\otimes n} \Big/ \left\{ \substack{k\text{-vector subspace spanned by all} \\ v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)} - v_1 \otimes \cdots \otimes v_n \text{ for all } \sigma \in S_n} \right\},$$
$$\Lambda^n(V) \coloneqq V^{\otimes n} \Big/ \left\{ \substack{k\text{-vector subspace spanned by all} \\ v_1 \otimes \cdots \otimes v_n \text{ such that } v_i = v_j \text{ for some } i \neq j} \right\}.$$

We write $v_1 v_2 \cdots v_n$ (resp. $v_1 \wedge v_2 \wedge \cdots \wedge v_n$) for the element of $S^n(V)$ (resp. $\Lambda^n(V)$) that is the image of $v_1 \otimes \cdots \otimes v_n \in V^{\otimes n}$ under the quotient map $V^{\otimes n} \twoheadrightarrow S^n(V)$ (resp. $V^{\otimes n} \twoheadrightarrow \Lambda^n(V)$).

Theorem 9.21: Universal Properties of the Alternating and Symmetric Algebras.

For all k-vector spaces W, the following diagram commutes:

$$\begin{tikzcd}
\mathrm{Hom}_k(\Lambda^n(V), W) \arrow[r, dashed, no head, "\cong"] \arrow[d, hook] & \mathrm{Alt}_k(V^{\times n}, W) \arrow[d, hook] \\
\mathrm{Hom}_k(V^{\otimes n}, W) \arrow[r, no head, "\cong"] & \mathrm{Multilin}_k(V^{\times n}, W) \\
\mathrm{Hom}_k(S^n(V), W) \arrow[r, dashed, no head, "\cong"] \arrow[u, hook] & \mathrm{Sym}_k(V^{\times n}, W) \arrow[u, hook]
\end{tikzcd}$$

where the middle isomorphism is from Equation (9.17.1).

For $v_1, \ldots, v_n \in V$ and $\sigma \in S_n$, we have the action $v_1 \wedge \ldots \wedge v_n \mapsto \mathrm{sgn}(\sigma) v_{\sigma(1)} \wedge \ldots \wedge v_{\sigma(n)}$.

We can prove this by decomposing σ as a product of 2-cycles $(i \quad j)$ with $i \neq j$, in which case

$$\begin{aligned} 0 &= v_1 \wedge \ldots \wedge \underbrace{(v_i + v_j)}_{i\text{th position}} \wedge \ldots \wedge \underbrace{(v_i + v_j)}_{j\text{th position}} \wedge \ldots \wedge v_n \\ &= v_1 \wedge \ldots \wedge v_i \wedge \ldots \wedge v_j \wedge \ldots \wedge v_n + v_1 \wedge \ldots \wedge v_j \wedge \ldots \wedge v_i \wedge \ldots \wedge v_n \\ &= v_1 \wedge \ldots \wedge v_i \wedge \ldots \wedge v_j \wedge \ldots \wedge v_n - v_1 \wedge \ldots \wedge v_i \wedge \ldots \wedge v_j \wedge \ldots \wedge v_n. \end{aligned}$$

When $\operatorname{char} k \neq 2$, this sign condition is equivalent to the given definition; however, in general the given definition is stronger. If we defined a wedge using the sign condition, then for all v, w,

$$v \wedge v + v \wedge w = v \wedge (v + w) = -(v + w) \wedge v = -v \wedge v - w \wedge v,$$

so $2(v \wedge v) = 0$, or equivalently when $\operatorname{char} k \neq 2$ $v \wedge v = 0$.

Proposition 9.22.

Let V be a finite-dimensional k-vector space with basis $e_1, \ldots, e_n$. Then for all $d \in \mathbb{Z}_0$,

(1) $\dim_k S^d(V) = \binom{n+d-1}{d}$ with basis $\{e_{i_1} e_{i_2} \cdots e_{i_d} \mid 1 \leqslant i_1 \leqslant \cdots \leqslant i_d \leqslant n\}$.

(2) $\dim_k \Lambda^d(V) = \binom{n}{d}$ with basis $\{e_{i_1} \wedge \cdots \wedge e_{i_d} \mid 1 \leqslant i_1 < \cdots < i_d \leqslant n\}$.

Proof. We only prove (2), leaving (1) as an exercise. Consider the map $V^{\otimes d} \to \Lambda^d(V)$ given by $e_{i_1} \otimes \cdots \otimes e_{i_d} \mapsto e_{i_1} \wedge \ldots \wedge e_{i_d}$. We know that $\{e_{i_1} \otimes \ldots \otimes e_{i_d} \mid i_1, \ldots, i_d \in \{1, \ldots, n\}\}$ spans $\wedge^d$, so their images span $\Lambda^d(V)$. But for all $i_1, \ldots, i_d$, if $i_j = i_k$ for some $j \neq k$ then $e_{i_1} \wedge \ldots \wedge e_{i_d} = 0$. Thus, to span $\Lambda^d(V)$, we may restrict to the d-tuples with all i_j distinct. Since $e_{i_1} \wedge \ldots \wedge e_{i_d} = \operatorname{sgn}(\sigma) e_{i_{\sigma(1)}} \wedge \ldots \wedge e_{i_{\sigma(d)}}$ for all $\sigma \in S_d$, we find that $\{e_{i_1} \wedge \ldots \wedge e_{i_d}\}_{i_1 < \ldots < i_d}$ span $\Lambda^d(V)$.

It remains to show linear independence.

- Case 1. $d = n$: Then by the above, $e_1 \wedge \ldots \wedge e_n \in \Lambda^n(V)$, so it suffices to show $e_1 \wedge \ldots \wedge e_n \neq 0$. We do this by writing down a $\lambda \in \operatorname{Alt}_k(V^{\times n}, k) \cong \operatorname{Hom}_k(\Lambda^n(V), k)$ such that $\lambda(e_1, \ldots, e_n) \neq 0$. This λ will be familiar: let $\{e_i^*\}_{i=1}^n$ be the dual basis, and for all $v_1, \ldots, v_n \in V$ set
$$\lambda(v_1, \ldots, v_n) = \sum\nolimits_{\sigma \in S_n} \operatorname{sgn}(\sigma) e_1^*(v_{\sigma(1)}) \cdots e_n^*(v_{\sigma(n)}).$$
Multilinearity of λ is then clear, and if $v_i = v_j$ for some $i \neq j$, then observe for any $\sigma \in S_n$ that, where $\tau = \sigma \circ (ij)$,
$$\begin{aligned} &\operatorname{sgn}(\sigma) e_1^*(v_{\sigma(1)}) \cdots e_n^*(v_{\sigma(n)}) + \operatorname{sgn}(\tau) e_1^*(v_{\tau(1)}) \cdots e_n^*(v_{\tau(n)}) \\ &\quad = \operatorname{sgn}(\sigma)\big[e_1^*(v_{\sigma(1)}) \cdots e_i^*(v_{\sigma(j)}) \cdots e_j^*(v_{\sigma(i)}) \cdots e_n^*(v_{\sigma(n)})\big] \\ &\qquad + \operatorname{sgn}(\tau)\big[e_1^*(v_{\tau(1)}) \cdots e_i^*(v_{\tau(j)}) \cdots e_j^*(v_{\tau(i)}) \cdots e_n^*(v_{\tau(n)})\big] \\ &\quad = \operatorname{sgn}(\sigma)\Big[\prod\nolimits_{\substack{l=1 \\ l \neq i,j}}^n e_l^*(v_{\sigma(l)})\Big]\big(e_i^*(v_{\sigma(j)}) e_j^*(v_{\sigma(i)}) - e_i^*(v_{\sigma(i)}) e_j^*(v_{\sigma(j)})\big) \\ &\quad = 0, \end{aligned}$$
where the last equality is because $v_i = v_j$. Thus the $n!$ terms in the sum cancel in pairs, and λ is alternating. Finally, $\lambda(e_1, \ldots, e_n) = 1$ since only $\sigma = \mathrm{id}$ contributes a nonzero

term.

- Case 2. $d < n$: Suppose we have a linear relation
$$\sum\nolimits_{1 \leqslant i_1 < \ldots < i_d \leqslant n} a_{i_1,\ldots,i_d} e_{i_1} \wedge \ldots \wedge e_{i_d} = 0 \text{ in } \Lambda^d V.$$
For $J = (j_1, \ldots, j_d)$ such that $j_1 < \ldots < j_d$, we use the linear map $e_J^* \colon \Lambda^d(V) \to \Lambda^n(V)$ given by $e_J(x) \coloneqq x \wedge (e_1 \wedge \cdots \wedge \widehat{e}_{j_1} \wedge \cdots\cdots \wedge \widehat{e}_{j_d} \wedge \cdots \wedge e_n)$, where the hat notation is to indicate all the $e_{j_1}, \ldots, e_{j_n}$ are to be omitted. Then
$$0 = e_J\left(\sum a_{i_1 \cdots i_d} e_{i_1} \wedge \ldots \wedge e_{i_d}\right) = \pm a_{j_1 \cdots j_d} e_1 \wedge \cdots \wedge e_n.$$
By the case $d = n$ above, this implies $a_{j_1 \cdots j_d} = 0$ for all J, as desired. □

Exercise 9.23.

Prove point (1) of Proposition 9.22. (Or see Lang XVI.8.1.)

The above proof of (2) of Proposition 9.22 used the k-algebra structure of $\Lambda^\bullet(V)$:

Exercise 9.24.

Show the k-algebra structure of the tensor algebra $T(V) = \bigoplus_{n=1}^{\infty} V^{\otimes n}$ induces a k-algebra structure on $\Lambda^\bullet(V) \coloneqq \bigoplus_{d \geqslant 0} \Lambda^d(V)$, the **symmetric algebra**, and on $S^\bullet(V) = \bigoplus_{d \geqslant 0} S^d(V)$, called the **exterior algebra**.

Exercise 9.25.

Show that $S^\bullet$ and $\Lambda^\bullet$ are functorial in the sense that any k-linear map $f \colon V \to W$ induces

- k-linear maps $S^d f \colon S^d(V) \to S^d(W)$ $\Lambda^d f \colon \Lambda^d(V) \to \Lambda^d(W)$, and
- k-algebra homomorphisms $\Lambda^\bullet f \colon \Lambda^\bullet(V) \to \Lambda^\bullet(W)$, $S^\bullet f \colon S^\bullet(V) \to S^\bullet(W)$.

The wedge powers $\Lambda^n(V)$ lead to the theory of determinants (for dimension n) vector spaces:

Corollary 9.26.

Let V be a K-vector space of dimension n. Let $T \in \operatorname{End}_K(\Lambda^n V) = K$ be multiplication by a scalar. This is $\det(T)$ (and can serve as the definition of determinant).

The proof of Corollary 9.26 can be found here.

This also gives conceptually clear proofs that $\det(AB) = \det(A)\det(B)$ (because $\det(AB)e_1 \wedge \ldots \wedge e_n = ABe_1 \wedge \ldots \wedge ABe_n = \det(A)Be_1 \wedge \ldots \wedge Be_n = \det(A)\det(B)e_1 \wedge \ldots \wedge e_n$ and the determinant is basis-invariant).

Note 9.27. Analogously, the minors of a matrix $A \in M_n(K)$ correspond to matrix entries of $\Lambda^d A$ in its standard basis. //

10 Math 6111 Final Qualifying Exam: Fall 2023

10.1 Review Exercises and Solutions

Exercise 10.1: RF1: #1, OSU Algebra Qualifying Exam, Autumn 2023.

Let H be a proper normal subgroup of a finite group G, and let p be a prime factor of $|G/H|$. Show that the number of Sylow p-subgroups of G/H divides the number of Sylow p-subgroups of G.

A solution to Exercise 10.1 can be found here.

Exercise 10.2: RF2: #2, OSU Algebra Qualifying Exam, Autumn 2023.

Let G be a finite group such that any two of its proper maximal subgroups are conjugate. Prove that G is cyclic.

A solution to Exercise 10.2 can be found here.

Exercise 10.3: RF3: #3, OSU Algebra Qualifying Exam, Autumn 2023.

Let R be a commutative ring, and $f_1, f_2, \dots, f_r \in R$ such that they generate the unit ideal. Show that an R-module M is finitely generated if and only if for all $i = 1, \dots, r$, the localization M_{f_i} is a finitely generated R_{f_i}-module. (Here R_{f_i} and M_{f_i} are the localizations $S^{-1}R$ and $S^{-1}M$ with respect to the multiplicative subset $S = \{f_i^n\}_{n \in \mathbb{Z}_{\geqslant 0}}$.)

A solution to Exercise 10.3 can be found here.

Exercise 10.4: RF4: #4, OSU Algebra Qualifying Exam, Autumn 2023.

Let D be a unique factorization domain. Define what it means for a polynomial $f(x) \in D[x]$ to be primitive. Prove that if $f(x)$ and $g(x) \in D[x]$ are both primitive, then $f(x) \cdot g(x)$ is primitive.

A solution to Exercise 10.4 can be found here.

Alternate Solution to 10.4. See here.

Exercise 10.5: RF5: #5, OSU Algebra Qualifying Exam, Autumn 2023.

(We did not cover determinants formally, so this material would not appear on the final qualifying exam.) Let A be an $n \times n$ matrix of rank k over a field. What is the rank of $\operatorname{adj}(A)$? Recall that $\operatorname{adj}(A)$ is the $n \times n$ matrix whose (i, j)-entry is $(-1)^{i+j}$ times the determinant of the $(n-1) \times (n-1)$ matrix obtained from A by removing the jth row and ith column.

A solution to Exercise 10.5 can be found here.

Exercise 10.6: RF6.

Classify up to isomorphism groups of order 245.

A solution to Exercise 10.6 can be found here.

Exercise 10.7: RF7.

Let G be a group, and let H be a finite index subgroup of G. Show there is a subgroup $N < H < G$ such that N is normal in G and $[G : N] < \infty$.

A solution to Exercise 10.7 can be found here.

Exercise 10.8: RF8.

Let $\mathbb{H}$ be the $\mathbb{R}$-algebra of quaternions (see the construction from class). Exhibit an injective $\mathbb{R}$-algebra homomorphism $\mathbb{H} \to M_2(\mathbb{C})$ (2-by-2 complex matrices).

A solution to Exercise 10.8 can be found here.

Exercise 10.9: RF9.

Let A be a commutative ring. An element $e \in A$ is called **idempotent** if $e^2 = e$.

(a) Give an example of a ring A and an idempotent $e \in A \setminus \{0, 1\}$.

(b) Show that if $e \in A$ is idempotent, so is $1 - e$.

(c) Prove the following are equivalent:

(i) A contains an idempotent $e \neq 0, 1$.

(ii) A is isomorphic as a ring to a direct product $A_1 \times A_2$ of nonzero rings A_1 and A_2.

A solution to Exercise 10.9 can be found here.

Exercise 10.10: RF10.

(a) Prove that $x^7 + 48x - 24$ is irreducible in $\mathbb{Q}[x]$. Is it irreducible in $(\mathbb{Q}(i))[x]$?

(b) Prove that $x^3 + y + y^5$ is irreducible in $\mathbb{C}[x, y]$.

A solution to Exercise 10.10 can be found here.

Exercise 10.11: RF11.

For each of the abelian groups

(a) $\mathbb{Q}$,

(b) $\mathbb{Q}/\mathbb{Z}$, and

(c) $\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$ (as a subring of $\mathbb{Q}(\sqrt{-3})$, or if you prefer, of $\mathbb{C}$), say whether they are

(i) finitely-generated,

(ii) torsion-free, or

(iii) free.

A solution to Exercise 10.11 can be found here.

Exercise 10.12: RF12.

Describe the primary ideals in a PID A.

A solution to Exercise 10.12 can be found here.

Exercise 10.13: RF13.

For a prime p, how many conjugacy classes are there in $\mathrm{GL}_2(\mathbb{Z}/(p))$?

A solution to Exercise 10.13 can be found here.

Exercise 10.14: RF14.

Let $v = (a_1, \ldots, a_n)$ be an element of $\mathbb{Z}^n$. Show that v extends to a basis of $\mathbb{Z}^n$ if and only if $\gcd(a_1, \ldots, a_n) = 1$.

A solution to Exercise 10.14 can be found here.

10.2 The Final and Solutions

Write your solutions neatly, including your name and the problem number on each page you submit. State clearly any results from class you use. You have 1 hour and 50 minutes. Good luck!

Exercise 10.15: F1.

Let p be a prime, and let P be a p-group (that is, $|P| = p^n$ for some $n \in \mathbb{Z}_{\geqslant 1}$). Let $Q \lhd P$ be a normal subgroup.

(a) (2.5 points) If $|Q| = p$, show that Q is contained in the center of P.

(b) (2.5 points) Show by an example that when $|Q| = p^2$, Q need not be contained in the center of P.

A solution to Exercise 10.15 can be found here.

Exercise 10.16: F2.

Let A be a commutative ring. Recall that on the homework (Exercise 10.3) we proved Nakayama's Lemma: If M is a finitely-generated A-module such that $J(A)M = M$, then

$M = 0$. You may use this in what follows.

(a) (1 point) If M is a finitely-generated A-module, and $N \subset M$ is an A-submodule such that $M = N + J(A)M$, show that $N = M$.

(b) (4 points) Let A and B be Noetherian local rings with maximal ideals $\mathfrak{m}_A$ and $\mathfrak{m}_B$, and let $\varphi\colon A \to B$ be a ring homomorphism such that $\varphi^{-1}(\mathfrak{m}_B) = \mathfrak{m}_A$.[a] Assume:

- φ makes B into a finitely-generated A-module.[b]
- φ induces an isomorphism $A/\mathfrak{m}_A \xrightarrow{\cong} B/\mathfrak{m}_B$.
- The restriction of φ gives a surjection $\mathfrak{m}_A \to \mathfrak{m}_B/\mathfrak{m}_B^2$.

Show that φ is surjective. Hint: Apply part (a) twice, first with "M" the B-module $\mathfrak{m}_B$, and then with "M" the A-module B.

[a] We call such a map φ a **local homomorphism** of local rings; this condition is ubiquitous in algebraic geometry.

[b] As a reminder, the A-module structure on B is $a \cdot b = \varphi(a)b$ for $a \in A, b \in B$.

A solution to Exercise 10.16 can be found here.

Exercise 10.17: F3.

Let A be a commutative ring, and let M be an A-module. When M is a finitely-generated A-module, show that[a]

$$V(\mathrm{Ann}_A(M)) = \mathrm{supp}(M).$$

[a] As a reminder, $M_{\mathfrak{p}}$ denotes the localization of M with respect to the multiplicative subset $A \smallsetminus \mathfrak{p}$ and $V(\mathrm{Ann}_A(M))$ denotes the set of prime ideals of A containing the annihilator of M.

A solution to Exercise 10.17 can be found here.

Exercise 10.18: F4.

Let A be an integral domain.

(a) (2 points) If A is a principal ideal domain, show that A is Noetherian.

(b) (3 points) Prove that the domain A is Artinian if and only if it is a field

A solution to Exercise 10.18 can be found here.

Exercise 10.19: F5.

Let V be a vector space over a field K, and let $T\colon V \to V$ be a K-linear map.

(a) (3 points) If $\dim_K(V) = 3$, show that T is determined up to conjugacy by its characteristic polynomial $p_T(x)$ and its minimal polynomial $m_T(x)$.

(b) (2 points) Show by an example that when $\dim_K(V) = 4$, $p_T(x)$ and $m_T(x)$ do not in general suffice to determine T up to conjugacy. Include in your solution matrix representatives of the non-conjugate transformations you exhibit.

A solution to Exercise 10.19 can be found here.

11 Proofs

Proof of Proposition 1.6. Let $x = a + bi + cj + dk \in \mathbb{H} \smallsetminus \{0\}$, where $a, b, c, d \in \mathbb{H}$ are not all zero. Set $\overline{x} = a - bi - cj - dk$. One can compute that $x \cdot \overline{x} = a^2 + b^2 + c^2 + d^2$, so since $x \neq 0$ we see $x \cdot \overline{x}$ is an element of $\mathbb{R} \smallsetminus \{0\}$, that is, is a nonzero real number. Thus

$$x \cdot \left(\frac{1}{a^2 + b^2 + c^2 + d^2} \cdot \overline{x} \right) = 1,$$

so x has a right inverse, and the same argument works for the left inverse. Thus $\mathbb{H}$ is a division ring. □

Proof of Proposition 1.12. If n is composite so that $n = ab$ for $a, b \neq 1$, then

$$(a \pmod{n})(b \pmod{n}) \equiv ab \pmod{n} \equiv 0 \pmod{n}.$$

Conversely, if n is prime, $ab \equiv 0 \pmod{p}$, then $p \mid ab$, so $p \mid a$ or $p \mid b$, and hence $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. □

Proof of Theorem 1.22. Define $\varphi_\alpha \colon R[G] \to A$ by $\sum_{g \in G} x_g[g] \mapsto \sum \varphi(x_g)\alpha(g)$. Showing this is the desired map is left as an easy check. □

Proof of Theorem 1.30. We first show (i). It is immediate from the definition of an ideal that $I \cap J$ is an ideal of R. If $z \in I + J$ then $z = x + y$ for some $x \in I$, $y \in J$, so $rz = rx + ry \in I + J$.

For the chain of inclusions in (ii), we only show the first. If $\sum_{i=1}^n x_i y_i \in I \cdot J$ with $x_i \in I, y_i \in J$, since $x_i \in I$ and I is an ideal, $x_i y_i \in I$, so $\sum_{i=1}^n x_i y_i \in I$; likewise, $\sum_{i=1}^n x_i y_i \in J$. □

Proof of Theorem 1.32. We need to check that this operation is well-defined, that is, given $a, a', b, b' \in R$, if $a + I = a' + I$ and $b + I = b' + I$, then $ab + I = a'b' + I$. To see this, note that $a' = a + x$ and $b' = b + y$ for some $x, y \in I$, so

$$a'b' = (a + x)(b + y) = ab + \underbrace{\overbrace{ay}^{\in I} + \overbrace{xb}^{\in I} + \overbrace{xy}^{\in I}}_{\in I} \in ab + I,$$

so $a'b' + I = ab + I$. Thus $\cdot$ is well-defined. As $\cdot$ is associative with identity 1, $1 + I$ is the identity. Therefore, we have made R/I into a ring under $+$ and $\cdot$. □

Proof of Theorem 1.44. We already know that $\overline{\varphi}$ exists as a homomorphism of the underlying additive abelian groups and induces a group isomorphism $A/\ker\varphi \xrightarrow{\cong} \operatorname{im}\varphi$, so it remains to show $\overline{\varphi}$ is a ring homomorphism, that is, that

(1) $\overline{\varphi}(1 + I) = 1$,

(2) $\overline{\varphi}((a + I)(b + I)) = \overline{\varphi}(a + I) \cdot \overline{\varphi}(b + I)$.

For (1), we have $\overline{\varphi}(1 + I) = \overline{\varphi}(\pi(1)) = \varphi(1) = 1$, and for (2), we have

$$\overline{\varphi}(a + I) \cdot (b + I) = \overline{\varphi}(\pi(a) \cdot \pi(b)) = \overline{\varphi}(\pi(ab)) = \varphi(a) \cdot \varphi(b)$$

$$= \overline{\varphi}(\pi(a)) \cdot \overline{\varphi}(\pi(b)) = \overline{\varphi}(a + I) \cdot \overline{\varphi}(b + I).$$

Thus $\overline{\varphi}$ is a ring homomorphism. Since $\overline{\varphi}$ is a bijection of sets, we conclude by a previous result that $\overline{\varphi}$ is a ring isomorphism. Showing $A/\ker\varphi \overset{\cong}{\to} \operatorname{im}\varphi$ is an isomorphism is left as an easy exercise. □

Proof of Theorem 1.45. This is a modification of the analogous theorem from group theory, and the details are left as an exercise. □

Proof of Theorem 1.46. This is a modification of the analogous theorem from group theory, and the details are left as an exercise. □

Proof of Theorem 1.59. This is left as an easy exercise. □

Proof of Theorem 1.61. Let I be any subset of A that generates A over $\mathbb{Z}$, that is, $A = \varphi(\mathbb{Z})[I]$, where $\varphi\colon \mathbb{Z} \to A$ is the canonical ring homomorphism. ($I = A$ works, but this is excessive.) Then by the universal mapping property of polynomial rings, there exists a unique ring homomorphism $\Phi\colon \mathbb{Z}[\{X_i\}_{\in I}] \to A$ determined by $X_i \mapsto i$. Since $A = \varphi(\mathbb{Z})[I]$, Φ is surjective, and hence induces an isomorphism

$$\mathbb{Z}[\{X_i\}_{i\in I}]/\ker\Phi \xrightarrow{\cong} A.$$ □

Proof of Theorem 2.31. Suppose $0 \longrightarrow M \xrightarrow{f} N \xrightarrow{g} P \longrightarrow 0$ is trivial via $\varphi\colon N \to M \oplus P$. Define $s\colon P \to N$ by

$$s(p) = \varphi^{-1}((0, p)).$$

This is a section of g, since $g \circ s(p) = g \circ \varphi^{-1}((0, p)) = \varphi_P((0, p)) = P$.

Conversely, assume g has a section $s\colon P \to N$, that is, the sequence is split. We want to show there exists a commutative diagram of the form

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "f"] \arrow[d, equal] & N \arrow[r, "g"] & P \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & M \arrow[r, hook, "\alpha_M"'] & M \oplus P \arrow[r, two heads, "\pi_P"'] \arrow[u, "\psi"', "\cong"] & P \arrow[r] & 0
\end{tikzcd}$$

for some isomorphism ψ. Define $\psi\colon M \oplus P \to N$ by $\psi(m, p) = f(m) + s(p)$. Remark: This is the canonical ψ induced by f and s from the universal mapping property of the direct sum.

The diagram commutes, since

$$g \circ \psi(m, p) = g(f(m) + s(p)) = \cancelto{0}{g(f(m))} + g(s(p)) = p = \pi_P(m, p)$$

(where we used that $\ker g = \operatorname{im} f$), so $g \circ s = \mathrm{id}_P$, meaning the right square commutes. And the left square commutes, since $\psi(\alpha(m)) = \psi(m, 0) = f(m)$.

To see ψ is an isomorphism, we note the following.

- ψ is injective: if for some $(m, p) \in M \oplus P$ is in the kernel, then

$$0 = \psi(m, p) = f(m) + s(p).$$

Applying g, we conclude $p = 0$. Thus $f(m) = 0$. But f is injective, so $m = 0$. Thus ψ is injective.

- ψ is surjective: Let $n \in N$ and set $n' = n - s(g(n))$. Then $g'(n') = g(n) - \underbrace{g(s}_{=\mathrm{id}}(g(n))) = g(n) - g(n) = 0$, so $n' \in \ker g$, which by exactness means $n' \in \operatorname{im} f$. Thus there exists $\min nM$ such that $f(m) = n' = n - s(g(n))$, that is,
$$n = f(m) + s(g(n)) = \psi(m, g(n)) \in \operatorname{im}(\psi).$$
So ψ is also surjective, and hence an isomorphism of R-modules. (We do not need to prove that ψ is a homomorphism of R-modules, since by the remark in this proof just above, ψ is a map from a certain universal mapping property, which we already know to be an R-module homomorphism). □

Solution to Exercise 2.37. (a) Suppose $x, x' \in \sqrt{I}$ and $a \in A$. Then there exists positive integers n, n' such that $x^n, x^{n'} \in I$. Let $N = \max\{n, m\}$. Since A is commutative, we can write
$$(ax + x')^{2N} = \sum\nolimits_{j=0}^{2N} (ax)^j (x')^{2N-j} = \sum\nolimits_{j=1}^{N} (ax)^j \underbrace{(x')^{2N-j}}_{\substack{\in I \text{ for all} \\ N+1 \leqslant j \leqslant 2N}} + \sum\nolimits_{j=N+1}^{2N} \underbrace{(ax)^j}_{\substack{\in I \text{ for all} \\ 0 \leqslant j \leqslant N}} (x')^{2N-j}$$
which is a sum of elements of I. Since I is an ideal and thus closed under addition, we conclude $(ax + x')^{2N} \in I$. Thus $(ax + x') \in \sqrt{I}$, so $\sqrt{I}$ is an ideal of A.

(b) Since
$$x \in \sqrt{I} \quad \Longrightarrow \quad x^n \in \sqrt{I} \;\; (\text{where } n = 1) \quad \Longrightarrow \quad x \in \sqrt{I},$$
we have $\sqrt{I} \subset \sqrt{\sqrt{I}}$. Conversely, suppose $x \in \sqrt{\sqrt{I}}$. Then $x^n \in \sqrt{I}$ for some integer $n \in \mathbb{Z}_{\geqslant 1}$, which means $(x^n)^{n'} \in I$ for some integer $n' \geqslant 1$. Thus $x^N \in I$ for some integer $N \in \mathbb{Z}_{\geqslant 1}$, namely $N = nn'$. Hence $\sqrt{\sqrt{I}} \subset \sqrt{I}$, so we conclude $\sqrt{\sqrt{I}} = \sqrt{I}$.

(c) First note that for any (possibly noncommutative) ring R,
$$\sqrt{(0)} = \{x \in R \mid x^n \in (0) \text{ for some integer } n \in \mathbb{Z}_{\geqslant 1}\} = \{x \in R \mid x \text{ is nilpotent}\},$$
so the nilradical of R is the collection of nilpotent elements of R. Consider the ring $R = M_2(\mathbb{R})$, and consider the elements $r, x \in R$ given by $r = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $x = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$. Then $x \in \sqrt{(0)}$, but $rx = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. But for all $n \in \mathbb{Z}_{\geqslant 1}$, we have $(rx)^n = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right)^n = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 1 \end{smallmatrix}\right) \neq \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$. Hence $rx \notin \sqrt{(0)}$, so $\sqrt{(0)}$ is not an ideal of R. □

Solution to Exercise 2.38. We first prove some useful auxiliary lemmas.

Lemma 11.1.

If A is an integral domain, then A is reduced.

Lemma 11.2.

If A is an integral domain and I is an ideal of A, then collection of nilpotent elements of A/I is $\pi(\sqrt{I})$, where $\pi \colon A \twoheadrightarrow A/I$ is the natural quotient map.

Lemma 11.3.

If A is an integral domain and I is an ideal of A, then A/I is an integral domain if and only if I is a prime ideal.

Lemma 11.4.

If A is an integral domain, then the univariate polynomial ring $A[x]$ is an integral domain.

Proof of Lemma 11.1. If A were not reduced, then there exists some nonzero nilpotent element $x \in A$ and an integer $n \in \mathbb{Z}_{\geqslant 1}$ such that $x^n = 0$. Since $x^1 = x \neq 0$, $n \in \mathbb{Z}_{\geqslant 2}$. But then $0 = x^n = x \cdot x^{n-1}$, so x is a zero divisor, contradicting A is an integral domain. □

Proof of Lemma 11.2. We need to show $\pi(\sqrt{I}) = \sqrt{(\overline{0})}$, where $\overline{0}$ denotes the additive identity in A/I. If $\overline{a} \in \pi(\sqrt{I})$, then since π is surjective there exists $a \in \sqrt{I}$ such that $\pi(a) = \overline{a}$. Thus $a^n = 0$ for some integer $n \in \mathbb{Z}_{\geqslant 1}$, so $\overline{a}^n = \pi(a)^n = \pi(a^n) = \pi(0) = \overline{0}$. Thus $\pi(\sqrt{I}) \subset \sqrt{(\overline{0})}$.

Conversely, suppose $\overline{x} \in A/I$ is an element of $\sqrt{(\overline{0})}$. Then $\overline{x}^n = \overline{0}$ for some integer $n \in \mathbb{Z}_{\geqslant 1}$. But $\overline{x} = \pi(x)$ for some $x \in A$, so $\overline{0} = \overline{x}^n = \pi(x)^n = \pi(x^n)$, so $x^n \in \ker \pi = I$. Thus $x \in \sqrt{I}$, so $\overline{x} = \pi(x) \in \pi(\sqrt{I})$. It follows that $\sqrt{(\overline{0})} \subset \pi(\sqrt{I})$, and hence $\sqrt{\overline{0}} = \pi(\sqrt{I})$. □

Proof of Lemma 11.4. Let $f(x), g(x) \in A[x]$ be nonzero and suppose $f(x)g(x) = 0$. We claim either $f(x) = 0$ or $g(x) = 0$. We can write

$$f(x) = \sum\nolimits_{i=0}^{m} a_i x^i \qquad \text{and} \qquad g(x) = \sum\nolimits_{i=0}^{n} b_i x^i,$$

where $a_i, b_i \in A$ for all $i \in \{0, \ldots, m\}$ and all $j \in \{0, \ldots, n\}$, and where $a_m, b_n \neq 0$. Then

$$f(x)g(x) = \left(\sum\nolimits_{i=0}^{m} a_i x^i\right) \cdot \left(\sum\nolimits_{j=0}^{n} b_j x^j\right) = \sum\nolimits_{k=0}^{m+n} \left(\sum\nolimits_{i+j=k} a_i b_j\right) x^k,$$

so $f(x)g(x) = 0$ if and only if

$$\sum\nolimits_{i+j=k} a_i b_j = 0 \text{ for all } k \in \{0, \ldots, m+n\}.$$

If we consider the case $k = m+n$, we obtain $a_m b_n = \sum_{i+j=m+n} a_i b_j = 0$, so either $a_m = 0$ or $b_n = 0$, a contradiction. □

We can now begin Exercise 7.2. First note $\mathbb{C}$ and $\mathbb{Z}$ are integral domains, so by Lemma 11.4, $\mathbb{C}[x]$ and $\mathbb{Z}[x]$ are integral domains.

We will use the following notation. Write $\overline{x}$ to mean the image $\pi(x)$ of x under the natural quotient map $\pi\colon A[x] \twoheadrightarrow A[x]/I$, where A, I are given in each part. Since π is surjective, we can write any element of the quotient ring as $\overline{f}$ for some $f(x) \in A[x]$. Note that since π is a ring homomorphism, for all $a, b \in \mathbb{Z}[x]$, we can write $\overline{a+b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a}\overline{b}$.

(a) We claim $\mathbb{C}[x]/(x^2+1)$ has zero divisors but is reduced. To see $\mathbb{C}[x]/(x^2+1)$ has zero divisors, by Lemma 11.3 it suffices to show (x^2+1) is not prime in $\mathbb{C}[x]$. And indeed, $x^2+1 = (x+i)(x-i)$, but neither $x+i$ nor $x-i$ are not elements of (x^2+1) (because, for example, if $f(x) \in (x^2+1)$ is nonzero then $\deg(f) \geqslant 2$). Thus (x^2+1) is not prime in $\mathbb{C}[x]/(x^2+1)$, so $\mathbb{C}[x]/(x^2+1)$ has zero divisors.

To see $\mathbb{C}[x]/(x^2+1)$ is reduced, by Lemma 11.2 it suffices to show $\pi(\sqrt{(x^2+1)}) = (\overline{0})$, or equivalently that $\sqrt{(x^2+1)} = (x^2+1)$. In other words, we claim (x^2+1) equals its own radical in $\mathbb{Z}[i]$. More generally, for any commutative ring A, a **radical ideal** of A is any ideal I of A such that $\sqrt{I} = I$.

To see (x^2+1) is radical, note that if this were false, then there exists some nonzero $f(x) \in \mathbb{C}[x]$ not divisible by (x^2+1) and an integer $n \in \mathbb{Z}_{\geqslant 2}$ such that $f(x)^n = 0$. But this contradicts the fact $\mathbb{C}[x]$ has no zero divisors. Hence $\sqrt{(x^2+1)} = (x^2+1)$, so $\pi(\sqrt{(x^2+1)}) = \pi((x^2+1)) = (\overline{0})$, as desired.

(b) We claim $\mathbb{Z}[x]/(x^2+1)$ has no zero divisors and is reduced. We will first assume $\mathbb{Z}[x]/(x^2+1)$ is isomorphic to the Gaussian integers $\mathbb{Z}[i]$ as rings, and then return to prove this after showing it implies the claim. By Lemma 11.1, it suffices to show $\mathbb{Z}[i]$ is an integral domain. And indeed, if $z_1, z_2 \in \mathbb{Z}[i]$ are nonzero and have complex polar coordinates $z_1 = r_1 e^{i\theta_1}, z_2 = r_2 e^{i\theta_2}$, then $z_1 z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}$ is also nonzero, as desired.

It only remains to show $\mathbb{C}[x]/(x^2+1) \cong \mathbb{Z}[i]$ as rings. Define $\mathrm{ev}_i \colon \mathbb{Z}[x] \to \mathbb{Z}[i]$ by $f(x) \mapsto f(i)$. Then ev_i is a well-defined map $\mathbb{Z}[x]$ into $\mathbb{Z}[i]$ and satisfies $\mathrm{ev}_i(1) = 1$, $\mathrm{ev}_i(f(x))\,\mathrm{ev}_i(g(x)) = f(i)g(i) = \mathrm{ev}_i(f(x)g(x))$, and $\mathrm{ev}_i(f(x)+g(x)) = f(i)+g(i) = \mathrm{ev}_i(f(x)) + \mathrm{ev}_i(g(x))$, so ev_i is a ring homomorphism. It is surjective, since any $a+bi \in \mathbb{Z}[i]$ is the image of $a+bx \in \mathbb{Z}[x]$. It remains to show $\ker \mathrm{ev}_i = (x^2+1)$. Certainly $(x^2+1) \subset \ker \mathrm{ev}_i$, since $\mathrm{ev}_i(f(x)(x^2+1)) = \mathrm{ev}_i(f(x))\,\mathrm{ev}_i(x^2+1) = f(i)(i^2+1) = 0$. Conversely, if $f(x) = \sum_{j=0}^n a_j x^j \in \ker \mathrm{ev}_i$, then $f(i) = 0$. And since ev_i is a ring homomorphism, we can write $\mathrm{ev}_i(f(-x)) = \sum_{j=0}^n a_j\,\mathrm{ev}_i(-x) = -\sum_{j=0}^n a_j\,\mathrm{ev}_i(x) = -f(i) = 0$. Now $f(i) = f(-i) = 0$, so $(x-i)$ and $(x+i)$ divide $f(x)$ when f is identified as a polynomial in $\mathbb{C}[x]$. Thus $f(x) \in (x^2+1)$, so $\ker \mathrm{ev}_i \subset (x^2+1)$, as desired.

(c) We claim $\mathbb{Z}[x]/(3, x^2+1)$ has no zero divisors and is reduced. Recall from recitation that if R is any commutative ring and $a, b \in R$, then by the second isomorphism theorem,

$$\frac{R}{(a,b)R} \cong \frac{R/aR}{(a,b)R/aR} \cong \frac{R/aR}{bR/aR} \cong \frac{R}{bR}.$$

It follows that

$$\frac{\mathbb{Z}[x]}{(3, x^2+1)} \cong \frac{\mathbb{Z}[x]/(x^2+1)}{(3)} \cong \mathbb{Z}[i]/(3),$$

where the second isomorphism is by part (b). We also showed in part (b) that $\mathbb{Z}[i]$ is an integral domain, so by Lemmas 11.1 and 11.3 it is enough to know (3) is a prime ideal of $\mathbb{Z}[i]$. Suppose $3 = \alpha\beta$ for some $\alpha, \beta \in \mathbb{Z}[i]$. Multiplying both sides by their complex conjugate, we obtain $9 = \alpha\overline{\alpha}\beta\overline{\beta} = (\alpha_1^2+\alpha_2^2)(\beta_1^2+\beta_2^2)$. Thus $(\alpha_1^2+\alpha_2^2), (\beta_1^2+\beta_2^2) \in \{1, 3, 9\}$. And $\alpha_1^2+\alpha_2^2 \neq 3$, since no integers x, y satisfy $x^2+y^2 = 3$. Similarly, $\beta_1^2+\beta_2^2 \neq 3$. Then without loss of generality $\beta_1^2+\beta_2^2 = 1$, so β must be a unit, meaning (3) is prime. Thus (3) is prime in $\mathbb{Z}[i]$.

(d) We claim $\mathbb{Z}[x]/(2, x^2+1)$ has zero divisors and is non-reduced. Since $2, x^2+1 \in (2, x^2+1)$, we have $\overline{x^2+1} = 0$ and $\overline{2} = \overline{0}$. Then $\overline{1} = \overline{-1}$, so

$$\overline{0} = \overline{x^2+1} = \overline{x}^2 + \overline{1} = \overline{x}^2 - \overline{1} = \overline{x^2-1} = \overline{(x+1)(x-1)}$$

$$= \overline{x+1} \cdot (\overline{x} - \overline{1}) = \overline{x+1} \cdot (\overline{x} + \overline{1})(\overline{x+1}) = (\overline{x+1})^2.$$

Since $\overline{x+1} \neq 0$, it follows that $\mathbb{C}[x]/(2, x^2+1)$ is non-reduced, and hence by Lemma 11.1 has zero divisors. □

Solution to Exercise 2.39. (a) Suppose $a \in A$ and $x \in (I : J)$. Then

$$\begin{aligned}
(ax)J &= \{(ax)y \mid y \in J\} && \text{(by definition of } (ax)J\text{)}\\
&= \{(xa)y \mid y \in J\} && \text{(since } A \text{ is commutative)}\\
&= \{x(ay) \mid y \in J\} && \text{(since multiplication is associative)}\\
&\subset \{xy' \mid y' \in J\} && \text{(since } y' \coloneqq ay \in J \text{ whenever } a \in A, y \in J\text{)}\\
&= xJ. && \text{(by definition of } xJ\text{)}
\end{aligned}$$

Thus $ax \in (I : J)$. Since $a \in A$ and $x \in (I : J)$ were arbitrary, we conclude $(I : J)$ is an ideal of A.

(b) Let $m, n \in \mathbb{Z}$ be given.

- Case 1: $n, m \in \mathbb{Z}$ *and* $m = 0$. Given an arbitrary $x \in \mathbb{Z}$, we have

$$x \in ((n) : (0)) \iff x(0) = \{x \cdot 0\} = \{0\} \subset (n)$$

which is always true. Thus $((n) : (0)) = \mathbb{Z}$.

- Case 2: $n, m \in \mathbb{Z}$, *and* $m \neq 0$. Given an arbitrary $x \in \mathbb{Z}$, we have

$$\begin{aligned}
x \in ((0) : (m)) &\iff x(m) = \{xmk \mid k \in \mathbb{Z}\} = (xm) \subset (0)\\
&\iff \text{for all } k \in \mathbb{Z},\ kxm = 0\\
&\iff xm = 0 \iff x = 0,
\end{aligned}$$

where the last equivalence is because $\mathbb{Z}$ is an integral domain and $m \neq 0$ by assumption. Thus $((0) : (m)) = (0)$.

- Case 3: $n, m \in \mathbb{Z}$ *and* $m, n \neq 0$. Given an arbitrary $x \in \mathbb{Z}$, we have

$$\begin{aligned}
x \in ((n) : (m)) &\iff x(m) = \{kxm \mid k \in \mathbb{Z}\} = (xm) \subset (n)\\
&\iff n \text{ divides } xm\\
&\iff \frac{n}{\gcd(n,m)} \text{ divides } \frac{xm}{\gcd(n,m)}\\
&\iff \frac{n}{\gcd(n,m)} \text{ divides } x\\
&\iff x \in \left(\frac{n}{\gcd(n,m)}\right),
\end{aligned}$$

where the penultimate equivalence is because $n/\gcd(n,m)$ and $m/\gcd(n,m)$ are always coprime, meaning $n/\gcd(n,m)$ dividing $x(m/\gcd(n,m))$ is equivalent to $n/\gcd(n,m)$ dividing x.

We conclude

$$((n) : (m)) = \begin{cases} \left(\dfrac{n}{\gcd(n,m)}\right) & \text{if } n, m \neq 0,\\ (0) & \text{if } n = 0 \text{ and } m \neq 0,\\ \mathbb{Z} & \text{if } m = 0. \end{cases}$$ □

Solution to Exercise 2.40. We first prove two auxiliary lemmas, and then argue that together these imply the statement of Exercise 7.4.

Lemma 11.5.

Any division ring is a simple ring.

Lemma 11.6.

Let R be any (possibly noncommutative) ring and let n be a positive integer. Then every two-sided ideal J of $M_n(R)$ takes the form

$$J = M_n(I) \coloneqq \{A \in M_n(R) \mid a_{ij} \in I \text{ for all } i, j \in \{1, \dots, n\}\},$$

where I is a two-sided ideal of R.

Proof of Lemma 11.5. Let D be a division ring and suppose I is a (two-sided) ideal of D. If $I = (0)$ then we are done, so assume $I \neq (0)$. Then there exists some nonzero $x \in D$ such that $x \in I$. Then x is a unit in D, since $D^\times = D \setminus \{0\}$. Thus there exists some $x^{-1} \in D$ such that $x^{-1}x = 1$. But $x \in I$, so $1 = x^{-1}x \in I$ since I is an ideal. But then

$$D = D \cdot \underbrace{1}_{\in I} \subset I,$$

forcing $I = D$. Since I was an arbitrary ideal of D, we conclude D is simple. □

Proof of Lemma 11.6. Let J be an ideal of $M_n(R)$ and let E_{ij} be the n-by-n matrix whose (k, ℓ) entry is $\delta_{ki}\delta_{j\ell}$ for all $k, \ell \in \{1, \dots, n\}$. Then $I = \{r \in R \mid rE_{1,1} \in J\}$ is an ideal of R, since if $r \in R$ and $x \in I$, then $rx \in I$ (resp. $xr \in I$) because $(rE_{1,1})(xE_{1,1}) = rxE_{1,1} \in J$ (resp. $(xE_{1,1})(rE_{1,1}) = xrE_{1,1} \in J$).

- $J \subset M_n(I)$: If $A = (a_{ij}) \in J$, then because J is an ideal of $M_n(R)$ and we have the identity
$$a_{ij}E_{1,1} = E_{1j}AE_{j1} \in J,$$
we have $a_{ij} \in I$. Hence $J \subset M_n(I)$.
- $M_n(I) \subset J$: If $x \in I$, then $(xI)E_{1,1} = xE_{1,1} \in J$ since J is an ideal of $M_n(R)$, which implies
$$xE_{ij} = E_{i1}(xE_{1,1})E_{1j} \in J,$$
so because $xE_{1,1} \subset J$ and J is a two-sided ideal, we conclude $xE_{i,j} \in J$ for all $x \in I$. But here i and j were arbitrary indices in $\{1, \dots, n\}$, so since any matrix $A = (a_{ij})$ can be written as $A = \sum_{i,j=1}^n a_{ij}E_{ij}$, we conclude $M_n(I) \subset J$.

Hence $J = M_n(I)$. Since J was an arbitrary ideal of $M_n(R)$, any ideal of $M_n(R)$ takes the form $M_n(I)$ for some ideal I of R. □

We can now prove the statement of Exercise 7.4. Let D be a division ring. By Lemma 11.5, any (two-sided) ideal J of $M_n(D)$ takes the form $M_n(I)$, which denotes the collection of

n-by-n matrices whose entries are elements of I. By Lemma 11.6 this implies the result, since then the only two-sided ideals of $M_n(D)$ are $M_n(D)$ and $M_n((0)) = (0)$. □

Solution to Exercise 2.41. (a) Let M be a left R-module and consider the map

$$\begin{aligned} \lambda\colon R &\longrightarrow \mathrm{End}_{\mathsf{Grp}}(M), \\ r &\longmapsto (m \mapsto \lambda(r)(m) \coloneqq r \cdot m). \end{aligned}$$

Then for any $m_1, m_2 \in M$ and any $r \in R$,

$$\lambda(r)(m_1 + m_2) = r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2 = \lambda(r)(m_1) + \lambda(r)(m_2) \in \mathrm{End}_{\mathsf{Grp}}(M),$$

so λ is a well-defined homomorphism of the underlying abelian groups $R \to \mathrm{End}_{\mathsf{Grp}}(M)$. For any $m \in M$ and any $r_1, r_2, r_3 \in R$, we have $\lambda(1)(m) = 1 \cdot m = m = \mathrm{id}_M(m)$, where $\mathrm{id}_M\colon M \to M$ is the identity group homomorphism $M \to M$, and

$$\begin{aligned} \lambda(r_1r_2 + r_3)(m) &= (r_1r_2 + r_3) \cdot m = r_1 \cdot (r_2 \cdot m) + r_3 \cdot m \\ &= \lambda(r_1)(\lambda(r_2)(m)) + \lambda(r_3)(m) = (\lambda(r_1) \circ \lambda(r_2) + \lambda(r_3))(m). \end{aligned}$$

Since m was arbitrary, we conclude $\lambda(1) = \mathrm{id}_M$ and $\lambda(r_1r_2 + r_3) = \lambda(r_1) \circ \lambda(r_2) + \lambda(r_3)$. Thus λ is a ring homomorphism.

Conversely, let M be an abelian group and suppose $\lambda\colon R \to \mathrm{End}_{\mathsf{Grp}}(M)$ is a ring homomorphism. Then consider the map

$$\begin{aligned} R \times M &\longrightarrow M, \\ (r, m) &\longmapsto r \cdot_\lambda m = \lambda(r)(m). \end{aligned}$$

Then $1 \cdot_\lambda m = \lambda(1)(m) = (m) = 0$, and for all $r_1, r_2, r_3 \in R$ and all $m_1, m_2 \in M$ we can write

$$\begin{aligned} (r_1r_2 + r_3) \cdot_\lambda (m_1 + m_2) &= \lambda(r_1r_2 + r_3)(m_1 + m_2) \\ &= \lambda(r_1)(\lambda(r_2)(m_1) + \lambda(r_2)(m_2)) + \lambda(r_3)(m_1) + \lambda(r_3)(m_2) \\ &= r_1 \cdot_\lambda (r_2 \cdot_\lambda m_1) + r_1 \cdot_\lambda (r_2 \cdot_\lambda m_2) + r_3 \cdot_\lambda m_1 + r_3 \cdot_\lambda m_3, \end{aligned}$$

so this defines a valid left module action.

The two above procedures are inverses of each other in the following sense.

- Given a ring homomorphism $\lambda\colon R \to \mathrm{End}_{\mathsf{Grp}}(M)$, we obtain a left action $\cdot_\lambda$, and applying the other procedure to this gives the ring homomorphism $R \to \mathrm{End}_{\mathsf{Grp}}(M)$ given by $\lambda(r)(m) = r \cdot_\lambda m$, which is what we started with.
- Conversely, given a left action $\cdot$ and an abelian group M, we obtain a ring homomorphism $\lambda\colon R \to \mathrm{End}_{\mathsf{Grp}}(M)$ given by $\lambda(r)(m) = r \cdot m$, and applying the other procedure to this gives the left action $\cdot_\lambda$ given by $r \cdot_\lambda m = \lambda(r)(m) = r \cdot m$, which is exactly what we started with.

We conclude that if R is a ring and M is any abelian group, then there is a bijective correspondence

$$\begin{aligned} \{\text{left actions } R \times M \to M\} &\longleftrightarrow \mathrm{End}_{\mathsf{Grp}}(M), \\ ((r, m) \mapsto r \cdot m) &\longmapsto (\lambda_r\colon m \mapsto r \cdot m), \\ ((r, m) \mapsto \lambda(r)(m)) &\longleftarrow\!\shortmid \lambda. \end{aligned}$$

(b) We are given $(R^{\text{op}}, +) = (R, +)$, which is an abelian group because R is a ring. It only remains to show $(R^{\text{op}}, \cdot_{\text{op}})$ is a monoid. The identity of $(R^{\text{op}}, \cdot_{\text{op}})$ is the same identity 1 as $(R, \cdot)$, because for all $r \in R$,

$$r \cdot_{\text{op}} 1 = 1 \cdot r = r \cdot 1 = 1 \cdot_{\text{op}} r.$$

Multiplication in $(R, \cdot_{\text{op}})$ is associative, because for all $r_1, r_2, r_3 \in R$,

$$\begin{aligned} r_1 \cdot_{\text{op}} (r_2 \cdot_{\text{op}} r_3) &= (r_2 \cdot_{\text{op}} r_3) \cdot r_1 = (r_3 \cdot r_2) \cdot r_1 \\ &= r_3 \cdot (r_2 \cdot r_1) = (r_2 \cdot r_1) \cdot_{\text{op}} r_3 = (r_1 \cdot_{\text{op}} r_2) \cdot_{\text{op}} r_3. \end{aligned}$$

Hence $(R, \cdot_{\text{op}})$ is a monoid, so R^{op} is a ring.

(c) Let N be a right R-module. Define

$$\begin{aligned} \rho \colon R^{\text{op}} &\longrightarrow \operatorname{End}_{\mathsf{Grp}}(N), \\ r &\longmapsto n \cdot r. \end{aligned}$$

First note that ρ indeed maps R^{op} into $\operatorname{End}_{\mathsf{Grp}}(N)$, because for any $r \in R^{\text{op}}$,

$$\rho(r)(n_1 + n_2) = (n_1 + n_2) \cdot r = n_1 \cdot r + n_2 \cdot r = \rho(r)(n_1) + \rho(r)(n_2),$$

so $\rho(r) \in \operatorname{End}_{\mathsf{Grp}}(N)$. To see ρ is a ring homomorphism, note that for any $r \in R^{\text{op}}$ and any $m \in M$, we have

$$\rho(1)(n) = n \cdot 1 = n = \operatorname{id}_N(n),$$

where $\operatorname{id}_N \colon N \to N$ is the identity homomorphism $n \mapsto n$. And for all $r_1, r_2, r_3 \in R$ and all $m \in M$, we have

$$\begin{aligned} \rho(r_1 \cdot_{\text{op}} r_2 + r_3)(m) &= m \cdot (r_1 \cdot_{\text{op}} r_2 + r_3) = (m \cdot r_2) \cdot r_1 + m \cdot r_3 \\ &= \rho(r_1)(\rho(r_2)(m)) + \rho(r_3)(m) = (\rho(r_1) \circ \rho(r_2) + \rho(r_3))(m). \end{aligned}$$

Since n was an arbitrary element of N, we conclude

$$\rho(1) = \operatorname{id}_N \text{ and } \rho(r_1 \cdot_{\text{op}} r_2 + r_3) = \rho(r_1) \circ \rho(r_2) + \rho(r_3).$$

Hence ρ is a ring homomorphism.

Conversely, suppose N is an abelian group and $\rho \colon R^{\text{op}} \to \operatorname{End}_{\mathsf{Grp}}(N)$ is a ring homomorphism. Define a right action on N by

$$\begin{aligned} N \times R &\longrightarrow N, \\ (n, r) &\longmapsto m \cdot_\rho r = \rho(r)(m). \end{aligned}$$

This is a right action because

- $0 \cdot_\lambda m = \lambda(0)(m) = \mathbf{0}(m) = 0$, where $\mathbf{0}$ denotes the zero homomorphism $M \to M$ given by $m \mapsto 0$, and
- for all $r_1, r_2, r_3 \in R$ and all $m_1, m_2 \in M$,

$$\begin{aligned} (n_1 + n_2) \cdot_\rho (r_1 \cdot_{\text{op}} r_2 + r_3) &= \rho(r_1 \cdot_{\text{op}} r_2 + r_3)(n_1 + n_2) \\ &= \rho(r_1)(\rho(r_2)(n_1 + n_2)) + \rho(r_3)(n_1 + n_2) \\ &= \rho(r_1)(\rho(r_2)(n_1) + \rho(r_2)(n_2)) + \rho(r_3)(n_1) + \rho(r_3)(n_2) \\ &= \rho(r_1)(\rho(r_2)(n_1)) + \rho(r_1)(\rho(r_2)(n_2)) + \rho(r_3)(n_1) + \rho(r_3)(n_2) \\ &= (n_1 \cdot_\rho r_2) \cdot_\rho r_1 + (n_2 \cdot_\rho r_2) \cdot_\rho r_1 + n_1 \cdot_\rho r_3 + n_3 \cdot_\rho r_3. \end{aligned}$$

These procedures are inverses of each other in the following sense.

- Given a ring homomorphism $\rho\colon R^{\mathrm{op}} \to \mathrm{End}_{\mathsf{Grp}}(N)$, we obtain a right action $\cdot_\rho$, and applying the other procedure to this gives the ring homomorphism $R^{\mathrm{op}} \to \mathrm{End}_{\mathsf{Grp}}(N)$ given by $n \cdot_\rho r$, that is, $\rho(r)(n)$, which is what we started with.
- Conversely, given a right action $\cdot$, we obtain a ring homomorphism $\rho\colon R^{\mathrm{op}} \to \mathrm{End}_{\mathsf{Grp}}(N)$ given by $\rho(r)(n) = n \cdot r$, and applying the other procedure to this gives the right action $\cdot_\rho$ given by $n \cdot_\rho r = \rho(r)(n) = n \cdot r$, which is exactly what we started with.

We conclude there is a bijective correspondence

$$\begin{aligned} \{\text{right actions } N \times R \to N\} &\longleftrightarrow \mathrm{End}_{\mathsf{Grp}}(N), \\ ((n,r) \longmapsto n \cdot r) &\longmapsto (\rho_r\colon n \mapsto r \cdot n), \\ ((n,r) \mapsto \rho(r)(n)) &\longleftarrow \lambda. \end{aligned}$$

□

Proof of Proposition 3.3. Point (i) is left as an exercise. For point (ii), recall $I \cdot J \subset I \cap J$ always. Let $x \in I \cap J$. By assumption, there exists $a \in I$ such and $b \in J$ such that $a + b = 1$. Thus $x = (a+b)x = ax + bx \in I \cdot J$, as desired. □

Proof of Theorem 3.5. We prove the claim by induction on integers $n \in \mathbb{Z}_{\geqslant 1}$. Most of the work will be in the base case.

(1) We with the case $n = 2$. Given $x_1, x_2 \in R$ and $I_1 + I_2 = R$, write $1 = a_1 + a_2$ for $a_1 \in I_1$ and $a_2 \in I_2$. Then $1 \equiv a_1 \pmod{I_2}$ and $1 \equiv a_2 \pmod{I_2}$. Then $x \equiv a_2 x_1 \pmod{I_1} \equiv x_1 \pmod{I_1}$ and $x \equiv a_1 x_2 \pmod{I_2} \equiv x_2 \pmod{I_2}$, so this x works.

For the induction step of (1), suppose (1) holds for $(n-1)$-tuples of pairwise coprime ideals. Then given $x_1, \ldots, x_n \in R$, apply the induction hypothesis to obtain $y \in R$ such that

$$y \equiv x_j \pmod{I}_j \text{ for all } j \in \{2, \ldots, n\}.$$

Now for all $j \in \{2, \ldots, n\}$, write $1 = a_j + b_j$, where $a_j \in I_1$ and $b_j \in I_j$. (We can do this, because for all such j, I_j and I_1 are coprime by assumption.) Then

$$1 = \prod_{j=2}^{n} (a_j + b_j) \in I_1 + \prod_{j=2}^{n} I_j$$

Then

$$\begin{aligned} \prod_j (a_j + b_j) = a_2 \cdots a_n + a_2 \cdots a_{n-1} b_n &+ a_2 \cdots b_n \\ &+ a_2 \cdots b_{n-1} a_n \\ &+ \\ &\vdots \\ &+ \\ &+ b_2 b_3 \cdots b_n \end{aligned}$$

and the sum of terms in the vertical column above is an element of I_1. Thus I_1 and $\prod_{j=2} I_j$ are coprime, so by the $n = 2$ case there exists $x \in R$ such that $x \equiv x_1 \pmod{I}_1$

and $x = y \ (\mathrm{mod} \prod)_{j=2}^{n} I_j$. But this implies $x \equiv y \ (\mathrm{mod}\, I_j) \equiv x_j \ (\mathrm{mod}\, I)_j$ for all $j = 2, \dots, n$.

(2) We get a ring homomorphism $\varphi \colon R \to \prod_{j=1}^{n} R/I_j$ given by $\varphi(x) = (x + I_j)_j$. This is surjective by part (1), and

$$\ker \varphi = \{x \in R \mid x \in I_j \text{ for all } j\} = \bigcap_{j=1}^{n} I_j,$$

so φ gives an isomorphism $R \Big/ \bigcap_{j=1}^{n} I_j \xrightarrow{\cong} \prod_{j=1}^{n} R/I_j$. The last claim that $\bigcap_{j=1}^{n} I_j = \prod_{j=1}^{n} I_j$ follows inductively from the remark that $I + J = R$ implies $I \cdot J = I \cap J$, since $I_1 + \prod_{j=2}^{n} I_j = R$. □

Proof of Theorem 3.17. Suppose $I \subset R$ is prime. This is equivalent to saying that both $I \neq R$ and for all $x, y \in R$ such that $xy \in I$, we have $x \in I$ or $y \in I$. This is equivalent to saying both for all $x, y \in R/I$ such that $xy = 0$ in R/I, $x = 0$ or $y = 0$ in R/I and $R/I \neq 0$, which in turn is equivalent to R/I being an integral domain. □

Proof of Theorem 3.23. Let $I \subset R$ be maximal. This is equivalent to the only ideals ofR/I being (0) and R/I (and $0 \neq R/I$), which in turn is equivalent to saying for all $x \in R/I \smallsetminus \{0\}$, $(x) = R/I$ (and $0 \neq R/I$). And this holds if and only if $1 \in (x)$ for all $x \in R/I \smallsetminus \{0\}$ (and $0 \neq R/I$), which happens if and only if R/I is a field. This last equivalence is because saying R/I is a field is to say R/I (is nonzero) and every nonzero element has a multiplicative inverse. □

Proof of Corollary 3.24. Since fields are integral domains,

$$I \text{ maximal} \implies R/I \text{ is a field} \implies R/I \text{ is an integral domain} \implies I \text{ is prime.}$$ □

Proof of Theorem 3.27. We use Zorn's Lemma. Let $(S, \leqslant)$ be the partially ordered set

$$S = \{\text{proper ideals in } R \text{ containing } I\},$$

where $J_1 \leqslant J_2$ if and only if $J_1 \subset J_2$. Let $T = \{J_\alpha\}_{\alpha \in A}$ be a totally ordered subset of S, where A is an index set. We want to show this is bounded above by some element of S. Consider

$$K = \bigcup_{\alpha \in A} J_\alpha.$$

Certainly $J \supset J_\alpha$ for all $\alpha \in A$. We claim J is a proper ideal:

- J is an ideal: if $x, y \in J$ then $x \in Jas\alpha$ and $y \in J_\beta$ for some $\alpha, \beta \in A$. Because T is totally ordered, $J_\alpha \subset J_\beta$ or $J_\beta \subset J_\alpha$. We may assume without loss of generality that $J_\alpha \subset J_\beta$. Then $x, y \in J_\beta$, and so $x + y \in J_\beta \subset J$. Likewise, if $r \in R$ and $x \in J$, then $x \in J_\alpha$ for some $\alpha \in A$, so $x \in J_\alpha \subset J$. Thus J is indeed an ideal.
- J is a proper ideal: If $1 \in J$, then $1 \in J_\alpha$ for some $\alpha \in A$, contradicting $J_\alpha \neq R$.

Thus $J \in S$ and J is an upper bound for T. It follows that all totally ordered subsets $T \subset S$ have upper bounds in S, so by Zorn's Lemma S contains at least one maximal element. The maximal elements of S are the maximal ideals of S, containing I, so there exists at least one maximal ideal containing I. □

Proof of Proposition 3.30. Suppose (f) is prime. Then if $f = gh$ for some $\deg g, \deg h \geqslant 1$, where g, h are not a unit multiple away from f. Then $g, h \notin (f)$, so g, h are nonzero in $k[x]/(f)$. But (f) is prime, so $k[x]/(f)$ is an integral domain, meaning $fg \neq 0$ in $k[x]/(f)$. But $gh = f \in (f)$ in $k[x]$, so $gh = 0$ in $k[x]/(f)$, a contradiction. Thus f is irreducible.

For the converse we can actually show something much stronger. We will show that if f is irreducible, then (f) is maximal (and so in particular prime). Indeed, if (f) is not maximal, there exists I such that $(f) \subsetneq I \subsetneq R$. Since R is a PID (by Exercise 8.1), $I = (g)$ for some $g \in k[x]$. So $F \in (f) \subsetneq (g)$, which means $f = gh$ for some h. Then $\deg(g) \geqslant 1$, since otherwise $(g) = R$. And $\deg(h) \geqslant 1$, since otherwise $g = fh^{-1}$, so $(g) \subset (f)$. So $(g) = (f)$. So $\deg g, \deg h > 1$, so f is reducible since it factors into a product of g, h which are nonunion because $\deg(g), \deg(h) \geqslant 1$. □

Proof of Theorem 3.37. (1) We argue by induction on n. The case $n = 1$ is clear, since if J is contained in I, then J is contained in I. Now assume the result holds for fewer than n many I_js for some $n \in \mathbb{Z}_{\geqslant 2}$. If we can show $J \subset \bigcup_{j=1, j\neq k}^{n} I_k$ then we are done, since the induction hypothesis would imply J is contained in I_j for some $i \in \{1, \ldots, k-1, k+1, \ldots, n\}$. To that end, suppose for a contradiction that instead

$$J \not\subset \bigcup_{\substack{j=1 \\ j\neq k}}^{n} I_j \text{ for all } k \in \{1, \ldots, n\}.$$

Then for any fixed $k \in \{1, \ldots, n\}$, there exists $x_k \in J$ such that $x_k \notin \bigcup_{j=1, j\neq k} I_j$. Since $x_k \in J \subset \bigcup_{j=1}^{n} I_j$, this means $x_k \in I_k$.

- Suppose $n = 2$. Let $x = x_1 + x_2$. Then $x \in J$ since $x_1, x_2 \in J$, and J is closed under addition as an ideal. But $x \notin I_1 \cup I_2$, since otherwise $x \in I_1$ or $x \in I_2$, which is cannot happen: if $x = I_1$ then $x_2 = x - x_1 \in I_1$, a contradiction, and if $x = I_2$, then $x_1 = x - x_2 \in I_2$, a contradiction.
- Now suppose $n \in \mathbb{Z}_{\geqslant 3}$. At least one element of $\{I_1, I_2, I_3\}$ is prime by hypothesis, so perhaps after a relabeling we may assume I_1 is prime. Then consider

  $$x = x_1 + x_2 x_3 \cdots x_n \in J.$$

  But $x_1 \in I_1$, $x_2, \ldots, x_n \notin I_1$, and I_1 is prime, so $x_2 x_3 \cdots x_n \notin I_1$, and thus $x \notin I_1$. And for all $k \in \{2, \ldots, n\}$, $x_2 x_3 \cdots x_n \in I_k$. But $x_1 \notin I_k$, so $x \notin I_k$. But then

  $$x \notin \bigcup_{j=1}^{n} I_j = J,$$

  which contradicts our assumption $x \in J$.

(2) Suppose for a contradiction $\mathfrak{p} \not\supset I_j$ for all $k = 1, \ldots, n$. Then for all j, there exists $x_j \in I_j$ such that $x_j \notin \mathfrak{p}$. Then $x = x_1 x_2 \cdots x_n \in I_k$ for all k, since $x_k \in I_k$. But $x \notin \mathfrak{p}$ because $\mathfrak{p}$ is prime, contradicting $\mathfrak{p} \supset \bigcap_{j=1}^{n} I_j$. In the case $\mathfrak{p} = \bigcap_{i=1}^{n}$, then since $\mathfrak{p} \supset I_k$ and $\mathfrak{p} = \bigcap_{i=1}^{n} I_j \subset I_k$, we conclude $\mathfrak{p} = I_k$. □

Solution to Exercise 3.39.

(a) Suppose $a(x), b(x) \in K[x]$ and $b(x) \neq 0$. First note that if $\deg(a(x)) < \deg(b(x))$ then we can choose $q(x) = 0$, $r(x) = a(x)$, since then $a(x) = 0 = b(x) \cdot 0 + a(x) = b(x)q(x) + r(x)$

and $\deg r(x) = \deg(a(x)) < \deg(b(x))$, affirming the claim. Thus we may assume

$$\deg(a(x)) \geqslant \deg(b(x)).$$

We argue by induction on the degree of $a(x)$, which we denote by n. The case $n = 0$ forces $\deg(b(x)) = 0$, so $a(x) = c_1$ and $a(x) = c_2$ for some $c_1, c_2 \in K$. By choosing $q(x) = c_1 c_2^{-1}$ and $r(x) = 0$, we obtain $a(x) = c_1 = c_2 \cdot (c_2^{-1} c_1) + 0 = b(x)q(x) + r(x)$ and $r(x) = 0$, affirming the claim.

Now suppose $n \in \mathbb{Z}_{\geqslant 1}$ and assume the claim holds for any element of $k[x]$ with degree less than n. Where $m = \deg(b(x))$, we can write

$$b(x) = b_m x^m + \cdots + b_0 \quad \text{and} \quad a(x) = a_n x^n + \cdots + a_0,$$

where $a_n, b_m \neq 0$. Let $\lambda = a_n b_m^{-1}$. Then $a_n - \lambda b_m = 0$, so in particular

$$a(x) - \lambda x^{n-m} b(x) = \cancelto{0}{(a_n - \lambda b_m)x^n} + (a_{n-1} - \lambda b_{m-1})x^{n-1} \cdots + (a_0 - \lambda b_0)x^{n-m}$$

is an element of $K[x]$ of degree at most $n - 1$. By the induction hypothesis, there exist $q^*(x), r^*(x) \in K[x]$ such that

$$a(x) - \lambda x^{n-m} b(x) = b(x)q^*(x) + r^*(x).$$

and either $r^*(x) = 0$ or $\deg(r^*(x)) < m$. We can write this as

$$a(x) = b(x)(\lambda x^{n-m} + q^*(x)) + r^*(x),$$

so by choosing $q(x) = \lambda x^{n-m} + q^*(x)$ and $r(x) = r^*(x)$ gives us the desired polynomials. Thus the degree function (restricted to $K[x] \setminus \{0\}$) is a Euclidean valuation for $K[x]$.

(b) Let R be a Euclidean domain, let $d\colon R \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$ be a Euclidean valuation, and let I be an ideal of R. It suffices to show I is principal. If $I = (0)$ then I is principal with generator 0, so we may assume $I \neq (0)$. Then the set $D = \{d(x) \mid x \in I\}$ is a nonempty subset of $\mathbb{Z}_{\geqslant 0}$, so it contains a minimal element d_0 with respect to the standard total ordering on $\mathbb{Z}_{\geqslant 0}$. Since $d_0 \in D$, there exists $w \in I$ such that $d(w) = d_0$.

We claim $I = (w)$. It suffices to show any element in I is divisible by w, so we consider an arbitrary element $y \in I$. Since d is an Euclidean valuation, there exist $q, r \in R$ such that $y = qw + r$ and either $r = 0$ or $d(r) < d(w)$. But then

$$r = \underbrace{y}_{\in I} - \underbrace{qw}_{\in I} \in I,$$

so $d(r) \in D$. This forces $r = 0$, since otherwise $d(r) < d(w)$, contradicting minimality of $d(w)$ in D. Hence $y = qw$, so $y \in (w)$. Since y was an arbitrary element of I, we conclude I is principal with generator w. Thus R is a principal ideal domain. □

Solution to Exercise 3.40.

- $\sqrt{(0)} \subset \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$: Let $f \in \sqrt{(0)}$. $\operatorname{Spec} R$ is nonempty since R has a maximal ideal and maximal ideals are prime. Thus we can consider an arbitrary $\mathfrak{p} \in \operatorname{Spec} R$. We argue $f \in \mathfrak{p}$ by induction on the smallest integer $n \in \mathbb{Z}_{\geqslant 1}$ such that $f^n \in \mathfrak{p}$. If $f = 0$ then $f \in \mathfrak{p}$, affirming the claim, and if $n = 1$ then $f = f^1 \in \mathfrak{p}$, also affirming the claim. Now suppose $n \in \mathbb{Z}_{\geqslant 2}$ is the smallest integer such that $f^n = 0$, and suppose any $g \in \sqrt{(0)}$ is contained in $\mathfrak{p}$ whenever $g^k \in \mathfrak{p}$ for any $1 \leqslant k \leqslant n - 1$. As $n \in \mathbb{Z}_{\geqslant 2}$ and $f^n = 0$, we have $f \cdot f^{n-1} = f^n = 0 \in \mathfrak{p}$. But $\mathfrak{p}$ is prime, so either $f \in \mathfrak{p}$ or $f^{n-1} \in \mathfrak{p}$. If $f \in \mathfrak{p}$ then we are done, and if f^{n-1} then $f \in \mathfrak{p}$ by the induction hypothesis, so we are also done. Thus $\sqrt{(0)} \subset \bigcap_{\mathfrak{p}\in\operatorname{Spec} R} \mathfrak{p}$.

- $\bigcap_{\mathfrak{p}\in\operatorname{Spec} R} \mathfrak{p} \subset \sqrt{(0)}$: Let $f \in \bigcap_{\mathfrak{p}\in\operatorname{Spec} R} \mathfrak{p}$. We claim $f^n = 0$ for some $n \in \mathbb{Z}_{\geqslant 1}$. Suppose for a contradiction $f^n \notin (0)$ for all $n \in \mathbb{Z}_{\geqslant 1}$. Then the set
$$\mathcal{S} = \{\text{proper ideals } I \text{ of } R \mid f^n \notin I \text{ for all } n \in \mathbb{Z}_{\geqslant 1}\}$$
is nonempty, since it contains (0). Equip $\mathcal{S}$ with the partial ordering with respect to inclusion, and let $\{I_\alpha\}_{\alpha\in A}$ be any totally ordered chain of $\mathcal{S}$ indexed by any set A. We claim the set
$$J \coloneqq \bigcup\nolimits_{\alpha\in A} I_\alpha.$$
is an upper bound for $\{I_\alpha\}_{\alpha\in A}$ in $\mathcal{S}$.
  - J is an ideal of R: If $x, x' \in J$ and $r \in R$, then $rx + x' \in I_\alpha$ since I_α is an ideal, and in turn $rx + x' \in J$ since $I_\alpha \subset J$.
  - J is a proper ideal of R: Suppose instead $J = R$. Then $1 \in J$, so $1 \in I_\alpha$ for some $\alpha \in A$. But then $I_\alpha = R$, contradicting the I_α are proper ideals of R.
  - $J \in \mathcal{S}$: Indeeed, if $f^n \in J = \bigcup_{\alpha\in A} I_\alpha$ for some $n \in \mathbb{Z}_{\geqslant 1}$, then $f^n \in I_\alpha$ for some $\alpha \in A$, which contradicts $I_\alpha \in \mathcal{S}$.
  - J is an upper bound for $\{I_\alpha\}_{\alpha\in A}$ with respect to inclusion, since J is the union of the I_α.

  Thus $\{I_\alpha\}_{\alpha\in A}$ is bounded above in $\mathcal{S}$, so by Zorn's Lemma $\mathcal{S}$ contains a maximal element M with respect to inclusion.

  We claim that M is a prime ideal of R. As an element of $\mathcal{S}$, M is a proper ideal of R. It then only remains to show $R \smallsetminus M$ is closed under multiplication. Suppose for a contradiction there exist elements $g, h \in R$ such that $gh \in M$ but $g, h \in R \smallsetminus M$. Then the ideals $M + (g)$ and $M + (h)$ strictly contain M, so $M + (g), M + (h)$ cannot belong to $\mathcal{S}$ by maximality of M. This means there exist $n, m \geqslant 1$ such that $f^n \in (g)$ and $f^m \in (h)$. But then in particular $f^n \in M + (g)$ and $f^m \in M + (h)$, so
$$f^{n+m} \in (M + (g))(M + (h)) = M + (g)(h) = M + (gh) = M,$$
contradicting $M \in \mathcal{S}$. Thus M is a prime ideal of R. But f is contained in all prime ideals of R, so $f \in M$. But as an element of $\mathcal{S}$, M cannot contain f^n for any $n \in \mathbb{Z}_{\geqslant 1}$, so in particular M cannot contain f, a contradiction. Then $\mathcal{S}$ must be empty, so $(0) \notin \mathcal{S}$, which is to say $f^n \in (0)$ for some $n \in \mathbb{Z}_{\geqslant 1}$. Hence $f \in \sqrt{(0)}$. Thus $\bigcap_{\mathfrak{p}\in\operatorname{Spec} R} \mathfrak{p} \subset \sqrt{(0)}$. □

Solution to Exercise 3.41.

(a) We prove in part (b) that $J(R)$ is an intersection of ideals in R, and our proof does not use $J(R)$ is an ideal. Thus $J(R)$ is an ideal of R, since the intersection of an arbitrary set of ideals is an ideal. (Indeed, if $\{I_\alpha\}_{\alpha\in A}$ is any collection of ideals of R indexed by a set A, and if $J = \bigcap_{\alpha\in A} I_\alpha$, then $J \neq \varnothing$ because $0 \in I_\alpha$ for all $\alpha \in A$, and if $x, x' \in J$, $r \in R$ then $rx + x' \in J$ since $rx + x' \in I_\alpha$ for each $\alpha \in A$, as I_α is an ideal for all $\alpha \in A$.)

(a) (Alternate Solution). Let $x, y \in J(R)$. Then for all z, $1 - xz \in R^\times$, $1 - yz \in R^\times$, so $1 - z$ is a unit. Then there exists u such that $u(1 - xz) = 1$. Then $(1 - (x + y)z)u = u(1 - xz - yz) = 1 - uyz = 1 - y(uz)$, which by hypothesis is a unit, so we are done.

(b)
- $J(R) \subset \bigcap_{\mathfrak{m}\in\operatorname{Max}(R)} \mathfrak{m}$: Suppose $x \in J(R)$ but there exists a maximal ideal $\mathfrak{m}$ not containing x. Then $R = \mathfrak{m} + (x)$, since otherwise $\mathfrak{m} \subsetneq \mathfrak{m} + (x) \subsetneq R$, contradicting $\mathfrak{m}$ is maximal. Thus $1 = m + rx$ for some $m \in \mathfrak{m}, r \in R$, so $1 - rx = m \in \mathfrak{m}$. Observe that $1 - rx$ is not a unit, since otherwise
$$1 = (1 - rx)^{-1} \underbrace{(1 - rx)}_{\in\mathfrak{m}} \in \mathfrak{m},$$
which means $\mathfrak{m} = R$, contradicting maximal ideals are proper. But $1 - rx$ must be a unit since $x \in J(R)$, a contradiction. It follows that $J(R) \subset \bigcap_{\mathfrak{m}\in\operatorname{Max}(R)} \mathfrak{m}$.
- $\bigcap_{\mathfrak{m}\in\operatorname{Max}(R)} \mathfrak{m} \subset J(R)$. Suppose $x \notin J(R)$. Then there exists $y \in R$ such that $1 - xy$ is not a unit. Then $(1 - xy)$ is a proper ideal, so there exists a maximal ideal $\mathfrak{m}$ of R containing $(1 - xy)$, and in particular $1 - xy \in \mathfrak{m}$. Observe that if $x \in \mathfrak{m}$, then
$$1 = \underbrace{1 - xy}_{\in\mathfrak{m}} + \underbrace{xy}_{\in\mathfrak{m}} \in \mathfrak{m}$$
(since $\mathfrak{m}$ is an ideal), so $\mathfrak{m} = R$, again contradicting maximal ideals are proper. Thus $x \notin \mathfrak{m}$, so $x \notin \bigcap_{\mathfrak{m}\in\operatorname{Max}(R)} \mathfrak{m}$. We conclude $\bigcap_{\mathfrak{m}\in\operatorname{Max}(R)} \mathfrak{m} \subset J(R)$. □

Solution to Exercise 3.42.

(a) Since $\sqrt{I}$ contains I any prime ideal containing $\sqrt{I}$ must also contain I. Hence $V(\sqrt{I}) \subset V(I)$. Similarly, since $I = (S)$ contains S, $V(I) \subset V(S)$. It only remains to show $V(S) \subset V(\sqrt{I})$. Suppose $\mathfrak{p} \in V(S)$. We need to show $\mathfrak{p}$ contains $\sqrt{I}$. To that end, let $f \in \sqrt{I}$ be arbitrary, so that $f^n \in I$ for some positive integer n. Then we are done if we can show $f \in \mathfrak{p}$. It is enough to show that $f^k \in \mathfrak{p}$ for some $k \in \mathbb{Z}_{\geqslant 1}$, since by primality of $\mathfrak{p}$ that $f \in \mathfrak{p}$ (see the induction argument in the proof of Exercise 8.2 for the details). Since $f^k \in I$ and $\mathfrak{p}$ is an ideal of R containing S, we have
$$f^n \in I = (S) = \bigcap_{\substack{\text{ideals } J \text{ of } R\\ \text{containing } S}} J \subset \mathfrak{p}.$$
Thus $f^n \in \mathfrak{p}$, so we are done by our previous remarks.

(b) Let $\tau^c \coloneqq \{V(I) \mid I \text{ is an ideal of } R\}$. We claim $\tau \coloneqq \{V^c \mid V \in \tau^c\}$ is a topology on $\operatorname{Spec} R$.
- $V(R) = \varnothing$, since prime ideals of R are proper ideals, so there can be no prime ideal of R containing R. Thus $\varnothing \in \tau^c$.
- $V((0)) = \operatorname{Spec} R$, since any ideal contains (0), so in particular any prime ideal contains (0). Thus $\operatorname{Spec} R \in \tau^c$.
- Let $\{V(I_\alpha)\}_{\alpha\in A}$ be an arbitrary collection of elements of τ^c indexed by a set A. We claim $\bigcap_{\alpha\in A} V(I_\alpha) = V(\bigcup_{\alpha\in A} I_\alpha)$.

  Suppose $\mathfrak{p} \in V(\bigcup_{\alpha\in A} I_\alpha)$. Then $\mathfrak{p}$ contains the union $\bigcup_{\alpha\in A} I_\alpha$, and thus contains I_α for each $\alpha \in I$. Hence $\mathfrak{p} \in V(I_\alpha)$ for all $\alpha \in A$, so $\mathfrak{p} \in \bigcap_{\alpha\in A} V(I_\alpha)$. Thus $V(\bigcup_{\alpha\in A} I_\alpha) \subset \bigcap_{\alpha\in A} V(I_\alpha)$. Conversely, suppose $\mathfrak{p} \in \bigcap_{\alpha\in A} V(I_\alpha)$. Then $\mathfrak{p}$ contains I_α for each $\alpha \in A$, so $\mathfrak{p}$ contains $\bigcup_\alpha I_\alpha$, which means $\mathfrak{p} \in V(\bigcup_{\alpha\in A} I_\alpha)$. Hence
$$\bigcap_{\alpha\in A} V(I_\alpha) = V\Big(\bigcup_{\alpha\in A} I_\alpha\Big),$$

which is an element of τ^c by part (a). (Indeed, although the union of ideals is not in general an ideal, it is a subset of R, so by part (a) this is indeed an element of τ^c.)

– Let $\{V(I_j)\}_{j=1}^n$ be any finite collection of elements of τ^c indexed by $j \in \{1, \ldots, n\}$. We claim $\bigcup_{j=1}^n V(I_j) = V(\bigcap_{j=1}^n I_j)$.

Suppose $\mathfrak{p} \in \bigcup_{j=1}^n V(I_j)$. Then $\mathfrak{p} \in V(I_k)$ for some $k \in \{1, \ldots, n\}$, which is to say $\mathfrak{p}$ contains I_k. Since $\bigcap_{j=1}^n I_j \subset I_k$, $\mathfrak{p}$ must also contain $\bigcap_{j=1}^n I_j$, which means $\mathfrak{p} \in V(\bigcap_{j=1}^n I_j)$. Conversely, suppose $\mathfrak{p} \in V(\bigcap_{j=1}^n I_j)$. Then $\mathfrak{p}$ contains $\bigcap_{j=1}^n I_j$, so by the second clause of the Prime Avoidance Theorem $\mathfrak{p}$ contains I_k for some $k \in \{1, \ldots, n\}$. Then $\mathfrak{p} \in V(I_k)$, which implies $\mathfrak{p} \in \bigcup_{j=1}^n V(I_j)$. We conclude

$$\bigcup_{j=1}^n V(I_j) = V\Big(\bigcap_{j=1}^n I_j\Big),$$

which is an element of τ^c.

It follows that the collection τ^c satisfies the axioms for the closed subsets of a topology on $\operatorname{Spec} R$, so the Zariski topology τ is indeed a topology on $\operatorname{Spec} R$.

(c) Consider the case $R = \mathbb{C}[x]$. We showed in recitation that if k is a field then $\operatorname{Spec} k[x] = \{(0)\} \cup \{(f(x)) \mid f(x) \text{ is an irreducible element of } k[x]\}$. Thus, as a set, we have

$$\operatorname{Spec} \mathbb{C}[x] = \{0\} \cup \{(x - z) \mid z \in \mathbb{C}\}. \tag{11.6.1}$$

Now equip $\operatorname{Spec} \mathbb{C}[x]$ with the Zariski topology. Since $\mathbb{C}[x]$ is a PID by Exercise 8.1, the closed sets of $\operatorname{Spec} \mathbb{C}[x]$ take the form $V((f(x)))$, where $f(x) \in \mathbb{C}[x]$. But if $f(x) \in \mathbb{C}[x]$, then we can write

$$f(x) = (x - z_1) \cdots (x - z_n),$$

where $\{z_j\}_{j=1}^n$ is some multiset of elements of $\mathbb{C}$ of size n. Since

$$(f(x)) = ((x - z_1) \cdots (x - z_n)) = (x - z_1) \cdot (x - z_2) \cdots (x - z_n),$$

the set of maximal ideals containing $(f(x))$ is $\{(x - z_j)\}_{j=1}^n$. (Indeed, if is instead $f(x) \in (x - t)$ for some $t \in \mathbb{C} \setminus \{z_1, \ldots, z_n\}$, then $(x - t)$ divides $f(x)$, but then $t = z_j$ for some $j \in \{1, \ldots, n\}$, a contradiction.) Thus, since $\operatorname{Spec} \mathbb{C}[x]$ contains only maximal ideals, by Equation (11.6.1) we must have

$$V((f(x))) = \{(x - z_1), \ldots, (x - z_n)\}.$$

Since $f(x) \in \mathbb{C}[x]$ was arbitrary, the closed sets of $\mathbb{C}[x]$ have finite cardinality. But $\operatorname{Spec} \mathbb{C}[x]$ is infinite, so the nonempty open sets of $\operatorname{Spec} \mathbb{C}[x]$ must have infinite cardinality. In particular, any two open subsets of $\operatorname{Spec} k[x]$ cannot be disjoint, since otherwise its (closed) complement must be infinite, but we just showed closed sets are finite. It follows that for any two distinct elements of $\operatorname{Spec} \mathbb{C}[x]$, there do not exist disjoint open subsets separating them, since pairs of open subsets of $\operatorname{Spec} \mathbb{C}[x]$ cannot even be disjoint. Thus the Zariski topology on $\operatorname{Spec} \mathbb{C}[x]$ is not Hausdorff. □

Solution to Exercise 3.43. First note that if I is any ideal of a commutative ring R, then since the quotient map $\pi \colon R \twoheadrightarrow R/I$ is surjective, the statement of Exercise 8.5 implies π induces a homeomorphism of $\operatorname{Spec}(R/I)$ onto the closed subset $V(\ker \pi) = V(I)$ of $\operatorname{Spec}(R)$.

We now prove the statement of Exercise 8.5. Define $\varphi^\sharp\colon \operatorname{Spec} B \to \operatorname{Spec} A$ by $\varphi^\sharp(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p})$. We first show $\varphi^\sharp$ is a well-defined map into $\operatorname{Spec} A$. To that end, we need to show for a given $\mathfrak{p} \in \operatorname{Spec} B$ that $\mathfrak{q} \coloneqq \varphi^{-1}(\mathfrak{p})$ is indeed a prime ideal of A. To see this, note that if $x, x' \in \mathfrak{q} = \varphi^{-1}(\mathfrak{p})$ and $a \in A$, then $\varphi(x), \varphi(x') \in \mathfrak{p}$, so since $\mathfrak{p}$ is an ideal we have

$$\varphi(rx + x') = \varphi(r)\underbrace{\varphi(x)}_{\in\mathfrak{p}} + \underbrace{\varphi(x')}_{\in\mathfrak{p}} \in \mathfrak{p},$$

so $\mathfrak{q}$ is an ideal of A. And $\mathfrak{q}$ is prime, since if $xx' \in \mathfrak{q} = \varphi^{-1}(\mathfrak{p})$ for some $x, x' \in A$, then $\varphi(xx') = \varphi(x)\varphi(x') \in \mathfrak{p}$, which by primality of $\mathfrak{p}$ implies $\varphi(x) \in \mathfrak{p}$ or $\varphi(x') \in \mathfrak{p}$. Hence x or x' is in $\varphi^{-1}(\mathfrak{p})$.

To show $\varphi^\sharp$ is a homeomorphism of $\operatorname{Spec} B$ onto the closed subset $V(\ker\varphi)$, it suffices to show

(i) $\varphi^\sharp$ is a closed map and $\operatorname{im}\varphi^\sharp = V(\ker\varphi)$,

(ii) $\varphi^\sharp$ is continuous, and

(iii) $\varphi^\sharp$ is injective.

Proof of (i). Let I be an ideal of B. It suffices to show $\varphi^\sharp(V(I)) = V(\varphi^{-1}(I))$.

($\subset$) Let $\mathfrak{p} \supset I$. We need to show $\varphi^{-1}(\mathfrak{p}) \subset \mathfrak{p}^{-1}(I)$, that is, that $\{a \in A \mid \varphi(a) \in \mathfrak{p}\} \subset \{a \in A \mid \varphi(a) \in I\}$. And this is true, because if $a \in A$ and $\varphi(a) \in I \subset \mathfrak{p}$, then $\varphi(a) \in \mathfrak{p}$. Hence $\varphi^\sharp(V(I)) \subset V(\varphi^{-1}(I))$.

($\supset$) Suppose $\varphi^{-1}(\mathfrak{p}) \supset \varphi^{-1}(I)$. We need to show $\mathfrak{p} \supset I$. If $b \in I$, then $\varphi^{-1}(b) \in \varphi^{-1}(\mathfrak{p})$ by hypothesis. Thus, whatever maps has image b also maps into $\mathfrak{p}$, which means $\mathfrak{p} \in b$. Since $b \in I$ was arbitrary, $\mathfrak{p} \supset I$.

Hence $\varphi^\sharp(V(I)) = V(\varphi^{-1}(I))$ for all ideals I of B, so $\varphi^\sharp$ is a closed map.

The above argument in particular shows that if $\varphi^\sharp(\operatorname{Spec} B) = \varphi^\sharp(V(0)) = V(\varphi^{-1}((0))) = V(\ker\varphi)$, so $\varphi^\sharp$ maps $\operatorname{Spec} B$ onto the closed subset $V(\ker\varphi)$ of $\operatorname{Spec} A$. □

Proof of (ii). We claim $\varphi^\sharp$ is continuous, so it is enough to show the preimages of closed sets under $\varphi^\sharp$ are closed. If J is an ideal of A, then

$$\begin{aligned}(\varphi^\sharp)^{-1}(V(J)) &= \{\mathfrak{p} \in \operatorname{Spec} B \mid \varphi^\sharp(\mathfrak{p}) \in V(J)\} = \{\mathfrak{p} \in \operatorname{Spec} B \mid \varphi^{-1}(\mathfrak{p}) \supset J\} \\ &= \{\mathfrak{p} \in \operatorname{Spec} B \mid \mathfrak{p} \supset \varphi(J)\} = V(\varphi(J)),\end{aligned}$$

which is closed in $\operatorname{Spec} B$. Thus $\varphi^\sharp$ is continuous. □

Proof of (iii). Suppose $\varphi^\sharp(\mathfrak{p}) = \varphi^\sharp(\mathfrak{p})$. Let $b \in B$. Since φ is surjective, there exists $a \in A$ such that $\varphi(a) = b$. Then

$$b \in \mathfrak{p} \iff a^{-1} \in \varphi^{-1}(\mathfrak{p}) = \varphi^{-1}(\mathfrak{p}') \iff b \in \mathfrak{p}'.$$

Hence $\mathfrak{p} = \mathfrak{p}'$, so $\varphi^\sharp$ is injective. Thus $\varphi^\sharp$ is a homeomorphism of $\operatorname{Spec} B$ onto the closed subset $V(\ker\varphi)$ of $\operatorname{Spec} A$. □

By our initial remarks, this completes the proof of Exercise 8.5. □

Proof of Theorem 4.6. Suppose R is a local ring with maximal ideal $\mathfrak{m}$. Then for any $u \in R \smallsetminus \mathfrak{m}$, (u) must equal R because $(u) \not\subset \mathfrak{m}$ and $\mathfrak{m}$ is the *only* maximal ideal. Hence $(u) = R$, so u is a unit. Thus $R \smallsetminus R^\times \subset \mathfrak{m}$. For the reverse inclusion, note that any u of R is not in $\mathfrak{m}$, since otherwise $R = (u) \subset \mathfrak{m} \subsetneq R$, a contradiction. Thus $\mathfrak{m} = R \smallsetminus R^\times$.

For the converse, assume $R \smallsetminus R^\times = \mathfrak{m}$, or equivalently that $R \smallsetminus \mathfrak{m} = R^\times$. We claim R is local with maximal ideal $\mathfrak{m}$. Let $I \subsetneq R$ be any proper ideal. Then $I \cap R^\times = \varnothing$ (since otherwise $I = R$ as above), so $I \subset R \smallsetminus R^\times = \mathfrak{m}$. Thus $\mathfrak{m}$ is the unique maximal ideal of R, so R is local with maximal ideal $\mathfrak{m}$. □

Proof of Proposition 4.11. If $(\sum_{n=0}^\infty a_n x^n)(\sum_{n=0}^\infty b_n x^n) = 1$ then $a_0 b_0 = 1$. Hence a_0 is a unit in R.

On the other hand, if $f = \sum_n a_n x^n$ and a_0 is a unit in R, $a_0 b_0 = 1$ for some $b_0 \in R$. Then $b_0 f = \sum_{n=0}^\infty b_0 a_n x^n = 1 + x \sum_{n=0}^\infty b_0 a_n x^{n-1} = 1 - xg$ for some $g = \sum_{n=0}^\infty (-b_0 a_n x^{n-1})$, so $b_0 f$ is a unit. Thus f is a unit. □

Proof of Proposition 4.14. To see $I \subset (x^{v(I)})$, suppose $f \in I$ such that $v(f) = v(I)$. Then $f = x^{v(f)}(a_0 + a_1 x + \cdots) = x^{v(I)} \cdot (\text{unit})$. Then $x^{v(I)} = \underbrace{f}_{\in I}(\text{unit})^{-1} \in I$. Thus $(x^{v(I)}) \subset I$.

Conversely, to see $(x^{v(I)}) \subset I$, note that if $f = \sum_{n=0}^\infty a_n x^n$ is any arbitrary element of the ideal I, then $f = x^{v(f)} g$ and $v(f) \geqslant v(I)$ (by definition of v), so $f = x^{v(f)} g = x^{v(I)}(x^{v(f)-v(I)} g) \in (x^{v(I)})$. Thus $I \subset (x^{v(I)})$. □

Proof of Proposition 4.20. We need to show $\sim$ is indeed an equivalence relation on $A \times S$, and that the ring operations are well-defined. $\sim$ is an equivalence relation on $A \times S$: It is immediate that it is reflexive and symmetric, and it is transitive because if $(a, s) \sim (b, t)$ and $(b, t) \sim (c, u)$ then there exist $v, w \in S$ such that

$$v(at - bs) = 0 \qquad \text{and} \qquad w(bu - ct) = 0,$$

that is,

$$vuw(at - bs) = 0 \qquad \text{and} \qquad svw(bu - ct) = 0.$$

Adding these two equations, we obtain

$$\pm vw(au - cs) = 0.$$

Now $tvw \in S$, since $t, v, w \in S$ and S is multiplicatively closed, so we can conclude $(a, s) \sim (c, u)$. The rest of the proof is left as an exercise. □

Proof of Lemma 4.29. Recall j is the canonical ring homomorphism $j \colon S^{-1}A \to A$ given by $a \mapsto (a, 1)$. Then $j(a) = (a, 1) = (0, 1)$ if and only if there exists $s \in S$ such that $s \cdot (a \cdot 1 - 0 \cdot 1) = 0$. □

Proof of Lemma 4.34. Define

$$\begin{aligned} R[x] &\longrightarrow R_f, \\ R \ni r &\longmapsto (r, 1), \end{aligned}$$

$$x \longmapsto (1, f).$$

This map is certainly a ring homomorphism. Since this map is surjective (any element $a/f^j \in A_f$ is the image of $ax^j \in R[x]$), it is enough to show its kernel is $(xf - 1)$. To see this, note that $(xf-1)h(x)$ has image $((1/f)f - 1)h(x) = 0 \cdot h(x) = 0$. On the other hand, if the image of $g(x) = \sum_{i=1}^{\deg g} b_i x^i$ is 0, then $0 = \sum_i b_i(1/f)^i = \sum_i b_i/f^i$, so by multiplying through by $f^{\deg g}$ we obtain $0 = \sum_{i=1}^{\deg g} b_i f^{\deg g - i} = 0$ (for the first equality here we used here that $f^{\deg g}$ is a unit in A_f to be able to multiply through by $f^{\deg i}$). Hence $(x - 1/f) = (1/f)(xf-1)$ divides g, so $g \in (xf - 1)$ in A_f (again since f is a unit in A_f). □

Proof of Proposition 4.36. For $a/s \in S^{-1}A$, define

$$\widetilde{\varphi}\left(\frac{a}{s}\right) \coloneqq \varphi(s)^{-1} \cdot \varphi(a).$$

φ is well-defined: If $a/s = b/t$ in $S^{-1}A$ (so $a, b \in A$, meaning by define there exists $u \in S$ such that $u(at - bs) = 0$ in A).

Applying φ, we get $0 = \varphi(u)(\varphi(a)\varphi(t) - \varphi(b)\varphi(s))$. Because $\varphi(s), \varphi(t), \varphi(u)\varphi(S) \subset B^\times$ in B, we deduce $\varphi(s)^{-1}\varphi(a) - \varphi(t)^{-1}\varphi(b) = 0$. Thus $\widetilde{\varphi}$ is well-defined.

$\widetilde{\varphi}$ is a ring homomorphism: We have $\widetilde{\varphi}(1, 1) = \varphi(1)^{-1}\varphi(1) = 1$ and

$$\widetilde{\varphi}\left(\frac{a}{s} \cdot \frac{b}{t}\right)\varphi(st)^{-1}\varphi(ab) = \varphi(s)^{-1}\varphi(a)\varphi(t)^{-1}\varphi(b) = \widetilde{\varphi}\left(\frac{a}{s}\right)\widetilde{\varphi}\left(\frac{b}{t}\right)$$

and

$$\begin{aligned}\widetilde{\varphi}\left(\frac{a}{s} + \frac{b}{t}\right) &= \widetilde{\varphi}\left(\frac{at + bs}{st}\right) = \varphi(st)^{-1}\varphi(at + bs) \\ &= \varphi(st)^{-1}\varphi(at + bs) = \varphi(s)^{-1}\varphi(a) + \varphi(t)^{-1}\varphi(b) = \widetilde{\varphi}(a/s) + \widetilde{\varphi}(b/t),\end{aligned}$$

so $\widetilde{\varphi}$ is a ring homomorphism. And $\widetilde{\varphi}$ makes the diagram commute, because $\widetilde{\varphi} \circ j(a) = \widetilde{\varphi}(a/1) = \varphi(a)$. Finally, $\widetilde{\varphi}$ is unique because for any ring homomorphism $\psi\colon S^{-1}A \to B$ such that $\psi \circ j = \varphi$, and for all $x = a/s \in S^{-1}A$, we have

$$\psi\left(\frac{s}{1} \cdot x\right) = \psi\left(\frac{a}{1}\right) = \psi \circ j(a) = \varphi(a).$$

And $\psi(j(s)) \cdot \psi(x) = \varphi(s) \cdot \psi(x)$. Again since $\varphi(s) \in B^\times$, this forces $\psi\left(\frac{a}{s}\right) = \varphi(s)^{-1} \cdot \varphi(a)$. Thus $\widetilde{\varphi}$ is unique. □

Proof of Lemma 4.41. Let J be an ideal of $S^{-1}A$. Let $I = j^{-1}(J)$, which is an ideal of A as the preimage of a ring homomorphism.

- $S^{-1}I \subset J$: It suffices to show that if $S^{-1}I$ is generated as an ideal of $S^{-1}A$ by $\{j(x) \mid x \in I\}$ then this set is in J. But $\{j(x) \mid x \in I\} \subset J$, so we are done.
- $J \subset S^{-1}I$: Let $x = a/s \in J$ for $a \in A$ and $s \in S$. Then $\frac{s \cdot x}{1} = \frac{a}{1} \in J$. But $\frac{a}{1} = j(a)$, so $a \in I$ by definition. Thus $x = \frac{a}{s} \in S^{-1}I$. That proves the surjectivity.

We now show the failure of injectivity. If $I \cap S \neq \varnothing$, then $S^{-1}I \cap (S^{-1}A)^\times \neq \varnothing$. Hence $S^{-1}I = S^{-1}A$. Conversely, if $S^{-1}A = S^{-1}I$, then we can write $(1 =)1/1 \in S^{-1}A$, since in

$S^{-1}A$ we have

$$\begin{aligned} 1 &= \sum\nolimits_{i=1}^{n} \frac{x_i}{s_i} \text{ for some } x_i \in I, s_i \in S \\ &= \sum\nolimits_{i=1}^{n} \frac{t_i \cdot x_i}{s_1 \cdots s_n}, \text{ where } t_i = s_1 \cdots s_{i-1} s_{i+1} \cdots s_n, \end{aligned}$$

that is, there exists $u \in S$ such that $u \cdot (s_1 \cdots s_n - \sum_{i=1}^{n} t_i x_i) = 0$ in A, hence

$$\underbrace{u \cdot \sum\nolimits_{i=1}^{n} t_i x_i}_{\substack{\in I, \text{ since} \\ \text{each } x_i \in I}} = \underbrace{u s_1 \cdots s_n}_{\substack{\in S, \text{ since} \\ u_1, s_1, \ldots, s_n \in S}} \text{ in } A$$

Thus $I \cap S \neq \varnothing$. □

Proof of Proposition 4.42. We first show this map is surjective. Give a prime $\mathfrak{q} \in \operatorname{Spec}(S^{-1}A)$, by Lemma 4.41 we can write $\mathfrak{q} = S^{-1}I$ for some ideal I of A such that $I \cap S = \varnothing$. So, to show surjectivity here, we just need to check I is prime. But when proving Lemma 4.41, we showed that we can take $I = j^{-1}(\mathfrak{q})$, and this is prime since the preimage of a prime ideal is a prime ideal. On the other hand, suppose we are given $\mathfrak{p} \in \operatorname{Spec} A$ such that $\mathfrak{p} \cap S = \varnothing$, we claim that

(a) $S^{-1}\mathfrak{p}$ is prime, and

(b) $j^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$. (Note that this is not true without the assumption $\mathfrak{p}$ is prime, and it is an exercise to find such examples.)

And (b) holds, since certainly $\mathfrak{p} \subset j^{-1}(S^{-1}\mathfrak{p})$. If $x \in j^{-1}(S^{-1}\mathfrak{p})$, then $j(x) \in S^{-1}\mathfrak{p}$, and hence can be written $x/1 = a/s$ for some $s \in S$ and $a \in \mathfrak{p}$. Thus there exists $u \in S$ such that $u(sx - a) = 0$ in A. Hence $usx = ua \in \mathfrak{p}$. But $u, s \in S$, so since $\mathfrak{p}$ is an ideal not intersecting S we must have $u, s \notin \mathfrak{p}$. Since $\mathfrak{p}$ is prime, we conclude $x \in \mathfrak{p}$, which proves (b). The proof of (a) is similar. □

Proof of Corollary 4.43. By last time, the bijection $\operatorname{Spec} A_{\mathfrak{p}} \xrightarrow{\cong} \{\mathfrak{q} \in \operatorname{Spec} A \mid \mathfrak{q} \cap (A \smallsetminus \mathfrak{p}) = \varnothing\} = \{\mathfrak{q} \in \operatorname{Spec} A \mid \mathfrak{q} \subset \mathfrak{p}\}$. □

Proof of Proposition 4.50. As $A \subset A_{\mathfrak{p}} \subset \operatorname{Frac} A$ for all $\mathfrak{p} \in \operatorname{Spec} A$, $A \subset \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} A_{\mathfrak{p}} \subset \bigcap_{\mathfrak{m} \in \operatorname{Max}(A)} A_{\mathfrak{m}}$, so it suffices to show $\bigcap_{\mathfrak{m} \in \operatorname{Max}(A)} \subset A$. To that end, suppose $x \in \bigcap_{\mathfrak{m} \in \operatorname{Max}(A)} A_{\mathfrak{m}}$. Consider

$$I = \{y \in A \mid xy \in A\}.$$

If $I = A$, then $1 \in I$ and we win. So we may assume I is a proper ideal of A. Then I is contained in some maximal ideal $\mathfrak{m}$. Since $x \in A_{\mathfrak{m}}$, we know there exists $s \in A \smallsetminus \mathfrak{m}$ such that $sx \in A$. Hence $s \in I \subset \mathfrak{m}$, a contradiction, since $x = a/s$ for some $a \in A$ and some $s \in A \smallsetminus \mathfrak{m}$. But then there are zerodivisors in A, but A has no zerodivisors. □

Proof of Theorem 4.54. We only prove that S^{-1} is exact (that is, preserves exact sequences). We are given $\ker g = \operatorname{im} f$,

$$S^{-1}g \circ S^{-1}f = S^{-1}(\underbrace{g \circ f}_{\text{the zero map}}),$$

so $\operatorname{im}(S^{-1}f) \subset \ker(S^{-1}g)$. Now suppose $n/s \in \ker S^{-1}g$ for some $n \in N$, $s \in S$. Then

$$\frac{g(n)}{s} = 0 \text{ in } S^{-1}P,$$

that is, there exists $t \in S$ such that $tg(n) = 0$ in P. Hence $g(tn) = 0$ in P, so $tn \in \ker g = \operatorname{im} f$, and we find $m \in M$ such that $f(m) = tn$. Thus $(S^{-1}f)\big(\frac{m}{st}\big) = \frac{n}{s}$ in $S^{-1}N$, so $n/s \in \operatorname{im}(S^{-1}f)$. This completes the proof. □

Proof of Definition 4.57. $M \cap P \subset M \subset P$, so $S^{-1}(M \cap P) \subset S^{-1}M \subset S^{-1}P$, so $S^{-1}(M \cap P) \subset (S^{-1}M) \cap (S^{-1}P)$.

Conversely, if $\alpha \in (S^{-1}(M)) \cap (S^{-1}(P)) \subset S^{-1}N$, then any element α of the left-hand side (the intersection) can be written as x/s and as y/t simultaneously, for $x \in M$, $y \in P$, $s, t \in S$. Then by definition of the equivalence relation, there exists $u \in S$ such that $u(xt - ys) = 0$ in N, so in particular in N we have

$$u\,\underbrace{x}_{\in M}\,t = u\,\underbrace{y}_{\in P}\,s$$

so $utx = usy \in M \cap P$. Then

$$\alpha = x/s = \frac{utx \in M \cap P}{uts \in S},$$

a contradiction. □

Proof of Proposition 4.61. We have

$$\begin{aligned}
j(m) = 0 &\iff (m, 1) \sim (0, 1)\\
&\iff \text{there exists } u \in S \text{ such that } u(m \cdot 1 - 0 \cdot 1) = 0\\
&\iff \text{there exists } u \in S \text{ such that } um = 0\\
&\iff \text{there exists } u \in S \cap \operatorname{Ann}_A(m)\\
&\iff S \cap \operatorname{Ann}_A(m) \neq \varnothing.
\end{aligned}$$

□

Proof of Lemma 4.74. Recall that the annihilator $\operatorname{Ann}(x) = \{a \in A \mid a \cdot x = 0\}$ of a nonzero element $x \in Q$ is a proper ideal of A (indeed, it is immediate that it is an ideal, and $1 \notin \operatorname{Ann}(x)$ since $1 \cdot x = x \neq 0$.) Thus $\operatorname{Ann}(x) \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m} \subset A$. Since $Q_{\mathfrak{m}} = 0$, $s \cdot x = 0$ for some $s \in A \smallsetminus \mathfrak{m}$. But then $s \in \operatorname{Ann}(x) \subset \mathfrak{m}$, a contradiction. We conclude $Q = 0$. □

Proof of Theorem 4.75. We know (1) $\implies$ (2) since localization is exact, and (2) $\implies$ (3) because maximal ideals are prime. It therefore suffices to assume (3) and prove (1). Since

$$\begin{aligned}
(1) &\iff \ker g = \operatorname{im} f\\
&\iff \operatorname{im} f \subset \ker g \text{ and } \ker g / \operatorname{im} f = 0 && (11.6.2)\\
&\iff \operatorname{im} f + \ker g = \ker g && (11.6.3)\\
&\iff (\operatorname{im} f + \ker g)/\ker g = 0,
\end{aligned}$$

it suffices to show $(\operatorname{im} f + \ker g)/\ker g = 0$. We will work with the short exact sequence $0 \to \operatorname{im} f \to \operatorname{im} f + \ker g \to (\operatorname{im} f + \ker g)/\operatorname{im} f \to 0$.

Note that for all $\mathfrak{m} \in \operatorname{Max}(A)$, the sequences

$$0 \longrightarrow \ker(g_{\mathfrak{m}}) \hookrightarrow N_m \xrightarrow{g_{\mathfrak{m}}} P_{\mathfrak{m}},$$
$$0 \longrightarrow \ker(g)_{\mathfrak{m}} \hookrightarrow N_{\mathfrak{m}} \xrightarrow{g_{\mathfrak{m}}} P_{\mathfrak{m}},$$

are exact; the first is immediate, and the second is a localization of the exact sequence $0 \to \ker g \hookrightarrow N \xrightarrow{g} P$, hence is exact. Thus (for instance, by the 5-lemma), we have $\ker(g_{\mathfrak{m}}) = \ker(g)_{\mathfrak{m}}$.

On the other hand, since $M \xrightarrow{f} \operatorname{im} f \to 0$ is exact, so is its localization $M_{\mathfrak{m}} \xrightarrow{f_{\mathfrak{m}}} N_{\mathfrak{m}} \to 0$, so by the same argument we obtain $\operatorname{im}(f_{\mathfrak{m}}) = \operatorname{im}(f)_{\mathfrak{m}}$.

Thus

$$\left(\frac{\operatorname{im}(f) + \ker(g)}{\ker(g)}\right)_{\mathfrak{m}} \cong \frac{\operatorname{im}(f)_{\mathfrak{m}} + \ker(g)_{\mathfrak{m}}}{\ker(g)_{\mathfrak{m}}} = \frac{\operatorname{im}(f_{\mathfrak{m}}) + \ker(g_{\mathfrak{m}})}{\ker(g_{\mathfrak{m}})} = 0$$

for all $\mathfrak{m}$, since the last equality above is equivalent to our assumption, (3). (Indeed, (3) holds $\iff$ $(\operatorname{im}(f_{\mathfrak{m}}) + \ker(g_{\mathfrak{m}}))/\ker(g_{\mathfrak{m}})$ follows from the same chain of equivalences as does Equation (11.6.2)). Then again applying Lemma 4.74, we obtain $(\operatorname{im} f + \ker g)/\ker g = 0$, that is, $\operatorname{im} f \subset \ker g$. We can then consider the quotient module $\ker g/\operatorname{im} f$, which must be 0 again by the claim; indeed, again by (3) we have

$$(\ker(g)/\operatorname{im}(f))_{\mathfrak{m}} = \ker(g)_{\mathfrak{m}}/\operatorname{im}(f)_{\mathfrak{m}} = \ker(g_{\mathfrak{m}})/\operatorname{im}(f_{\mathfrak{m}}) = 0$$

for all $\mathfrak{m}$. Thus $\ker(g) = \operatorname{im}(f)$. □

Solution to Exercise 4.76. (a) Let $m/s, n/t, w/q \in S^{-1}M$ be arbitrary.

$\sim$ *is reflexive:* $m/s \sim m/s$, since

$$\underbrace{1}_{\in S} \cdot (sm - sm) = 1 \cdot 0 = 0 \text{ in } M.$$

$\sim$ *is symmetric:* If $m/s \sim n/t$, then there exists $u \in S$ such that $0 = u(tm - sn) = -u(sn - tm)$. Multiplying both sides by the element -1 of A, we obtain

$$0 = \underbrace{u}_{\in S}(sn - tm),$$

so $n/t \sim m/s$.

$\sim$ *is transitive:* Suppose $m/s \sim n/t$ and $n/t \sim w/q$. Then there exist $u, v \in S$ such that

$$0 = u(tm - sn) \tag{11.6.4}$$
$$0 = v(qn - tw). \tag{11.6.5}$$

We want some $\ell \in S$ such that $0 = \ell(qm - sw)$. Multiplying Equation (11.6.4) by qv and multiplying Equation (11.6.5) by su, we obtain the equations

$$qvutm = qvusn \tag{11.6.6}$$

and

$$suvqn = suet, \tag{11.6.7}$$

respectively, in A. And $suvqn = qvutm$ since A is commutative, so Equations (11.6.6) and (11.6.7) imply $qvutm = suvtw$, that is,

$$vut(qm - sw) = 0.$$

Thus we can choose $\ell = vut$, and this is a valid choice bc $v, u, t \in S$ and S is multiplicatively closed.

(b) We first show $S^{-1}M$ is an abelian group with addition $S^{-1}M \times S^{-1}M \to S^{-1}M$ given by

$$\frac{m_1}{t_1} + \frac{m_2}{t_2} \coloneqq \frac{t_2 m_1 + t_1 m_2}{t_1 t_2}.$$

To show addition is well-defined, we will argue similar to showing transitivity of $\sim$ in part (a). Suppose $m_1'/t_1' = m_1/t_1$ and $m_2'/t_2' = m_2/t_2$. We claim

$$\frac{t_2 m_1 + t_1 m_2}{t_1 t_2} = \frac{t_2' m_1' + t_1' m_2'}{t_1' t_2'}.$$

We seek an $\ell \in S$ such that

$$\ell(t_1 t_2 (t_2' m_1' + t_1' m_2') - t_1' t_2' (t_2 m_1 + t_1 m_2)) = 0 \text{ in } M,$$

which by expanding out is equivalent to

$$\ell(t_1 t_2 t_2' m_1' + t_1 t_2 t_1' m_2' - t_1' t_2' t_2 m_1 - t_1' t_2' t_1 m_2) = 0 \text{ in } M. \tag{11.6.8}$$

Since $m_1'/t_1' = m_1/t_1$ and $m_2'/t_2' = m_2/t_2$, there exist $u_1, u_2 \in S$ such that

$$0 = u_1(t_1' m_1 - t_1 m_1') = u_2(t_2' m_2 - t_2 m_2') \text{ in } M.$$

Then in particular we have

$$u_1 t_1' m_1 = u_1 t_1 m_1' \tag{11.6.9}$$

and

$$u_2 t_2' m_2 = u_2 t_2 m_2' \tag{11.6.10}$$

in M. Then if we set $\ell = u_1 u_2$, then $\ell \in S$ since S is multiplicatively closed, and the left-hand side of Equation (11.6.8) can be written as

$$\begin{aligned}
\ell(t_1 t_2 t_2' m_1' + t_1 t_2 t_1' m_2' - t_1' t_2' t_2 m_1 - t_1' t_2' t_1 m_2) &= u_1 u_2 t_1 t_2 t_2' m_1' + u_1 u_2 t_1 t_2 t_1' m_2' \\
&\qquad - u_1 u_2 t_1' t_2' t_2 m_1 - u_1 u_2 t_1' t_2' t_1 m_2 \\
&= \underbrace{u_1 t_1 m_1'}_{=A} \underbrace{u_2 t_2' t_2}_{=:D} + \underbrace{u_2 t_2 m_2'}_{=B} \underbrace{(u_1 t_1' t_1)}_{=:C} - \underbrace{(u_1 t_1' m_1)}_{=:A} \underbrace{u_2 t_2' t_2}_{=D} - \underbrace{(u_1 t_1' t_1)}_{=C} \underbrace{(u_2 t_2' m_2)}_{=:B} \\
&= AD + BC - AD - CB = 0 \text{ in } A,
\end{aligned}$$

as desired. Thus addition is well-defined. This addition operation has identity $0/1$, inverses $-(m/t) = (-m)/t$, and is associative because

$$\begin{aligned}
\left(\frac{m_1}{t_1} + \frac{m_2}{t_2}\right) + \frac{m_3}{t_3} &= \frac{t_2 m_1 + t_1 m_2}{t_1 t_2} + \frac{m_3}{t_3} = \frac{t_3(t_2 m_1 + t_1 m_2) + (t_1 t_2) m_3}{(t_1 t_2) t_3} \\
&= \frac{t_2(t_3 m_1) + t_3(t_1 m_2) + (t_1 t_2) m_3}{t_1(t_2 t_3)} = \frac{(t_2 t_3) m_1 + t_1(t_3 m_2 + t_2 m_3)}{t_1(t_2 t_3)} \\
&= \frac{m_1}{t_1} + \left(\frac{t_1 m_2 + t_2 m_3}{t_2 t_3}\right) = \frac{m_1}{t_1} + \left(\frac{m_2}{t_2} + \frac{m_3}{t_3}\right).
\end{aligned}$$

Hence $S^{-1}M$ is an abelian group under the above definition of addition.

Define $S^{-1}A \times S^{-1}M \to S^{-1}M$ by

$$\frac{a}{m} \cdot \frac{m}{t} \coloneqq \frac{am}{st}.$$

To see this map is well-defined, suppose $a'/s' = a/s$ in $S^{-1}A$ and $m'/t' = m/t$ in $S^{-1}M$. Then there exist $u, v \in S$ such that $usa' = us'a$ and $vtm' = vt'm$. Then $\ell \coloneqq uv$ is an element of S since $u, v \in S$ and S is multiplicatively closed, and

$$\ell(sta'm' - s't'am) = ((vtm')(usa') - (vt'm)(us'a)) = 0.$$

so

$$\frac{a'}{s'} \cdot \frac{m'}{t'} = \frac{a'm'}{s't'} = \frac{am}{st} = \frac{a}{m} \cdot \frac{m}{t}.$$

Hence this is a well-defined map. To see this map is a ring action, first let $m/t, m_1/t_1, m_2/t_2 \in S^{-1}M$ and $r/s, r_1/s_1, r_2/s_2 \in S^{-1}A$ be arbitrary. Then

- $\frac{1}{1} \cdot \frac{m}{t} = \frac{1 \cdot m}{1 \cdot t} = \frac{m}{t}$,
- $\frac{r_1}{s_1} \cdot \left(\frac{r_2}{s_2} \cdot \frac{m}{t}\right) = \frac{r_1}{s_1} \cdot \frac{r_2 m}{s_2 t} = \frac{r_1 r_2 m}{s_1 s_2 t} = \left(\frac{r_1}{s_1} \cdot \frac{r_2}{s_2}\right) \cdot \frac{m}{t}$,
- $\left(\frac{r_1}{s_1} + \frac{r_2}{s_2}\right) \cdot \frac{m}{t} = \left(\frac{r_1 s_2 + r_2 s_1}{s_1 s_2}\right) \cdot \frac{m}{t} = \frac{(r_1 s_2 + r_2 s_1) \cdot m}{s_1 s_2 \cdot t} = \frac{r_1 s_2 m + r s_1 m}{s_1 s_2 t} = \frac{r_1 s_2 m}{s_1 s_2 t} + \frac{r_2 s_1 m}{s_1 s_2 t} = \left(\frac{s_2}{s_2} \cdot \frac{r_1}{s_1}\right) + \left(\frac{s_1}{s_1} \cdot \frac{r_2}{s_2}\right) \cdot \frac{m}{t} = \frac{r_1}{s_1} \cdot \frac{m}{t} + \frac{r_2}{s_2} \cdot \frac{m}{t}$, where in the last step we used the fact $s_1/s_1 = s_2/s_2 = 1/1$, which is true because
$$\underbrace{1}_{\in S}(1 \cdot s_1 - s_1 \cdot 1) - \underbrace{1}_{\in S}(1 \cdot s_1 - s_1 \cdot 1) = 0.. \tag{11.6.11}$$
- Finally,
$$\begin{aligned} \frac{r}{s}\left(\frac{m_1}{t_1} + \frac{m_2}{t_2}\right) &= \frac{r}{s}\left(\frac{t_2 m_1 + t_1 m_2}{t_1 t_2}\right) = \frac{r(t_2 m_1 + t_1 m_2)}{s t_1 t_2} \\ &= \frac{r t_2 m_1 + r t_1 m_2}{s t_1 t_2} = \frac{r t_2 m_1}{s t_1 t_2} + \frac{r t m_2}{s t_1 t_2} = \frac{r}{s} \cdot \frac{m_1}{t_1} + \frac{r}{s} \cdot \frac{m_2}{t_2}, \end{aligned}$$
where the reasoning in the last step above is similar to that of Equation (11.6.11).

□

Solution to Exercise 4.77. Let J be the ideal of the ring $S^{-1}A$ generated by $j(I)$. As an ideal of $S^{-1}A$, J is a submodule of $S^{-1}A$ when we identify $S^{-1}A$ as a module over itself.

On the other hand, let $S^{-1}I$ be the $S^{-1}A$-module constructed as in Exercise 9.1 from the A-module I (that is, from the submodule I of A when viewing A as a module over itself). We claim $S^{-1}I$ and J can be canonically identified as $S^{-1}A$-modules.

- $S^{-1}I \subset (j(I))$: Let $m/t \in S^{-1}I$, so that $m \in I$. Then
$$\frac{m}{t} = \frac{1}{t} \cdot \frac{m}{1} = \underbrace{\frac{1}{t}}_{\in S^{-1}A} \cdot \underbrace{j(m)}_{\in j(I)} \in (S^{-1}A) \cdot j(I) \subset (j(I)).$$
- $(j(I)) \subset S^{-1}I$: Let $m/t \in (j(I))$. Then for some $n \in \mathbb{Z}_{\geqslant 1}$, $a_j \in A$, $b_j \in I$, $s_j \in S$, we have
$$\frac{m}{t} = \sum\nolimits_{j=1}^{n} \left(\frac{a_j}{s_j}\right) j(b_j).$$

Then

$$\frac{m}{t} = \sum\nolimits_{j=1}^{n} \frac{a_j}{s_j} \cdot \frac{b_j}{1} = \frac{\sum_{j=1}^{n} (\prod_{k=1, k \neq j}^{n} s_k) a_j b_j}{(\prod_{j=1}^{n} s_j)}.$$

This is an element of $S^{-1}I$, because the numerator is a linear combination elements in I, and the denominator is in S. □

Solution to Exercise 4.80. We can now prove the statement of Exercise 9.4

(a) Let $S = A \smallsetminus \mathfrak{p}$. Computing in $A_{\mathfrak{p}}$, we have

$$\sqrt{(0)} \quad \overset{\substack{\text{Exercise} \\ 8.2}}{=} \bigcap\nolimits_{\mathfrak{w} \in \operatorname{Spec} A} \mathfrak{w} = \bigcap\nolimits_{\substack{\mathfrak{q} \in \operatorname{Spec} A \\ \mathfrak{q} \supset \mathfrak{p}}} S^{-1}\mathfrak{q} \overset{\substack{\text{minimality} \\ \text{of } \mathfrak{p} \text{ in Spec } A}}{=} S^{-1}\mathfrak{p} \overset{\substack{\text{Exercise} \\ 9.2}}{=} \mathfrak{p}A_{\mathfrak{p}},$$

where the second inequality is because the map $S^{-1} \colon A \to S^{-1}A$ via $q \mapsto q/1$ induces an inclusion-preserving bijection of $\{\mathfrak{q} \in \operatorname{Spec} A \mid \mathfrak{p} \supset \mathfrak{q}\}$ onto $\operatorname{Spec}(A_{\mathfrak{p}})$. Hence $\mathfrak{p}A_{\mathfrak{p}}$ is the nilradical of the local ring $A_{\mathfrak{p}}$, and in particular all elements of $\mathfrak{p}A_{\mathfrak{p}}$ are nilpotent in $A_{\mathfrak{p}}$. Before showing that if A is reduced then $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ is a field, we prove an important result.

Lemma 11.7.

If A is a commutative ring and $\mathfrak{p} \in \operatorname{Spec} A$, then $A_{\mathfrak{p}}$ is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$.

Proof of Lemma 11.7. It suffices to show $A_{\mathfrak{p}} \smallsetminus \mathfrak{p}A_{\mathfrak{p}} = A_{\mathfrak{p}}^{\times}$.

($\subset$): Suppose $f/s \in A_{\mathfrak{p}} \smallsetminus \mathfrak{p}A_{\mathfrak{p}}$. Then $f \notin \mathfrak{p}$, since otherwise $f/s \in \mathfrak{p}A_{\mathfrak{p}}$ since $1/s \in A_{\mathfrak{p}}$. But this means $f \in A \smallsetminus \mathfrak{p}$, so $j(f) = f/1$ is a unit of $A_{\mathfrak{p}}$, since its inverse $1/f$ is an element of $A_{\mathfrak{p}}$ by construction. Hence $A_{\mathfrak{p}} \smallsetminus \mathfrak{p}A_{\mathfrak{p}} \subset A_{\mathfrak{p}}^{\times}$.

($\supset$): Suppose $f/s \in A_{\mathfrak{p}}^{\times}$. Then there exists $g/t \in A_{\mathfrak{p}}$ such that $fg/st = 1/1$ in $A_{\mathfrak{p}}$. Equivalently, there exists $u \in A \smallsetminus \mathfrak{p}$ such that $u(1 \cdot fg - st \cdot 1) = 0$. Since $0 \in \mathfrak{p}$ and $u \notin \mathfrak{p}$, we must have $fg - st \in \mathfrak{p}$ because $\mathfrak{p}$ is prime. But primality of $\mathfrak{p}$ also implies that $st \notin \mathfrak{p}$, since $s, t \notin \mathfrak{p}$. Thus $fg = st$ is not in $\mathfrak{p}$. If $f \in \mathfrak{p}$, then since $\mathfrak{p}$ is an ideal we must have $fg = st \in \mathfrak{p}$, a contradiction, so we conclude $f \notin \mathfrak{p}$. Hence $f/s \in A_{\mathfrak{p}} \smallsetminus \mathfrak{p}A_{\mathfrak{p}}$, so $A_{\mathfrak{p}}^{\times} \subset A_{\mathfrak{p}} \smallsetminus \mathfrak{p}A_{\mathfrak{p}}$. This completes the proof. □

Now suppose A is reduced. Then $A_{\mathfrak{p}}$ is reduced for the following reason: If A is reduced and $(a, s) \in S^{-1}A$, $a \in A$, $s \in S$ such that $(a, s)^n = 0$, then $(a^n, s^n) = (0, 1)$. In A we have $a^n 0 = 0$ for some $u \in S$, so $a^n u = 0$ for some $u \in S$. Then $a^n u^n = (au)^n = 0$, so $au = 0$. But then $(a, s) = (0, 1)$, so $A_{\mathfrak{p}}$ is reduced. It follows that $\mathfrak{p}A_{\mathfrak{p}} \subset \sqrt{(0)} = (0)$, so

$$A_{\mathfrak{p}} \cong A_{\mathfrak{p}}/(0) \cong A_{\mathfrak{p}}/\sqrt{(0)} = A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}},$$

which is a field because $\mathfrak{p}A_{\mathfrak{p}}$ is a (the) maximal ideal of $A_{\mathfrak{p}}$ by Lemma 11.7.

(b) For each $\mathfrak{p} \in \operatorname{Spec} A$, let $j_{\mathfrak{p}} : A \to A_{\mathfrak{p}}$ be the natural localization map $a \mapsto a/1$. We claim

$$\begin{aligned} \Pi \colon A &\longrightarrow \prod\nolimits_{\substack{\text{minimal} \\ \mathfrak{p} \in \operatorname{Spec} A}} j_{\mathfrak{p}}, \\ a &\longmapsto \prod\nolimits_{\substack{\text{minimal} \\ \mathfrak{p} \in \operatorname{Spec} A}} j_{\mathfrak{p}}(a) \end{aligned}$$

is injective. We know this map is a ring homomorphism by the universal mapping property of the Cartesian product of modules, and its kernel is

$$\ker \Pi = \bigcap\nolimits_{\substack{\text{minimal} \\ \mathfrak{p}\,\in\,\operatorname{Spec} A}} \ker j_{\mathfrak{p}} = \bigcap\nolimits_{\substack{\text{minimal} \\ \mathfrak{p}\,\in\,\operatorname{Spec} A}} \{a \in A \mid sa = 0 \text{ in } A \text{ for some } s \in A \smallsetminus \mathfrak{p}\}.$$

It follows that if $x \in \ker \Pi$, then for all minimal prime ideals $\mathfrak{p}$, there exists $s_{\mathfrak{p}} \in A_{\mathfrak{p}}$ such that $s_{\mathfrak{p}} x = 0 \in \mathfrak{p}$. But $s_{\mathfrak{p}} \notin \mathfrak{p}$, so $x \in \mathfrak{p}$ since $\mathfrak{p}$ is prime. Before continuing, we need the following result:

Lemma 11.8.

If $\mathfrak{p}$ is a prime ideal of a nonzero commutative ring A, then $\mathfrak{p}$ contains some minimal prime ideal $\mathfrak{p}_0$.

Proof of Lemma 11.8. Since A is nonzero, it contains a maximal (hence prime) ideal $\mathfrak{p}$. Thus the set $\operatorname{Spec} A$ of all prime ideals of R is nonempty, and it is ordered by reverse-inclusion. Let A be a totally ordered subset of $\operatorname{Spec} A$. Then A is bounded above (with respect to reverse-inclusion) by the ideal $J = \bigcap_{I \in A} I$, which is an element of $\operatorname{Spec} A$ because it is prime: to see A is prime, let $xy \in J$. Then $xy \in I$ for all $I \in A$. Now let $B = \{I \in A \mid y \in I\}$. Let $K = \bigcap_{I \in B} I$. Since A is totally ordered, either $K = J$ (and we're done, since then $y \in J$) or $K \supset J$ and for all $I \in A$ such that I is properly contained in K, we have $y \notin I$. But that means that for all those $I, x \in I$, since they are prime. Hence $x \in J$. In either case, J is prime as desired. Hence by Zorn's lemma we get a maximal element which in this case is a minimal prime ideal. Thus if $\mathfrak{p}$ is any prime ideal of A, then by the argument above $A_{\mathfrak{p}}$ has a minimal prime ideal $\mathfrak{p}_0'$. Then by Corollary 4.43, $\mathfrak{p}_0'$ pulls back to a minimal ideal $\mathfrak{p}_0$ of A contained in $\mathfrak{p}$. □

Thus by Lemma 11.8 all prime ideals $\mathfrak{q}$ of A contain some minimal prime ideal $\mathfrak{p}_0$, so it follows that x is contained in *all* prime ideals of A, and in particular $x \in \bigcap_{\mathfrak{p}\,\in\,\operatorname{Spec} A} \mathfrak{p}$, and this intersection equals $\sqrt{(0)}$ by Exercise 8.2. But $\sqrt{(0)} = 0$ since A is reduced, so $x = 0$. Since x was an arbitrary element of $\ker \Pi$, we conclude Π is injective. Hence Π is an isomorphism. This completes the proof of Exercise 9.4. □

Note that the argument above shows the following useful fact:

Corollary 11.9.

If A is a commutative ring, then

$$A = \bigcap\nolimits_{\mathfrak{p}\,\in\,\operatorname{Spec} A} \mathfrak{p} = \bigcap\nolimits_{\substack{\text{minimal} \\ \mathfrak{p}\,\in\,\operatorname{Spec} A}} \mathfrak{p}.$$

Solution to Exercise 4.81. Let $A = \mathbb{C}[x, y]$. The collection of zerodivisors of $A/(xy)$ is precisely $(x) \cup (y)$, so we can write $\operatorname{Frac}(A/(xy)) = S^{-1}(A/(xy))$ for $S = A \smallsetminus ((x) \cup (y))$. Since

$$\operatorname{Frac}(A/(xy)) = S^{-1}(A/(xy)) \cong S^{-1}A/S^{-1}((xy)),$$

it suffices to exhibit a surjective ring homomorphism $S^{-1}A \to \mathbb{C}(x) \times \mathbb{C}(y)$ with kernel $S^{-1}((xy))$. Define $\psi_x \colon A \to \mathbb{C}(x)$ by $\psi_x(f) \coloneqq f(x, 0)/1$. (Well-definedness is clear since $A = \mathbb{C}[x, y]$.)

- ψ_x *is a well-defined surjective ring homomorphism*: If $f, g \in A$ then $\psi_x(1) = 1/1$, $\psi(f) + \psi_x(g) = f(x,0)/1 + g(x,0)/1 = (f+g)(x,0)/1 = \psi_x(f+g)$, and $\psi_x(f)\psi_x(g) = \frac{f(x,0)}{1} \cdot \frac{g(x,0)}{1} = \frac{(f \cdot g)(x,0)}{1} = \psi_x(fg)$. Thus ψ_x is a ring homomorphism.
- ψ *descends to a well-defined ring homomorphism* $\widetilde{\psi}_x \colon S^{-1}A \to \mathbb{C}(x)$: If $f \in S$ then $\psi(f) = f(x,0) \neq 0$ in $\mathbb{C}(x)$, since otherwise $f \in (y)$, contradicting $f \in S = \mathbb{C}[x,y] \smallsetminus ((x) \cup (y))$. Thus $\psi_x(f) \in \mathbb{C}(x)^\times$, so $\psi_x(S) \subset \mathbb{C}(x)^\times$ since f was an arbitrary element of S. Then by the universal mapping property of localization, there exists a unique ring homomorphism $\widetilde{\psi}_x \colon S^{-1}A \to \mathbb{C}(x)$ such that $\widetilde{\psi}_x \circ j = \psi_x$. By the proof of this result, the formula for $\widetilde{\psi}_x$ at any $f/s \in S^{-1}A$ is
$$\widetilde{\psi}_x(f/s) = \psi_x(s)^{-1}\psi_x(f) = f(x,0)/s(x,0).$$
- $\widetilde{\psi}_x$ *is surjective:* Suppose $f(x)/g(x) \in \mathbb{C}(x)$, so that $g(x)$ is a nonzero element of $g(x)$. Then $\frac{f(x)+y}{g(x)+y}$ is an element of $S^{-1}A$, which can be seen as follows. If $g(x) + y \notin S$ then either $g(x) + y \in (x)$ or $g(x) + y \in (y)$. The former case fails, since otherwise y can be written as a polynomial in x, so we may assume $g(x) + y \in (y)$. But then $g(x) = 0$, a contradiction. Thus $\frac{f(x)+y}{g(x)+y} \in S^{-1}A$, and its image under $\widetilde{\psi}_x$ is
$$\widetilde{\psi}_x\left(\frac{f(x)+y}{g(x)+y}\right) = \psi_x(g(x)+y)^{-1}\psi_x(f(x)+y) = (g(x)+0)^{-1}(f(x)+0) = f(x)/g(x),$$
as desired.
- $\ker\widetilde{\psi}_x = S^{-1}((y))$*:* Note $f/s \in \ker\widetilde{\psi}_x$ if and only if $\psi_x(s)^{-1}\psi_x(s) = 0$. Because $\widetilde{\psi}_x(s(x))$ is a unit in $\mathbb{C}(x)$ and hence not a zerodivisor in $\mathbb{C}(x)$, this happens if and only if $\psi_x(f(x,y)) = 0$. Since $\psi_x(f(x,y)) = f(x,0)$, we conclude $f(x,y)/s(x,y) \in \ker\widetilde{\psi}_x$ if and only if $f(x,y) \in (y)$. Thus
$$\ker\widetilde{\psi}_x = \left\{ \frac{f(x,y)}{s(x,y)} \in S^{-1}A \;\middle|\; f(x,y) \in (y) \text{ in } \mathbb{C}[x,y] \right\} = (y)(S^{-1}A) = S^{-1}((y)).$$

In summary, we obtained a ring homomorphism $\widetilde{\psi}_x \colon \mathbb{C}[x,y] \to \mathbb{C}(x)$ with kernel $S^{-1}((y))$.

Running through the exact same arguments as above, *mutatis mutandis*, we obtain a surjective ring homomorphism $\widetilde{\psi}_y \colon \mathbb{C}[x,y] \to \mathbb{C}(y)$ with kernel $S^{-1}((x))$. Then the product ring homomorphism $\Pi \coloneqq \widetilde{\psi}_x \times \widetilde{\psi}_y \colon S^{-1}(\mathbb{C}[x,y])$ is surjective ring homomorphism with kernel
$$\ker\widetilde{\psi}_x \cap \ker\widetilde{\psi}_y = S^{-1}((x)) \cap S^{-1}((y)) = S^{-1}((x) \cap (y)) = S^{-1}((xy)),$$
where we used that $(x) \cap (y) = (xy)$. (Indeed, if $x \in (x) \cap (y)$ then we can write $f(x,y)$ as both $xh(x,y)$ and $yk(x,y)$ for some $h(x,y), k(x,y) \in \mathbb{C}[x,y]$, so both x and y divide $f(x,y)$, and hence $f(x,y) \in (xy)$. Conversely, if $f \in (xy)$ then $f \in (x) \cap (y)$ because $(xy) = (x)(y) \subset (x) \cap (y)$.) Thus $\ker\Pi = S^{-1}((xy))$, so by the first isomorphism theorem Π descends to an isomorphism $\operatorname{Frac}(\mathbb{C}[x,y]/(xy)) \xrightarrow{\cong} \mathbb{C}(x) \times \mathbb{C}(y)$. □

Proof of Proposition 5.4. (1) $\iff$ (2) is a formality of partially ordered sets: given (2), a chain $N_0 \subset N_1 \subset \cdots$ in M has a maximal element, and hence stabilizes; given (1), if $T \in \Sigma$ has no maximal element, then we can inductively construct a non-terminating chain—namely, choose $N_0 \in T$; since N_0 is not maximal, there exists $N_1 \in T$ such that $N_0 \subsetneq N_1$, and so on.

(2) $\implies$ (3): Let N be a submodule of M, and let Σ be the set of finitely generated A-submodules of N. Then $\Sigma \neq \varnothing$ because $(0) \in \Sigma$, so Σ has a maximal element $N_0 \subset N$ with respect to inclusion. If $N_0 \neq N$, then for any $n \in N \smallsetminus N_0$, we have $N_0 \subsetneq N_0 + A \cdot n \subset N$, and $N_0 + Ani$s still finitely generated. Thus $N_0 = N$ (is finitely generated).

(3) $\implies$ (1): Let $N_0 \subset N_1 \subset \cdots$ be a chain of submodules of M. Then $N = \bigcup_{j=0}^{\infty}$ is a submodule of M (because it is a chain! We saw a similar argument for ideals), and hence is finitely generated, that is, $N = \sum_{i=1}^{r} A_{x_i}$ with $x_i \in N_{j_i}$ for some j_i.

Let $k = \max\{j_1, \dots, j_r\}$. Then for all i, $x_i \in N_k$, and thus $N = N_k$, so the chain stabilizes. □

Proof of Lemma 5.6. Assume M is Noetherian. Any chain of submodules $N_0 \subset N_1 \subset \cdots$ of M_1 (resp. M_2) gives a chain of submodules M via $i(N_0) \subset i(N_1) \subset \cdots$ (resp. $\pi^{-1}(N_0) \subset \pi^{-1}(N_1) \subset \cdots$); this chain stabilizes in M, and hence so too does the original chain by taking i^{-1} (resp. π).

Conversely, assume M_1 and M_2 are Noetherian and let $N_0 \subset N_1 \subset \cdots$ be a chain of submodules of M. Then $\{i^{-1}(N_\ell)\}_{\ell \geqslant 0}$ and $\{\pi(N_\ell)\}_{\ell \geqslant 0}$ are chains of submodules of M_1 and M_2, and hence becomes stable for all $\ell \geqslant \ell_0$ for some ℓ_0. The same holds for N_ℓ: for $\ell \geqslant \ell_0$, we have a commutative diagram of the form

$$\begin{tikzcd}
0 \arrow[r] & i^{-1}(N_2) \arrow[r] \arrow[d, equal] & N_\ell \arrow[r] \arrow[d, hook] & \pi(N_\ell) \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & i^{-1}(N_{\ell+1}) \arrow[r] & N_{\ell+1} \arrow[r] & \pi(N_{\ell+1}) \arrow[r] & 0
\end{tikzcd}$$

with exact rows, from which we see $N_\ell = N_{\ell+1}$ by a straightforward diagram chase. □

Proof of Proposition 5.8. (1) $\implies$ (2): This is immediate from the last proposition.

(2) $\implies$ (1): M is finitely generated over A means there exist $m_1, \dots, m_r \in M$ such that $M = \sum_{i=1}^{r} Am_i$. Thus the map $A^n \to M$ given by $(a_1, \dots, a_n) \mapsto a_1m_1 + \cdots + a_nm_n$ is surjective. Since A is Noetherian (as a ring), A is a Noetherian A-module. By Lemma 5.6, A^n is thus also a Noetherian A-module, which can be seen by induction using the short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & A^{n-1} \arrow[r, "{(x_1,\dots,x_n)\mapsto(x_1,\dots,x_{n-1},0)}"] & A^n \arrow[r, "{(x_1,\dots,x_{n-1},x_n)\mapsto x_n}"'] & A \arrow[r] & 0
\end{tikzcd}$$

and because quotients of Noetherian A-modules are Noetherian. Hence, by another application of Lemma 5.6, we conclude M is Noetherian. □

Proof of Proposition 5.21. Suppose x is not a product of irreducible elements. Then $x = x_1a$ for some $x_1, a \notin R^\times$, $x_1 = x_2a'$, $x_2 = x_3a''$, and so on. Then

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

is a strictly increasing chain of ideals, so R is not Noetherian. □

Proof of Theorem 5.24. Let $I \subset A[x]$ be an ideal. We want to show I is finitely generated. Consider the set $LT(I)$ of leading coefficients of elements of I. More precisely, for $f \in A[x]$, define

$$LT(f) \coloneqq \begin{cases} 0 & \text{if } f = 0, \\ a_n & \text{if } f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 \text{ such that } a_n \neq 0 \text{ and } a_i \in A. \end{cases}$$

and define

$$LT(I) \coloneqq \{LT(f) \mid f \in I\}.$$

- *$LT(I)$ is an ideal of A*: We have $LT(0) = 0$, and for $f \in I$ we have $LT(-f) = -LT(f)$, so $LT(I)$ has inverses. More generally, for all $c \in A$, $LT(c \cdot f) = c \cdot LT(f)$, so $LT(I)$ is stable under A-multiplication. $LT(I)$ is closed under addition, since $0 \in LT(I)$, and it is enough to check that for $f, g \in I$ such that $LT(f) + LT(g) \neq 0$, then $LT(f) + LT(g) \in LT(I)$. We may assume $\deg f \geqslant \deg g$. Then
$$LT(\underbrace{f + x^{\deg(f)-\deg(g)} \cdot g}_{\in I}) = LT(f) + LT(g),$$
as desired. (So, we have avoided the cancellation that could have happened in $f + x^{\deg(f)-\deg(g)} \cdot g$ by restricting to the case $LT(f) + LT(g) \neq 0$.)

Since A is Noetherian, $LT(I)$ is finitely generated, by some $a_1, \dots, a_r \in LT(I)$. By definition, there exist $f_i \in I$ such that $LT(f_i) = a_i$ for each $i \in \{1, \dots, r\}$. Then the ideal

$$I' \coloneqq (f_1, \dots, f_r)$$

is an ideal of $A[x]$ contained in I. Let

$$d \coloneqq \max_{i \in \{1,\dots,r\}} \deg(f_i),$$

and let $M \subset A[x]$ be the A-submodule spanned by $\{1, x, \dots, x_{d-1}\}$. (So M is the collection of polynomials of degree $< d$).

- *For all $f \in I$, there exist $g \in M$ and $h \in I'$ such that $f = g + h$, that is, such that $I = \underbrace{M \cap I}_{g \,=\, f-h \,\in\, I} + I'$*: If $\deg(f) < d$, then this is clear because $g = f$ and $h = 0$. If $\deg(f) \geqslant d$, then since $LT(f) \in LT(I) = (a_1, \dots, a_n) \subset A$, then $LT(f) = \sum_{i=1}^{r} c_i a_i$ for some $c_i \in A$. Next consider $F \coloneqq f - \sum x^{\deg(f)-\deg(f_i)} \cdot c_i \cdot f_i$. Then $\deg(F) < \deg(f)$, since the leading term cancelled out. Then the claim follows by iterating this argument inductively.

Now M is a finitely generated A-module, and hence is a Noetherian A-module by a previous proposition, so the A-submodule $M \cap I \subset M$ is also finitely generated as an A-module, say by $g_1, \dots, g_s \in I$. Then

$$I = (g_1, \dots, g_s, f_1, \dots, f_r) \text{ is finitely generated.}$$ □

Proof of Corollary 5.25. We argue by induction on $n \in \mathbb{Z}_{\geqslant 1}$. The base case $n = 1$ is just Hilbert's basis theorem. In the general case, recall that by Theorem 1.61 a finitely generated A-algebra is isomorphic to a quotient $A[x_1, \dots, x_n]/I$ for some $n \in \mathbb{Z}_{\geqslant 1}$ and some ideal I, and hence is Noetherian by the induction hypothesis. □

Solution to Exercise 5.27. (a) We first show $\sqrt{I+J} \subset \sqrt{\sqrt{I}+\sqrt{J}}$. Note that if K, L are ideals of a commutative ring and $K \subset L$, then $\sqrt{K} \subset \sqrt{L}$. (To see this, consider an arbitrary $a \in \sqrt{K}$. Then there exists $n \in \mathbb{Z}_{\geqslant 1}$ such that $a^n \in K$. But $K \subset L$, so $a^n \in L$. Therefore, $a \in \sqrt{L}$.) Given that $I \subset \sqrt{I}$ and $J \subset \sqrt{J}$, it follows that $I + J \subset \sqrt{I} + \sqrt{J}$.

It remains to show $\sqrt{\sqrt{I}+\sqrt{J}} \subset \sqrt{I+J}$. Suppose $f^n \in \sqrt{I} + \sqrt{J}$ for some $n \in \mathbb{Z}_{\geqslant 1}$. This means that $f^n = a + b$ for some $a \in \sqrt{I}$ and $b \in \sqrt{J}$, so there exist $m_1, m_2 \in \mathbb{Z}_{\geqslant 1}$ such that $a^{m_1} \in I$ and $b^{m_2} \in J$. We claim $f^{n(m_1+m_2)} \in \sqrt{I+J}$. We have

$$f^{n(m_1+m_2)} = (a+b)^{m_1+m_2} = \sum\nolimits_{j=0}^{m_1+m_2} \binom{m_1+m_2}{j} G_j,$$

where $G_j = a^j b^{m_1+m_2-j}$. (Note that we used commutativity of A to obtain the second equality above.) It is enough to show that for all $j \in \{0, \ldots, m_1+m_2\}$, either $G_j \in I$ or $G_j \in J$.

- If $m_1 \leqslant m_2$, then for $j \leqslant m_2$, $G_j \in J$ since $b^{m_1+m_2-j} \in J$ (since $m_1 + m_2 - j \geqslant m_2$). For $j \geqslant m_2$, $a^j \in I$ (since $j \geqslant m_1$), so $G_j \in I$.
- If $m_2 \leqslant m_1$, then, arguing similarly as the previous point, if $j \leqslant m_1$ then $G_j \in J$ and if $j \geqslant m_1$ then $G_j \in I$.

We conclude $f^{n(m_1+m_2)} \in I + J$, so $f \in \sqrt{I+J}$. Since $\sqrt{\sqrt{I}+\sqrt{J}} \subset \sqrt{I+J}$, which gives us $\sqrt{I+J} = \sqrt{\sqrt{I}+\sqrt{J}}$.

(b) Suppose $\sqrt{I} + \sqrt{J} = A$. Then

$$A = \sqrt{A} = \sqrt{\sqrt{I}+\sqrt{J}} = \sqrt{I+J},$$

where the last equality is by part (a), so in particular $1 \in \sqrt{I+J}$. But this means there exists $n \in \mathbb{Z}_{\geqslant 1}$ such that $1 = 1^n \in I + J$, so $I + J$ is the unit ideal, hence $I + J = A$.

(c) Let $n \in \mathbb{Z}_{\geqslant 1}$ and suppose $\mathfrak{p} \in \operatorname{Spec} A$. $\mathfrak{p} \subset \sqrt{\mathfrak{p}^n}$ because any $x \in \mathfrak{p}$ has $x^n \in \mathfrak{p}^n$, hence $x \in \sqrt{\mathfrak{p}^n}$. To see $\sqrt{\mathfrak{p}^n} \subset \mathfrak{p}$, note that if $a \in A \smallsetminus \mathfrak{p}$ then $a^m \in A \smallsetminus \mathfrak{p}$ for all $m \in \mathbb{Z}_{\geqslant 1}$ (because $A \smallsetminus \mathfrak{p}$ is multiplicatively closed), and in particular $a^n \in A \smallsetminus \mathfrak{p}^n$ (since $\mathfrak{p}^n \subset \mathfrak{p} \implies A \smallsetminus \mathfrak{p} \subset A \smallsetminus \mathfrak{p}^n$). Thus $a \notin \sqrt{\mathfrak{p}}$, so $\mathfrak{p} \supset \sqrt{\mathfrak{p}^n}$, which implies $\mathfrak{p} = \sqrt{\mathfrak{p}^n}$.

Now suppose $k, \ell \geqslant 1$ and let $\mathfrak{m}_1, \mathfrak{m}_2$ be distinct maximal ideals of A. We want to show $\sqrt{\mathfrak{m}_1^k} + \sqrt{\mathfrak{m}_2^\ell} = A$, in which case we are done by part (b). Since maximal ideals are prime, our argument in the previous paragraph shows that $\sqrt{\mathfrak{m}_1^k} = \mathfrak{m}_1$ and $\sqrt{\mathfrak{m}_2^\ell} = \mathfrak{m}_2$, so it suffices to show $\mathfrak{m}_1 + \mathfrak{m}_2 = A$. But this is clear: the fact $\mathfrak{m}_1 \neq \mathfrak{m}_2$ implies $\mathfrak{m}_1, \mathfrak{m}_2 \subsetneq \mathfrak{m}_1 + \mathfrak{m}_2$, which by maximality of $\mathfrak{m}_1, \mathfrak{m}_2$ forces $\mathfrak{m}_1 + \mathfrak{m}_2 = A$, as desired. □

Solution to Exercise 5.28. (a) Let I be an ideal of A. Since A is Noetherian, we can write $\sqrt{I} = (x_1, \ldots, x_r)$ for some $x_1, \ldots, x_r \in \sqrt{I}$. For each $j \in \{1, \ldots, r\}$, there exists $m_j \in \mathbb{Z}_{\geqslant 1}$ such that $x_j^{m_j} \in I$ (since $x_j \in \sqrt{I}$).

We claim $(\sqrt{I})^n \subset I$ when $n = r \max\{m_1, \ldots, m_r\}$. To see this, consider an arbitrary $q \in (\sqrt{I})^n$. We can write

$$q = \sum\nolimits_{k=1}^{N} y_{k,1} \cdots y_{k,n}$$

for some $N \in \mathbb{Z}_{\geqslant 1}$ and some $y_{k,j}$ for each $k \in \{1, \ldots, N\}$, for all $j \in \{1, \ldots, n\}$. Since

$\sqrt{I} = (x_1, \dots, x_r)$, we can write

$$y_{k,j} = \sum\nolimits_{\ell=1}^{N_{k,j}} a_{k,\ell,j} x_\ell$$

for some $a_{j,k,\ell} \in A$ and some $N_{k,j} \in \mathbb{Z}_{\geqslant 1}$, for all $\ell \in \{1, \dots, N_{k,\ell}\}$ and all $j \in \{1, \dots, n\}$. Hence

$$q = \sum\nolimits_{k=1}^{N} \Big(\prod\nolimits_{j=1}^{n} \Big(\sum\nolimits_{\ell=1}^{N_{k,j}} a_{k,\ell,j} x_\ell \Big) \Big).$$

After expanding out (or by observing that the product of n terms, each of which have some x_j as a factor), we see that each term has at least n factors that are elements of the set $\{x_1, \dots, x_r\}$, which has r elements. Since $n = r \cdot \max\{m_1, \dots, m_r\}$, by the pigeonhole principle each term has at least one factor in I. (Note that this requires A be commutative to collect the x_j into $x_j^{m_j}$; whatever that j may be depends on the term in question, but this shows that at least one exists, which is all we need.) Hence $q \in I$.

(b) By part (a), the ideal (0) contains some power of $\sqrt{(0)}$, that is, $(\sqrt{(0)})^n = 0$ for some $n \in \mathbb{Z}_{\geqslant 1}$. Thus $\sqrt{(0)}$ is nilpotent.

(c) Consider commutative ring $A = \mathbb{C}[x_1, x_2, x_3, \dots]$ and the ideal $I = (x_1^1, x_2^2, x_3^3, \dots)$ of A. We claim the nilradical of A/I is the ideal $(x_1, x_2, x_3, \dots) + I$.

($\supset$) If $a \in (x_1, x_2, x_3, \dots) + I$ then a is a linear combination of elements $x_j + I$, each of which are in the nilradical (because $x_j^j \in I$ for each j, so $(x_j + I)^j = x_j^j + I = I$, which is the zero element of A/I), so because the nilradical is an ideal we conclude $a \in \sqrt{(0)}$.

($\subset$) Now suppose an element $a + I$ of A/I satisfies $(a + I)^n = 0 + I$ for some $n \in \mathbb{Z}_{\geqslant 1}$. Then $a^n + I = 0 + I$, so in A we have $a^n \in I = (x_1^1, x_2^2, x_3^3, \dots) \subset (x_1, x_2, \dots)$, so a^n. Hence $a + I \subset (x_1, x_2, x_3, \dots) + I$ in A/I.

We conclude the nilradical of A/I is the ideal $\sqrt{(0)} = (x_1, x_2, x_3, \dots) + I$. But $(x_1, x_2, x_3, \dots)$ is not nilpotent, since for any $n \in \mathbb{Z}_{\geqslant 1}$, the element $x_{n+1}^n \in (\sqrt{(0)})^n$ but $x_{n+1}^n \neq 0$. Then by (b), A/I must be non-Noetherian. Thus A/I is an example of a non-Noetherian commutative ring with non-nilpotent nilradical. □

Solution to Exercise 5.29. Suppose for a contradiction $M \neq 0$. Then there exists a minimal generating set $\{m_1, \dots, m_n\}$ of M for some $n \in \mathbb{Z}_{\geqslant 1}$. By hypothesis $M = J(A)M$, so $m_n = a_1 m_1 + \cdots + a_{n-1} m_{n-1} + a_n m_n$ for some $a_1, \dots, a_n \in J(A)$. We can rewrite this as

$$(1 - a_n) m_n = a_1 m_1 + \cdots + a_{n-1} m_{n-1}.$$

The element $1 - a_n$ is a unit in A by definition of $J(A)$, so multiplying through by $b \coloneqq (1 - a_n)^{-1}$ we obtain

$$m_n = b a_1 m_1 + \cdots + b a_{n-1} m_{n-1}.$$

But then $\{m_1, \dots, m_{n-1}\}$ is a generating set for M, contradicting the minimality of the original generating set. Hence $M = 0$. □

Solution to Exercise 5.30. First note that (a) and (b) are mutually exclusive: if we assume $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ for all $n \in \mathbb{Z}_{\geqslant 1}$, then because $\mathfrak{m}^{n+1} \subset \mathfrak{m}^n$ we know if $\mathfrak{m}^n = 0$ for some n, then $\mathfrak{m}^{n+1} = 0 = \mathfrak{m}^n$, contrary to our assumption.

Now we can assume for any $n \in \mathbb{Z}_{\geqslant 1}$ that $\mathfrak{m}^n = \mathfrak{m}^{n+1}$. Given $n \in \mathbb{Z}_{\geqslant 1}$, we need to show $\mathfrak{m}^n = 0$. Since A is Noetherian, $\mathfrak{m}^n$ is finitely generated as an A-module (since $\mathfrak{m}^n$ is a submodule of A when equipping A with the natural A-module structure.) Since A is local with maximal ideal $\mathfrak{m}$, we have

$$J(A) \overset{(8.3)}{=} \bigcap\nolimits_{\mathfrak{m} \in \operatorname{Max}(A)} \mathfrak{m} = \mathfrak{m},$$

so

$$J(A)\mathfrak{m}^n = \mathfrak{m} \cdot \mathfrak{m}^n = \mathfrak{m}^{n+1} = \mathfrak{m}^n,$$

where the last equality is by assumption. Applying Nakayama's Lemma (Exercise 10.3), we conclude $\mathfrak{m}^n = 0$. □

Solution to Exercise 5.31. If $\ker f = 0$ then f is an isomorphism, so we may assume $\ker f \neq 0$. Since M is Noetherian and $0 \subsetneq \ker f \subset \ker(f \circ f) \subset \cdots$ is an ascending chain of submodules of M, there exists $k \in \mathbb{Z}_{\geqslant 1}$ such that

$$\ker f^{\circ k} = \ker f^{\circ(k+1)} = \cdots . \tag{11.9.1}$$

Suppose $x \in \ker f$. Note that $f^{\circ k}$ is surjective since f is, so there exists $m \in M$ such that $f^{\circ k}(m) = x$. But then

$$f^{\circ(k+1)}(m) = f(f^{\circ k}(m)) = f(x) = 0,$$

so $m \in \ker f^{\circ(k+1)} \overset{(11.9.1)}{=} \ker f^{\circ k}$. But then $x = f^{\circ k}(m) = 0$, so since x was an arbitrary element of $\ker f$, we conclude $\ker f = \{0\}$. □

Proof of Proposition 6.4. Suppose $\mathfrak{p} \in \operatorname{Spec} A$, so that $A/\mathfrak{p}$ is an integral domain. It is enough to show $A/\mathfrak{p}$ is a field. Let $x \in (A/\mathfrak{p}) \smallsetminus \{0\}$ and consider the descending chain $(x) \supset (x^2) \supset (x^3) \supset \cdots$. Since A and hence $A/\mathfrak{p}$ is Artinian, this chain stabilizes, so there exists $n \in \mathbb{Z}_{\geqslant 1}$ such that $(x^n) = (x^{n+1})$, that is, x^n is a multiple of x^n. But x^{n+1} is always a multiple of x^n, so there exists a unit $u \in A$ such that $x^n = x^{n+1} \cdot u$. Since $A/\mathfrak{p}$ is an integral domain and $x \neq 0$, $1 = x \cdot u$ in $A/\mathfrak{p}$. This shows x is a unit in $A/\mathfrak{p}$, so since x was an arbitrary element of $(A/\mathfrak{p}) \smallsetminus \{0\}$, we conclude $(A/\mathfrak{p}) \smallsetminus \{0\} = (A/\mathfrak{p})^\times$. Thus $A/\mathfrak{p}$ is a field. □

Proof of Proposition 6.8. Consider the set

$$\Sigma \coloneqq \{\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_k \mid k \in \mathbb{Z}_{\geqslant 1}, \mathfrak{m}_1, \ldots, \mathfrak{m}_k \in \operatorname{Max}(A)\}.$$

Σ is nonempty since A has maximal ideals (and because we may assume $A \neq 0$), so since A is Artinian Σ has a minimal element, say $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. (Here we are using the equivalent condition to being Artinian that any nonempty subset of ideals of A has a maximal element.)

Now let $\mathfrak{m}$ be any maximal ideal of A. Then $\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$ is an element of Σ and is contained in $\mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$, so by minimality $\mathfrak{m} \cap \mathfrak{m}_1 \cap \cdots \mathfrak{m}_n = \mathfrak{m}_1 \cap \cdots \cap \mathfrak{m}_n$. Thus $\mathfrak{m} \supset \mathfrak{m}_1 \cap \cdots \mathfrak{m}_n$, so by prime avoidance $\mathfrak{m} \supset \mathfrak{m}_i$ for some $i \in \{1, \ldots, n\}$. Since $\mathfrak{m}_i$ is maximal, $\mathfrak{m} = \mathfrak{m}_i$. Thus $\operatorname{Max}(A) = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$. □

Proof of Proposition 6.11. We have

$$\sqrt{(0)} \overset{(8.2)}{=} \bigcap\nolimits_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p} \overset{\text{(Artinian)}}{=} \bigcap\nolimits_{\mathfrak{m} \in \operatorname{Max}(A)} \mathfrak{m} = J(A).$$

Consider the chain

$$\sqrt{(0)} \supset (\sqrt{(0)})^2 \supset (\sqrt{(0)})^3 \supset \cdots .$$

Since A is Artinian, this chain stabilizes, say at $I \coloneqq (\sqrt{(0)})^k = (\sqrt{(0)})^{k+1} = \cdots$. We want to show $I = 0$. Indeed, consider the set

$$\Sigma \coloneqq \{\text{ideals } J \text{ of } A \mid J \cdot I \neq 0\}.$$

If $I \neq 0$, then $\Sigma \neq \varnothing$ (since $A \in \Sigma$). Then Σ has a maximal element J_0. In particular, there exists $x \in J_0$ such that $x \cdot I \neq 0$ (since $J_0 \cdot I = 0$). Then $(x) \subset J_0$ and $(x) \in \Sigma$, so $(x) = J_0$. Computing, we have

$$xI \cdot I = x \underbrace{I^2}_{=(\sqrt{(0)})^{2k} = (\sqrt{(0)})^k} = xI.$$

But then $xI \in \Sigma$, and $xI \subset (x) = J_0$, so again by minimality we must have $xI = (x)$. Thus $x \cdot y = x$ for some $y \in I$, and hence $x \cdot y^n = x$ for all $n \in \mathbb{Z}_{\geqslant 1}$. But $y \in I = (\sqrt{(0)})^k \subset \sqrt{(0)}$, that is, y is in the nilradical, so $\sqrt{(0)}^n = 0$ for some $n \in \mathbb{Z}_{\geqslant 1}$. Thus $x = 0$. Since x was an arbitrary element of I, we conclude $I = 0$. □

Proof of Proposition 6.14. By the proposition, every chain is finite, so any increasing or decreasing chain stabilizes.

Conversely, if M is Noetherian and Artinian, then there exists a maximal submodule M_1 of M (with respect to inclusion): indeed, if not, then there exists an infinite strictly increasing chain of submodules, contradicting M is Noetherian.

Similarly, M_1—which is Artinian and Noetherian as a submodule of the Artinian and Noetherian module M—has a maximal submodule, say M_2. Continuing this process, we obtain a strictly decreasing chain of submodules

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq M_3 \supsetneq \cdots ,$$

and M is Artinian, hence this sequence stabilizes. It therefore must stabilize at 0 (since otherwise we could obtain another maximal proper submodule to get yet another proper submodule, contradicting stabilization.) This completes the proof. □

Proof of Corollary 6.18. We know $\dim A = 0$ by Proposition 6.4, and $\operatorname{Spec} A = \operatorname{Max} A = \{\mathfrak{m}_1, \cdots, \mathfrak{m}_n\}$. Since there exists $k \in \mathbb{Z}_{\geqslant 1}$ such that $J(A)^k = 0$,

$$\prod_{i=1}^n \mathfrak{m}_i^k = \left(\prod_{i=1}^n \mathfrak{m}_i\right)^k \subset \left(\bigcap_{i=1}^n \mathfrak{m}_i\right)^k = 0.$$

The proof of the corollary is then completed by the following key lemma, Lemma 6.19. □

Proof of Lemma 6.19. Consider the chain of ideals

$$R \supset \mathfrak{n}_1 \supset \mathfrak{n}_1\mathfrak{n}_2 \supset \cdots \supset \mathfrak{n}_1 \cdots \mathfrak{n}_{r-1} \supset \mathfrak{n}_1 \cdots \mathfrak{n}_r = 0.$$

Let $gr_0 = R/\mathfrak{n}_1$ and $gr_i \coloneqq \mathfrak{n}_1 \cdots \mathfrak{n}_i / \mathfrak{n}_1 \cdots \mathfrak{n}_{i+1}$ for $i \in \{1, \ldots, r-1\}$. Each gr_i is an R-module where $\mathfrak{n}_{i+1}$ acts trivially, that is, it is an $R/\mathfrak{n}_{i+1}$-module, or equivalently a vector space over the field $R/\mathfrak{n}_{i+1}$. Now

$$\begin{aligned} R \text{ is Artinian (resp. Noetherian)} &\iff R \text{ is an Artinian (resp. Noetherian) } R\text{-module} \\ &\iff \text{for all } i \in \{0, \dots, r-1\},\ gr_i \text{ is an Artinian (resp. Noetherian) } R\text{-module} \\ &\qquad\qquad (\text{by applying Proposition 6.14 to } 0 \to \mathfrak{n}_1 \cdots \mathfrak{n}_{i+1} \to \mathfrak{n}_1 \cdots \mathfrak{n}_i \to gr_i \to 0) \\ &\iff \text{for all } i \in \{0, \dots, r-1\},\ gr_i \text{ is an Artinian (resp. Noetherian) } (R/\mathfrak{n}_{i+1})\text{-module.} \end{aligned}$$

Next note that

(1) gr_i is Noetherian as an $(R/\mathfrak{n}_{i+1})$-module if and only if $\dim_{R/\mathfrak{n}_{i+1}} gr_i < \infty$ (that is, the vector spaces gr_i is finite-dimensional) because a module over a Noetherian ring is Noetherian if and only if it is finitely generated.

(2) gr_i is Artinian if and only if $\dim_{R/\mathfrak{n}_{i+1}} gr_i < \infty$. (Indeed, if $\dim_{R/\mathfrak{n}_{i+1}} < \infty$, then any descending chain $gr_i \supset N_0 \supset N_1 \supset \cdots$ of $(R/\mathfrak{n}_{i+1})$-modules is a descending chain of vector subspaces, hence stabilizes.)

If $\dim_{R/\mathfrak{n}_{i+1}} gr_i = \infty$, with linear independent set $\{v_1, v_2, \dots\} \subset gr_i$, then $\operatorname{span}\{v_1, v_2, \dots,\} \supsetneq \operatorname{span}\{v_2, v_3, \dots\} \supsetneq \operatorname{span}\{v_3, v_4, \dots\} \supsetneq \cdots$ is an infinite strictly descending chain of $(R/\mathfrak{n}_{i+1})$-submodules of gr_i. Since (1) and (2) are the same condition, we conclude that R is Artinian if and only if R is Noetherian. □

Proof of Corollary 6.20. We know $\operatorname{Max}(A) = \{\mathfrak{m}_1, \mathfrak{m}_2, \dots, \mathfrak{m}_r\}$ for some $r \in \mathbb{Z}_{\geqslant 1}$, and

$$\prod_{i=1}^{n} \mathfrak{m}_i^k \overset{(10.3)}{=} \bigcap_{i=1}^{r} \mathfrak{m}_i^k = \left(\bigcap_{i=1}^{r} \mathfrak{m}_i\right)^k = 0 \text{ for some } k \geqslant 1.$$

Now consider the natural ring homomorphism $A \to \prod_{i=1}^r A/\mathfrak{m}_i^k$. Its kernel is the intersection $\bigcap_{i=1}^r \mathfrak{m}_i^k = 0$, and since for all $i \neq j$, $\mathfrak{m}_i^k + \mathfrak{m}_j^k \overset{10.2}{=} A$, by the Chinese remainder theorem the homomorphism is surjective. Thus $A \xrightarrow{\cong} \prod_{i=1}^r A/\mathfrak{m}_i^k$ is an isomorphism, and each $A/\mathfrak{m}_i^k$ are Artinian (as a quotient of an Artinian ring) and local (because the unique maximal ideal is now the ideal induced by $\mathfrak{m}_i$, or more precisely, because of the bijection $\operatorname{Max}(A/\mathfrak{m}_i^k) \leftrightarrow \{\mathfrak{m} \in \operatorname{Max}(A) \mid \mathfrak{m} \supset \mathfrak{m}_i^k\} = \{\mathfrak{m}_i\}$.) □

Proof of Proposition 6.21. Let A be Noetherian of dimension 0. By Theorem 6.52, A has finitely many minimal primes $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$. But since $\dim A = 0$, $\operatorname{Spec} A = \operatorname{Max} A$ is the collection of minimal primes of A, that is, $\{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$. By Exercise 10.2, $\sqrt{(0)}$ is nilpotent since A is Noetherian, so $\prod_{i=1}^k \mathfrak{p}_i^k = \bigcap_{i=1}^k \mathfrak{p}_i^k = 0$ for some $k \in \mathbb{Z}_{\geqslant 1}$ (as in an earlier argument). But by Lemma 6.19, since A is Noetherian and a finite product of maximal ideals is (0), we conclude A is Artinian. □

Proof of Proposition 6.25. We already know the forward implication. On the other hand, if R is Noetherian, then finiteness and discreteness of $\operatorname{Spec} R$ implies $\dim R = 0$, hence R is Artinian. □

Proof of Lemma 6.29. We give an inductive argument. Let Σ be the set of ideals of A for which the statement of the lemma is false for I, that is, the collection of all ideals that is not a finite intersection of irreducible ideals.

If $\Sigma = \varnothing$ then we are done, so suppose for a contradiction $\Sigma \neq \varnothing$. Since A is Noetherian, Σ has a maximal element I_0 (with respect to inclusion) by Proposition 5.4. In particular, I_0 is *not* irreducible. Then there exist ideals $J_1, J_2 \neq I_0$ such that $I_0 = J_1 \cap J_2$. Since J_1, J_2 strictly contain I_0 and I_0 is maximal in Σ, it follows that $J_1, J_2 \notin \Sigma$, hence J_1, J_2 are intersections of finitely many irreducible ideals. But then $I_0 = J_1 \cap J_2$ is an intersection of finitely many irreducible ideals, a contradiction. □

Proof of Proposition 6.31. By consulting the definitions, this is a straightforwrad chain of equivalences, which goes as follows:

$$\begin{aligned}
\mathfrak{p} \text{ is primary} &\iff \text{for all } x, y \in R, \text{ if } xy \in \mathfrak{p} \text{ and } x \notin \mathfrak{p} \text{ then } y^n \in \mathfrak{p} \text{ for some } n \in \mathbb{Z}_{\geqslant 1} \\
&\iff \text{for all } x, y \in R, \text{ if } (x+\mathfrak{p})(y+\mathfrak{p}) = 0 \text{ in } R/\mathfrak{p} \\
&\qquad \text{and } R + \mathfrak{p} \neq 0 + \mathfrak{p} \text{ in } R/\mathfrak{p}, \text{ then } (y+\mathfrak{p})^n = 0 \text{ for some } n \\
&\iff \text{for all } \overline{x}, \overline{y} \in R/\mathfrak{p}, \text{ if } \overline{y} \text{ is a zerodivisor, then } \overline{y} \text{ is nilpotent} \\
&\iff \text{the zerodivisors of } A/\mathfrak{p} \text{ are nilpotent.}
\end{aligned}$$

□

Proof of Lemma 6.34. Suppose $a, b \in A$ satisfy $ab \in \sqrt{\mathfrak{q}}$. Then there exist $n \in \mathbb{Z}_{\geqslant 1}$ such that $a^n b^n \in \mathfrak{q}$. Since $\mathfrak{q}$ is primary, $a^n \in \mathfrak{q}$ or $(b^n)^m \in q$ for some $m \in \mathbb{Z}_{\geqslant 1}$. But this tells us that either $a \in \sqrt{\mathfrak{q}}$ or $b \in \sqrt{\mathfrak{q}}$. Hence $\mathfrak{q}$ is prime. □

Proof of Lemma 6.45. To see (1), note everything in A multiplies x into $\mathfrak{q}$, so there is nothing to show in this case.

It remains to prove (2): If $yx \in \mathfrak{q}$ and $x \notin \mathfrak{q}$, then by definition of primary we have $y \in \sqrt{\mathfrak{q}} = \mathfrak{p}$. Thus $\mathfrak{q} \subset (\mathfrak{q} : x) \subset \mathfrak{p}$. Taking radicals, we obtain

$$\sqrt{\mathfrak{p}} \subset \sqrt{(\mathfrak{q} : x)} \subset \sqrt{\mathfrak{p}} = \mathfrak{p},$$

hence $\sqrt{(\mathfrak{q} : x)} = \mathfrak{p}$. To see that $(\mathfrak{q} : x)$ is primary, suppose $yz \in (\mathfrak{q} : x)$ for some $y, z \in A$ and $y \notin \sqrt{(\mathfrak{q} : x)} = \mathfrak{p}$. We want to show $z \in (\mathfrak{q} : x)$. Since $xyz \in \mathfrak{q}$ (by definition) and $y \notin \sqrt{\mathfrak{q}}$, we must have $xz \in \mathfrak{q}$ (just by definition of primary), that is, $z \in (\mathfrak{q} : x)$. This proves the lemma. □

Proof of Proposition 6.46. (i) Suppose $S \cap \mathfrak{p} = \varnothing$. Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal in A. We need to show that $S^{-1}\mathfrak{q}$ in $S^{-1}A$ is $S^{-1}\mathfrak{p}$-primary. Consider any element $\frac{a}{s}$ in $S^{-1}A$ such that $\frac{a}{s} \cdot \frac{b}{t} \in S^{-1}\mathfrak{q}$ for some $\frac{b}{t} \in S^{-1}A$. This implies $ab \in \mathfrak{q}$ and $s, t \notin \mathfrak{p}$. Since $\mathfrak{q}$ is $\mathfrak{p}$-primary and $ab \in \mathfrak{q}$, at least one of a or b is in $\mathfrak{p}$ or $b^n \in \mathfrak{q}$ for some n. This implies $\frac{a}{s} \in S^{-1}\mathfrak{p}$ or $\left(\frac{b}{t}\right)^n \in S^{-1}\mathfrak{q}$, thus $S^{-1}\mathfrak{q}$ is primary. Since radicals commute with localization (Check!), it follows that $S^{-1}\mathfrak{q}$ is $S^{-1}\mathfrak{p}$-primary (since $\sqrt{S^{-1}\mathfrak{q}} = S^{-1}(\sqrt{\mathfrak{q}}) = S^{-1}\mathfrak{p}$). Conversely, pulling any $S^{-1}\mathfrak{p}$-primary ideal of $S^{-1}A$ back to A results in a primary ideal (Check!), so this correspondence is bijective.

(ii) Assume $S \cap \mathfrak{p} = \varnothing$ and $\mathfrak{q}$ is $\mathfrak{p}$-primary. We need to show that $S^{-1}\mathfrak{q} = S^{-1}A$. For any element $q \in \mathfrak{q}$ and $s \in S$, consider $\frac{q}{s}$ in $S^{-1}A$. Since $\mathfrak{q}$ is $\mathfrak{p}$-primary, elements of $\mathfrak{q}$ are nilpotent modulo $\mathfrak{p}$. As S has no intersection with $\mathfrak{p}$, the elements of S are not zero-divisors modulo $\mathfrak{p}$. Therefore, $\frac{q}{s}$ becomes a unit in $S^{-1}A$, implying that $S^{-1}\mathfrak{q} = S^{-1}A$. □

Proof of Proposition 6.47. $S^{-1}I = \bigcap_{i=1}^n S^{-1}\mathfrak{q}_i \overset{(4.42)}{=} \bigcap_{i=1}^m S^{-1}\mathfrak{q}_i$ by Section 11, and $S^{-1}\mathfrak{q}_i$ is $S^{-1}\mathfrak{p}_i$-primary for each $i \in \{1, \ldots, m\}$. Since the $\mathfrak{p}_i$ are distinct, so are the $S^{-1}\mathfrak{p}_i$ for all $1 \leqslant i \leqslant m$, hence we have a minimal primary decomposition. Taking the preimage by j of both sides, we obtain

$$j^{-1}(I) = j^{-1}(S^{-1}I) = \bigcap_{i=1}^m j^{-1}(S^{-1}\mathfrak{q}_i) = \bigcap_{i=1}^m \mathfrak{q}_i,$$

again by Section 11. □

Proof of Lemma 6.48. Let A be a Noetherian ring and let $\mathfrak{q}$ be an irreducible ideal of A. By passing to $A/\mathfrak{q}$, we may assume $\mathfrak{q} = (0)$. We can do this because

$$(0) \text{ is irreducible in } A/\mathfrak{q} \overset{\substack{\text{correspondence}\\ \text{theorem}}}{\Longleftrightarrow} \mathfrak{q} \text{ is irreducible in } A$$

and

$$(0) \text{ is primary in } A/\mathfrak{q} \overset{\substack{\text{primary iff}\\ \text{zerodivisors}\\ \text{are nilpotent}}}{\Longleftrightarrow} \mathfrak{q} \text{ is primary in } A,$$

so it is enough to treat the case where (0) is an irreducible ideal of our (new) ring A.

So suppose $xy = 0$ and $y \neq 0$. We want to show $x^n \in (0)$ for some $n \in \mathbb{Z}_{\geqslant 1}$, that is, that x is nilpotent. Consider the increasing chain of ideals

$$\mathrm{Ann}_A(x) \subset \mathrm{Ann}_A(x^2) \subset \mathrm{Ann}_A(x^3) \subset \cdots .$$

(Here we recall that for all b in a ring B, we recall $\mathrm{Ann}_B(b) = \{c \in B \mid cb = 0\}$, and the definition for modules is similar.) Since A is Noetherian, there exists $n \in \mathbb{Z}_{\geqslant 1}$ such that

$$\mathrm{Ann}_A(x^n) = \mathrm{Ann}_A(x^{n+1}) = \cdots .$$

We claim $(x^n) \cap (y) = \varnothing$. Indeed, if $z \in (x^n) \cap (y)$, then $zx = 0$ (since $z \in (y)$ and $yx = 0$). But $z \in (x^n)$ too, so $z = x^n w$ for some $w \in A$. Multiplying by x, we obtain $0 = xz = x^{n+1}w$, so $w \in \mathrm{Ann}_A(x^{n+1}) = \mathrm{Ann}_A(x^n)$. Hence $z = x^n w = 0$, so $(x^n) \cap (y) = 0$. We have assumed (0) is irreducible, and we have $(0) = (x^n) \cap (y)$ with $(y) \neq 0$, so $(x^n) = (0)$, that is, $x^n = 0$. This completes the proof. □

Proof of Lemma 6.50. Consider a minimal prime $\mathfrak{p}$ containing $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$. Taking radicals,

$$\mathfrak{p} = \sqrt{\mathfrak{p}} \supset \sqrt{\bigcap_{j=1}^n \mathfrak{q}_k} = \bigcap_{j=1}^n \sqrt{\mathfrak{q}_j} = \bigcap_{j=1}^n \mathfrak{p},$$

where the middle equality is by Exercise 10.2(b) that $V(I_1 \cap I_2) = V(I_1) \cup V(I_2)$. Thus $\mathfrak{p}$ contains $\mathfrak{p}_j$ for some $j \in \{1, \ldots, n\}$. By minimality, $\mathfrak{p} = \mathfrak{p}_j$. □

Proof of Lemma 6.54. Let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ be some (not necessarily reduced) primary decomposition. Then let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \{\sqrt{\mathfrak{q}_1}, \ldots, \sqrt{\mathfrak{q}_n}\}$ such that where the $\mathfrak{p}_i$s are distinct. For each $j \in \{1, \ldots, r\}$, set

$$\tilde{q}_j = \bigcap_{\substack{i \text{ such that} \\ \sqrt{q_i} = p_j}} q_i.$$

We show in Exercise 11.2 that $\widetilde{\mathfrak{q}}_j$ itself is $\mathfrak{p}_j$-primary. Since $I = \bigcap_{j=1}^{r} \widetilde{\mathfrak{q}}_j$, condition (1) of Definition 6.53 holds; to see condition (2), note that if any $\widetilde{\mathfrak{q}}_j$ contains $\bigcap_{k \neq j} \widetilde{\mathfrak{q}}_k$, omit $\widetilde{\mathfrak{q}}_j$. □

Proof of Theorem 6.58. (1) Let $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ be a reduced primary decomposition and set $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. We will show that

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \{\text{primes of the form } \sqrt{(I : x)} \text{ for some } x \in A\} \tag{11.9.2}$$

for some $x \in A$. Recall from Exercise 7.3 that $(I : x)$ denotes the ideal quotient of x, which is the collection of elements that multiply x into I, that is,

$$(I : x) = \{y \in A \mid yx \in I\} = \operatorname{Ann}_A \underbrace{(x + I)}_{\in A/I}.$$

Observe that for any $x \in A$,

$$\sqrt{(I : x)} = \sqrt{\left(\bigcap_{i=1}^{n} \mathfrak{q}_i : x\right)} = \sqrt{\bigcap_{j=1}^{n} (\mathfrak{q}_i : x)} = \bigcap_{j=1}^{n} \sqrt{(\mathfrak{q}_i : x)}. \tag{11.9.3}$$

Now by Lemma 6.45 and Equation (11.9.3), we conclude

$$\sqrt{(I : x)} \overset{\text{above}}{=} \bigcap_{j=1}^{n} \sqrt{(\mathfrak{q}_j : x)} = \bigcap_{j \text{ such that } x \notin \mathfrak{q}_i} \mathfrak{p}_j$$

Now suppose x has the additional property that $\sqrt{(I : x)}$ is prime. Since

$$\sqrt{\underbrace{(I : x)}_{\text{prime}}} = \bigcap_{j=1}^{n} \sqrt{(\mathfrak{q}_j : x)} = \bigcap_{\substack{j \text{ such} \\ \text{that } x \notin \mathfrak{q}_i}} \mathfrak{p}_j, \tag{11.9.4}$$

we have $\sqrt{(I : x)} = \mathfrak{p}_i$ for some i such that $x \notin \mathfrak{q}_i$.

Conversely, since the primary decomposition is reduced, for all $i \in \{1, \ldots, n\}$, there exists $x_j \notin \mathfrak{q}_i$, but $x_i \in \bigcap_{j \neq i} \mathfrak{q}_j$. Then

$$\sqrt{(I : x_i)} = \mathfrak{p}_i,$$

so we obtain the other inclusion of Equation (11.9.2).

(2) A set Σ of prime ideals contained in an ideal I is said to be **isolated** if it satisfies the following condition: if $\mathfrak{p}'$ is a prime ideal contained in I and $\mathfrak{p}' \subset \mathfrak{p}$ for some $\mathfrak{p} \in \Sigma$, then $\mathfrak{p}' \in \Sigma$.

Let Σ be an isolated set of prime ideals contained in I, and let $S = A \setminus \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p}$. Then S is multiplicatively closed and, for any prime ideal $\mathfrak{p}'$ belonging to I we have

$$\mathfrak{p}' \in \Sigma \implies \mathfrak{p}' \cap S = \varnothing;$$

and

$$\mathfrak{p}' \notin \Sigma \implies \mathfrak{p}' \notin \bigcup_{\mathfrak{p} \in \Sigma} \mathfrak{p} \implies \mathfrak{p}' \cap S \neq \varnothing.$$

Hence, from Proposition 6.47 we can prove the statement of (2) as follows:

We have $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m} = j^{-1}(I)$, where $j \colon A \to S^{-1}A$ is the natural map and $S = A \setminus (\mathfrak{p}_{i_1} \cup \cdots \cup \mathfrak{p}_{i_m})$, hence depends only on ga (since the $\mathfrak{p}_i$ depend only on I). Thus the isolated primary components (that is, the primary components $\mathfrak{q}_t$ corresponding to minimal prime ideals $\mathfrak{p}_i$) are uniquely determined by I, and thus independent of the primary decomposition of I. □

Proof of Corollary 6.62. Note $ZD = \bigcup_{x \neq 0} \{y \in A \mid yx = 0\} = \bigcup_{x\neq 0}((0) : x)$, and (noting that for any *subset* S of A, by $\sqrt{S}$ we mean the collection of elements have some power in S) $\sqrt{ZD} = ZD$. Hence

$$ZD = \sqrt{ZD} = \sqrt{\bigcup_{x\neq 0}((0) : x)} = \bigcup_{x \neq 0} \sqrt{((0) : x)}.$$

But by the proof of the theorem (in particular, by Equation (11.9.4)), we saw that $\sqrt{((0) : x)} = \bigcap_{\substack{j \text{ such} \\ \text{that } x \notin \mathfrak{q}_i}} \mathfrak{p}_j$. Then for any $x \neq 0$, there exists i such that $x_i \notin \mathfrak{q}_i$, so $\sqrt{((0) : x)}$ is an intersection in which $\mathfrak{p}_i$ appears, hence $\sqrt{((0) : x)} \subset \mathfrak{p}_i$. Thus

$$ZD = \bigcup_{x \neq 0} \sqrt{((0) : x)} \subset \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

To see the other inclusion, note that by part (1) of the theorem, each $\mathfrak{p}_i$ could be written as $\sqrt{((0) : x_i)}$ for some x_i, so $\mathfrak{p}_i \subset \bigcup_{x\neq 0} \sqrt{((0) : x)}$. This completes the proof. □

Proof of Corollary 6.63. We have $(0) = \sqrt{(0)} = \bigcap_{\substack{\text{minimal} \\ \mathfrak{p} \in \operatorname{Spec} A}} \mathfrak{p}$ is a primary decomposition. □

Solution to Exercise 6.64. We first prove a useful lemma.

Lemma 11.10.

Let I be an ideal of a commutative ring A. Then

$$\sqrt{I} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p},$$

where we recall $V(I) = \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} \text{ contains } I\}$.

Proof. Let $\pi \colon A \twoheadrightarrow A/I$ be the natural quotient map. By Lemma 11.2the nilradical of A/I is $\pi(\sqrt{I})$, so

$$\pi(\sqrt{I}) \overset{(8.2)}{=} \bigcap_{\mathfrak{p} \in \operatorname{Spec}(A/I)} \mathfrak{p} = \bigcap_{\substack{\mathfrak{p} \in \operatorname{Spec} A \\ \mathfrak{p} \supset I}} \pi(\mathfrak{p}) = \bigcap_{\mathfrak{p} \in V(I)} \pi(\mathfrak{p}),$$

where the middle equality is by the correspondence theorem. Applying π^{-1} to both sides, we obtain

$$\sqrt{I} = \pi^{-1}(\pi(\sqrt{I})) = \pi^{-1}\left(\bigcap_{\mathfrak{p} \in V(I)} \pi(\mathfrak{p})\right) = \bigcap_{\mathfrak{p} \in V(I)} \pi^{-1}(\pi(\mathfrak{p})) = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p},$$

where the first and last equalities are because π is surjective, and the penultimate equality is because preimages preserve intersections. □

We now return to the statement of Exercise 11.1. Let $A = \mathbb{Z}[x]$, let $\mathfrak{m} = (2, x)$, and let $\mathfrak{q} = (4, x)$. Since $\mathbb{Z}[x]/(2, x) \cong (\mathbb{Z}[x]/(x))/(2) \cong \mathbb{Z}/2\mathbb{Z}$ is a field, $\mathfrak{m}$ is maximal in $\mathbb{Z}[x]$. To see $\mathfrak{q}$ is $\mathfrak{m}$-primary, we can use Exercise 10.1 to write

$$\sqrt{\mathfrak{q}} = \sqrt{(4, x)} = \sqrt{(4) + (x)} \overset{(10.1)}{=} \sqrt{\sqrt{(4)} + \sqrt{(x)}} = \sqrt{(2) + (x)} = \sqrt{(2, x)} = \sqrt{\mathfrak{m}} = \mathfrak{m}.$$

To see $\mathfrak{q}$ is not a power of $\mathfrak{m}$, note that for all $n \in \mathbb{Z}_{\geqslant 3}$,

$$\mathfrak{m}^n \subset \mathfrak{m}^2 = (4, 4x, x^2) \underbrace{\subsetneq}_{\text{e.g. x}} \mathfrak{q} = (4, x) \underbrace{\subsetneq}_{\text{e.g. 2}} \mathfrak{m} = (2, t),$$

so $\mathfrak{q} \neq \mathfrak{m}^n$ for all $n \in \mathbb{Z}_{\geqslant 1}$. □

Solution to Exercise 6.65. We first need the following lemma.

Lemma 11.11: Radical Commutes with Finite Intersections.

If $\{I_j\}_{j=1}^n$ is any finite collection of ideals of a commutative ring A, then

$$\sqrt{\bigcap\nolimits_{j=1}^n I_j} = \bigcap\nolimits_{j=1}^n \sqrt{I_j}.$$

Proof of Lemma 11.11. Suppose $a \in \bigcap_{j=1}^n \sqrt{I_j}$. Then $a \in I_k$ for all $k \in \{1, \dots, n\}$, so there exist $m_1, \dots, m_j \in \mathbb{Z}_{\geqslant 1}$ such that for all j, $a^{n_j} \in I_j$. Hence $b^m \in \bigcap_{j=1}^n I_j$ for all $m \geqslant \max\{m_1, \dots, m_n\}$, so $\bigcap_{j=1}^n I_j \subset \bigcap_{j=1}^n \sqrt{I_j}$. (Note this inclusion requires the intersection be finite.)

Conversely, suppose $a \in \sqrt{\bigcap_{j=1}^n I_j}$. Then $a^m \in \bigcap_{j=1}^n$ for some $n \in \mathbb{Z}_{\geqslant 1}$, so $a^n \in I_j$ for each $j \in \{1, \dots, n\}$. Hence $a \in \bigcap_{j=1}^n \sqrt{I_j}$, so we conclude $\bigcap_{j=1}^n \sqrt{I_j} \subset \sqrt{\bigcap_{j=1}^n I_j}$. (Note this inclusion holds for arbitrary intersections.) This completes the proof. □

We can now prove the statement of Exercise 11.2. Suppose we have $a, b \in A$ such that $ab \in \bigcap_{j=1}^n \mathfrak{q}$ and $a \notin \bigcap_{j=1}^n \mathfrak{q}_j$. Then $a \notin \mathfrak{q}_k$ for some $k \in \{1, \dots, n\}$ and $ab \in \mathfrak{q}_j$ for all $j \in \{1, \dots, n\}$; in particular $ab \in \mathfrak{q}_k$, so since $a \notin \mathfrak{q}_k$ and $\mathfrak{q}_j$ is $\mathfrak{p}$-primary, we must have $b \in \mathfrak{p}$. Since we can write

$$\mathfrak{p} = \bigcap\nolimits_{j=1}^n \mathfrak{p} = \bigcap\nolimits_{j=1}^n \sqrt{\mathfrak{q}_j} \overset{(11.11)}{=} \sqrt{\bigcap\nolimits_{j=1}^n \mathfrak{q}_j},$$

we conclude $b \in \sqrt{\bigcap_{j=1}^n \mathfrak{q}_j}$. Hence $\bigcap_{j=1}^n \mathfrak{q}_i$ is $\mathfrak{p}$-primary. □

Solution to Exercise 6.66. (a) $\mathfrak{p}$ is prime, hence primary. Now let $n \in \mathbb{Z}_{\geqslant 2}$. To see $\mathfrak{q}_n$ is primary, we opt to work in the quotient ring $A/\mathfrak{q}_n$; this is a finitely generated k-algebra with generating set $\{1, x, y, y^2, \dots, y_{n-1}\}$ and relations

$$x^2 = xy = y^n = 0. \tag{11.11.1}$$

Now suppose $f \in A/\mathfrak{q}_n$ is *not* nilpotent. We claim f is not a zerodivisor. First write $f = a_0 + a_1'x + a_1y + a_2y^2 + \cdots + a_{n-1}y^{n-1}$, where $a_0, a_1', a_1, a_2, \dots, a_n \in k$. Since f is not nilpotent, the constant term a_0 of f must be nonzero. To see this, suppose instead $a_0 = 0$. Then the degree of any nonzero term[1] of f is positive, hence the degree of any term of f^n is at least n, but $A/\mathfrak{q}_n$ has no nonzero monomials of degree n by the relations in Equation (11.11.1). Thus $a_0 \neq 0$. Now suppose $fg = 0$ for some $g = b_0 + b_1'x + b_1y + b_2y^2 + \cdots + b_{n-1}y^{n-1} \in A/\mathfrak{q}_n$. Then

$$\begin{aligned} 0 = fg &= (a_0 + a_1'x + a_1y + \cdots + a_{n-1}y^{n-1})(b_0 + b_1'x + b_1y + \cdots + b_{n-1}y^{n-1}) \\ &= a_0b_0 + (a_0b_1' + a_1'b_0)x + (a_0b_1 + a_1b_0)y + (a_0b_2 + a_1b_1 + a_2b_0)y^2 + \cdots. \end{aligned}$$

Since $a_0 \neq 0$, the condition $a_0b_0 = 0$ forces $b_0 = 0$, which by looking at the x- (resp. y-) coefficient implies $b_1' = 0$ (resp. $b_1 = 0$). In the general case, if for some $k \geqslant 2$ we have $b_0 = b_1 = \ldots = b_{k-1} = 0$, then consider the coefficient of y^k in fg, which is the sum

[1] Note that the degree of nonzero monomials m of $A/\mathfrak{q}_n$ is well-defined, since any of its preimages in A differ by a *sum* of elements of $\mathfrak{q}_n$, so we can define the degree of m in $A/\mathfrak{q}_n$ as the degree in A of the unique element of its preimage in A that is also a monomial.

of products $a_i b_j$ such that $i + j = k$. By the inductive hypothesis, all terms $a_i b_j$ with $i + j = k$ and $i > 0$ must have $b_j = 0$ (since $j < k$), so the coefficient of y^k in fg is $a_0 b_k$. But $fg = 0$, so $a_0 b_k = 0$, implying $b_k = 0$ (since k is an integral domain as a field). Then $g = 0$, so f is not a zerodivisor. We have now shown that non-nilpotent elements are non-zerodivisors, or equivalently that $\mathfrak{q}_n$ is primary in A.

Lastly, note that $\mathfrak{p} \cap \mathfrak{q}_n$ is a primary decomposition of I for all $n \in \mathbb{Z}_{\geqslant 2}$, since

$$\begin{aligned}\mathfrak{p} \cap \mathfrak{q}_n &= (Ax) \cap (Ax^2 + Axy + Ay^n) \\ &= (Ax \cap Ax^2) + (Ax \cap Axy) + (Ax \cap Ay^n) \\ &= (Ax^2) + (Axy) + (0) = (x^2, xy) = I.\end{aligned}$$

(b) We have

$$\begin{aligned}\sqrt{\mathfrak{q}_n} = \sqrt{(x^2, xy, y^n)} = \sqrt{(x^2) + (xy) + (y^n)} &\overset{(10.1)}{=} \sqrt{\sqrt{(x^2)} + \sqrt{(xy)} + \sqrt{(y^n)}} \\ &= \sqrt{(x) + (xy) + (y)} = \sqrt{(x, xy, y)} = \sqrt{(x, y)} = (x, y).\end{aligned}$$

which is independent of n. Hence $\sqrt{\mathfrak{q}_n}$ yields the same associated prime of I regardless of $n \in \mathbb{Z}_{\geqslant 1}$, so that $\operatorname{Ass}(I) = \{\mathfrak{p}, \mathfrak{q}_2\} = \{(x), (x, y)\}$. □

Solution to Exercise 6.67. Suppose for sets I, J there exist A-module isomorphisms $\varphi_I \colon M \xrightarrow{\cong} \bigoplus_I A$ and $\varphi_J \colon M \xrightarrow{\cong} \bigoplus_J A$, and let $\mathfrak{m}$ be a maximal ideal of A, so that $k \coloneqq A/\mathfrak{m}$ is a field.

Lemma 11.12.

If M is an A-module and I is an ideal of A, then A/I is an (M/IM)-module in the natural way. Furthermore, any A-module isomorphism $\varphi \colon M \xrightarrow{\cong} N$ induces an (A/I)-module isomorphism $\widetilde{\varphi} \colon M/IM \xrightarrow{\cong} N/IN$. [a]

[a] Note that once we have tensor products at our disposal, this will follow quickly.

Proof. Define a map $A/I \times M/IM \to M/IM$ by $(a + I) \cdot (m + IM) \coloneqq (am) + IM$. This map is well-defined, since if $m - m' \in IM$ and $a - a' \in A$, then

$$\begin{aligned}(a' + I)(m' + IM) = a'm' + IM &= a'm' + \overbrace{\underbrace{(a - a')}_{\in I}\underbrace{m'}_{\in M}}^{\in IM} + \overbrace{\underbrace{a}_{\in A}\underbrace{(m - m')}_{\in IM}}^{\in IM} + IM \\ &= \cancel{a'm'} + \cancel{am'} - \cancel{a'm'} + am - \cancel{am'} + IM = am + IM = (a + I)(m + IM).\end{aligned}$$

Next note that M/IM is an abelian group under addition since as groups it is precisely the abelian group M/IM (as an A-module) under addition. Lastly note that the proposed map satisfies the (A/I)-module axioms for arbitrary $m + IM, m' + IM \in IM, a + I, a' + I \in I$, since

- $(0 + IM)(m + IM) = (0m + IM) = 0 + IM$,
- $(a + I)((a' + I)(m + I)) = (a + I)(a'm + IM) = (aa'm + IM) = (aa')m + IM = ((a + I)(a' + I))(m + IM)$,

- $(a+I)((m+IM)+(m'+IM)) = (a+I)((m+m')+IM) = (am+am')+IM = (am+IM)+(am'+IM)$, and
- $((a+I)+(a'+I))(m+IM) = ((a+a')+I)(m+IM) = (a+a')m+IM = (am+a'm)+IM = (am+IM)+(a'm+IM)$.

Thus M/MI is an (A/I)-module. The second statement follows from considering the commutative diagram

$$\begin{tikzcd}
0 \arrow[r] \arrow[d, "\cong"'] & IM \arrow[r] \arrow[d, "\varphi|_{IM}"'] & M \arrow[r] \arrow[d, "\varphi"] & M/IM \arrow[r] \arrow[d, "\overline{\varphi}"] & 0 \arrow[d, "\cong"] \\
0 \arrow[r] & IN \arrow[r] & N \arrow[r] & N/IN \arrow[r] & 0
\end{tikzcd}$$

and the fact that $\varphi(IM) = I\cdot\varphi(M) = IN$. □

Now by the lemma, φ_I and φ_J induce k-vector space isomorphisms $\widetilde{\varphi}_I\colon M/\mathfrak{m}M \xrightarrow{\cong} (\bigoplus_I A)/\mathfrak{m}(\bigoplus_I A)$ and $\widetilde{\varphi}_J\colon M/\mathfrak{m}M \xrightarrow{\cong} (\bigoplus_J A)/\mathfrak{m}(\bigoplus_I A)$.

Before continuing, we need to show $(\bigoplus_I A)/\mathfrak{m}(\bigoplus_I A) \cong \bigoplus_I k$. Define $\varphi\colon (\bigoplus_I A)/\mathfrak{m}(\bigoplus_I A) \to \bigoplus_I k$ by $\varphi(\{a_i + \mathfrak{m}(\bigoplus_I A)\}) := \{a_i+\mathfrak{m}\}_{i\in I}$. If two elements of $(\bigoplus_I A)/\mathfrak{m}(\bigoplus_I A)$ are equal, then their components differ by elements of $\mathfrak{m}$ in A, which means by definition of φ that their images under φ coincide. And φ is k-linear, as this follows directly from the component-wise operations in $(\bigoplus_I A)/\mathfrak{m}(\bigoplus_I A)$ and $\bigoplus_I k$. To see φ is injective, suppose $\varphi((a_i+\mathfrak{m}(\bigoplus_I A))) = 0$; then each a_i must be in $\mathfrak{m}$, so $\{a_i+\mathfrak{m}(\bigoplus_I A)\}_{i\in I}$ the zero element in $(\bigoplus_I A)/\mathfrak{m}(\bigoplus_I A)$. For surjectivity, observe that any $(a_i+\mathfrak{m})_{i\in I} \in \bigoplus_I k$ is the image under φ of $\{a_i+\mathfrak{m}(\bigoplus_I A)\}_{i\in I}$. Thus φ is an k-vector space isomorphism.

Thus we can identify φ_I, φ_J with isomorphisms $M/\mathfrak{m}M \xrightarrow{\cong} \bigoplus_I k$ and $M/\mathfrak{m} \xrightarrow{\cong} \bigoplus_J k$, respectively. And k is a field, so we obtain an isomorphism of k-vector spaces

$$\Phi := \widetilde{\varphi}_J \circ \widetilde{\varphi}_I\colon \bigoplus_I k \xrightarrow{\cong} \bigoplus_J k.$$

Let $\overline{1}$ denote the identity of k, and let δ_{ij} denote $\overline{1}$ if $i=j$ and 0 otherwise. It is immediate from the componentwise operations that the collections $\{\{\delta_{\alpha\beta}\}_{\alpha\in I} \mid \beta\in I\}$ and $\{\{\delta_{\alpha\beta}\}_{\alpha\in J} \mid \beta\in J\}$, are bases for $\bigoplus_I k$ and $\bigoplus_J k$, respectively. Since the cardinality of any basis is invariant under isomorphism we conclude I and J have the same cardinality. □

Solution to Exercise 6.68. (a) Since π is surjective, there exists $m_i \in M$ such that $\pi(m_i) = \{\delta_{ij}\}_{j\in I}$. Repeating this for each $i\in I$, we obtain a collection $\{m_i\}_{i\in I} \subset M$. Then for each $i \in A$, define $s(\{\delta_{ij}\}) := m_i$, and extend linearly, that is, for any $a = \sum_{k=1}^n a_{i_k} \in P$, define $s(\sum_{k=1}^n a_{i_k}) = \sum_{k=1}^n s(a_{i_k}) = \sum_{k=1}^n m_{i_k}$. Since this is the canonical homomorphism by the universal mapping property of the direct sum of modules, so we already know s is a well-defined homomorphism $P \to M$.

The injectivity of s follows from the fact that $\pi\circ s$ is the identity on P: if $s(p) = s(p')$ for some $p, p' \in P$, then by applying π we obtain $p = \pi(s(p)) = \pi(s(p')) = p'$.

To see $M = \ker(\pi)\oplus s(P)$, note that any $m\in M$ can be uniquely written as $m = k+s(p)$ for some $k\in\ker(\pi)$, where $p = \pi(m)$. Indeed, if $m = k+s(p) = k'+s(p')$, then by applying π and noting $\pi \circ s = \mathrm{id}_P$, we obtain $p = \pi(k) + \pi(s(p)) = \pi(k') + \pi(s(p')) = \pi(m') = p'$ π gives $p = p'$, hence $k = k'$. Thus $M = \ker \pi \oplus s(P)$.

(b) Let A be a PID, let $M \cong A^{\oplus d}$, and let N be a submodule of M. We claim $N \cong A^{\oplus d'}$ for some $d' \leqslant d$. If $N = \{0\}$ then $N \cong \bigoplus_{\varnothing} A \cong \{0\}$ (by convention), so assume $N \neq \{0\}$.

If $d = 1$ then $M = A$, so $N \cong I$ for some ideal I of A. As A is a PID, $I = Aa$ for some $a \in A$. Then the A-linear map $N = Aa \to A$ determined by $a \mapsto 1$ (more precisely, the map $a' \mapsto a'a$) is an isomorphism of A-modules: there is no issue with A-linearity; it is injective since $a'a \in Aa$ maps to 0 if and only if $a = 0$ (since A is a PID and hence has no zerodivisors); and it is surjective because any $a' \in A$ is the image of $a'a \in Aa$. Thus $N = Aa \cong A$, so N is a free A-module. This affirms the claim in the base case.

Now suppose $d \geqslant 2$ and the claim holds for all integers up to $d-1$. Let $\pi\colon A^{\oplus d} \to A^{\oplus(d-1)}$ be the projection $(a_1, \ldots, a_{d-1}, a_d) \mapsto (a_1, \ldots, a_{d-1})$. Then $\pi(N)$ is a submodule of $A^{\oplus(d-1)}$, so by the induction hypothesis $\pi(N) \cong A^{\oplus(d'-1)}$ for some $d' \leqslant d$. Then since the restriction $\pi|_N\colon N \to A^{\oplus(d-1)}$ is surjective as a map $N \to \pi(N)$, by part (a) there exists an (injective) section $s\colon A^{\oplus(d'-1)} \to N$ such that

$$N = \ker(\pi|_N) \oplus s(A^{\oplus(d'-1)}). \tag{11.12.1}$$

By definition of s from part (a),

$$\begin{aligned} s(A^{\oplus(d'-1)}) &= \{(s(a_1), \ldots, s(a_{d'-1})) \mid a_1, \ldots, a_{d'-1} \in A\} \\ &= \{(a_1, \ldots, a_{d'-1}, 0) \mid a_1, \ldots, a_{d'-1} \in A\} = A^{\oplus(d'-1)} \times \{0\} \cong A^{\oplus(d'-1)}, \end{aligned}$$

so if $\ker(\pi|_N) = \{0\}$ or $\ker(\pi|_N) \cong A$ then we are done by Equation (11.12.1). We thus assume $\ker(\pi|_N) \neq \{0\}$ and prove $\ker(\pi|_N) \cong A$. But this follows quickly, since by definition of π above we have $\pi(a_1, \ldots, a_d) = (0, \ldots, 0)$ if and only if $a_1 = \cdots = a_{d-1} = 0$, so

$$\ker(\pi|_N) = \{(a_1, \ldots, a_d) \in N \mid a_1 = \cdots = a_{n-1} = 0\} \cong (\{0\}^{\oplus(d'-1)} \oplus L),$$

where L is the set of elements $\ell \in A$ such that $(0, \ldots, 0, \ell) \in \ker(\pi|_N)$. And L is nonzero (since otherwise $\ker(\pi|_N) = 0$ and we are done), we know $L = (a) = Aa$ for some $a \in A$ since A is a PID. But then just as in the base case $L \cong A$ as modules, hence $\ker(\pi|_N) \cong \{0\}^{\oplus(d'-1)} \times A \cong A$, as desired. □

Proof of Lemma 7.3. If x is reducible, then $x = yz$. But if $x \mid yz$, $x \mid y$ or $x \mid z$, so without loss of generality $x\alpha = y$. Then $x\alpha z = yz = x$, so $\alpha z = 1$, which completes the proof. □

Proof of Theorem 7.9. ($\Longrightarrow$) Let R be a UFD and let $x \in R$ be nonzero. Suppose $yz \in (x)$. Without loss of generality $y, z \notin R^\times$. We can write $xw = yz$ for some $w \in R$. We can then write $xw_1 \cdots w_n = y_1 \cdots y_a z_1 \cdots z_b$ for irreducible elements y_i and z_j.

Since R is a UFD, there exists i and $w \in R^\times$ such that $x = wy_i$ or $x = wz_i$, so $y_i \in (x)$ or $z_i \in (x)$, hence $y \in (x)$ or $z \in (x)$, as desired.

($\Longleftarrow$) Supposes some $x \in R$ is nonzero but factors into irreducibles (up to units u, u') in two ways:

$$x = ux_1 \cdots x_n = u'x'_1 \cdots x'_n$$

We will argue by induction on n. The case $n = 0$ holds since then x is a unit, hence factors uniquely up to units.

Now suppose $n \in \mathbb{Z}_{\geqslant 1}$, $x_n \mid x$. Since x_n is irreducible by hypothesis, it is prime. Thus

$$x_n \mid x_1' \cdots x_m',$$

so $x_m' = \alpha x_n$ for some α. Since x_n' is irreducible, $\alpha \in R^\times$. Now

$$x = (ux_1 \cdots x_{n-1})x_n = (v\alpha x_1' \cdots x_{m-1}')x_\alpha.$$

Since R is an integral domain,

$$u = x_1 \cdots x_{n-1} = v\alpha x_1' \cdots x_{n-1}',$$

which completes the proof. □

Proof of Proposition 7.13. We will extract the contents of f, g, and fg as follows. Write $f = c(f) \cdot f_1$, $g = c(g) \cdot g_1$, where f_1, g_1 are primitive. Then $c(fg) = c(c(f)f_1c(g)g_1) = c(f)c(g)c(f_1)c(g_1)$, where in the last step we were able to pull out the scalar because for all $a \in k \smallsetminus \{0\}$, $h \in k[x] \smallsetminus \{0\}$, $c(ah) = c(a) \cdot c(h)$. To prove the proposition, it is enough to check $c(f_1g_1) = 1$.

We want to show for all p, $\operatorname{ord}_p(f_1g_1) = 0$, or equivalently that f_1g_1 has nonzero image in $(A/(p))[x]$. But f_1 and g_1 have nonzero image in $(A/(p))[x]$ because their contents are 1, so since $A/(p)$ is an integral domain (since (p) is prime) f_1g_1 has nonzero image in $(A/(p))[x]$. □

Proof of Corollary 7.14. Let $f \in A[x]$ and $g, h \in k[x]^\times = k[x] \smallsetminus k$ such that $f = gh$. Taking the content of both sides, we obtain $c(f) = c(gh)$, which by Proposition 7.13 is $c(g)c(h)$. Since

$$f = gh = \underbrace{c(g)c(h)}_{\in A}\overbrace{g_1}^{\in A[x]}\underbrace{h_1}_{\in A[x]},$$

with g_1, h_1 primitive in $A[x]$, we now have a factorization of f in $A[x]$, which shows f is reducible in $A[x]$ as well. □

Proof of Theorem 7.16. ($\implies$) For any $f \in A$, we know the existence of factorizations of f (since f is a UFD), so we may assume $f \notin A$.

- *Existence of a factorization of f*: $k[x]$ is a UFD, so there exists a factorization $f = p_1 \cdots p_r$ such that each $p_i(x) \in k[x]$ is an irreducible element in $k[x]$. Taking contents, by Proposition 7.13, we have $c(f) = c(p_1) \cdots c(p_r)$, and $f = c(p_1) \cdots c(p_r)p_1' \cdots p_r'$, where $p_i = c(p_i)p_i'$ for all i, so $p_{i'}$ is a primitive element in $A[x]$, which is therefore irreducible in $A[x]$ (by the contrapositive of Note 7.15). Since $\prod_i c(p_i) = c(f) \in A$, we get $f = c(f) \cdot p_1' \cdots p_r'$, and factoring $c(f)$ in A we get a factorization of f in $A[x]$, as desired.
- *Uniqueness of factorizations of f*: Suppose $f = p_1 \cdots p_r = q_1 \cdots q_s$, where p_i, q_j are

irreducible in $A[x]$, where $d \coloneqq c(A)$ factors (in A)[2] and we may assume the g_j are primitive polynomials in $A[x]$ that are irreducible in $k[x]$. Since $k[x]$ is a UFD, we have $r = s$, so there exists $\sigma \in S_r$ and $a_1, \ldots, a_r \in k^\times$ such that $p_i' = a_i q_{\sigma(i)}$ for all $i \in \{1, \ldots, r\}$. Since $c(p_i') = 1$ and $c(q_{\sigma(i)}) = 1$, we see $c(a_i) = 1$ for all i, that is, $a_i \in A^\times$ for all i. Thus this factorization is just the other factorization, up to a unit.

□

Proof of Theorem 7.18. We prove the contrapositive. If f were reducible in $(\mathrm{Frac}(A)[x])$, say $f = gh$ for some irreducible $g, h \in (\mathrm{Frac}\, A)[x]$. Then $f \pmod I = (g \pmod I)(h \pmod I))$, so because $f \pmod I$ is irreducible (by hypothesis) we know either $g \pmod I$ or $h \pmod I$ is a unit in $(A/I)[x]$. But the units of any polynomial ring are precisely the units of the ground ring, so either $g \pmod I \in (A/I)^\times$ or $h \pmod I \in (A/I)^\times$. Without loss of generality we may assume $g \pmod I \in (A/I)^\times$, so in particular the degree of $g \pmod I$ is zero. Since the leading coefficient of f is not in I, the degree of f in $A[x]$ is the same as the degree of $f \pmod I$ in $(A/I)[x]$, so this condition forces the degree of $h \pmod I$ in $(A/I)[x]$ to equal the degree of f in $A[x]$, which in turn equals the degree of f in $\mathrm{Frac}(A)$. But this forces g to have degree 0 in $\mathrm{Frac}(A)$ as well. But this means g is a unit (as a nonzero constant in the field $\mathrm{Frac}(A)$), and hence g is a unit in $\mathrm{Frac}(A/I)$, which contradicts our assumption g is irreducible in $(\mathrm{Frac}(A))[x]$. □

Proof of Theorem 7.22. Relabel $R \coloneqq A$. Suppose $f = gh$, where $g = b_0 + b_1 x + \cdots + b_k x^k$, $h = b_0' + b_1' x + \cdots + b_k' x^{k'}$, where $k + k' = n$. We have $a_n = b_k b_{k'}' \notin \mathfrak{p}$, so $b_k, b_{k'}' \notin \mathfrak{p}$.

Now consider everything modulo $\mathfrak{p}$. Then

$$\overline{a}_n x^n = \left(\overline{b}_0 + \overline{b}_1 x + \cdots + \overline{b}_k x^k\right)\left(\overline{b}_0' + \overline{b}_1' x + \cdots + \overline{b}_k' x^{k'}\right),$$

so $\overline{b}_0 \overline{b}_0' = 0$. But $\mathfrak{p}$ is prime, so $\overline{b}_0 = 0$ or $\overline{b}_0' = 0$. By induction, we deduce (since $A/\mathfrak{p}$ is an integral domain D, and if you're working over an integral domain, then the only factors of x^n in $D[x]$ are monomials) that $\overline{b}_0, \ldots, \overline{b}_{k-1} = 0$, $\overline{b}_0', \ldots, \overline{b}_{k'-1}$ in $R/\mathfrak{p}$. Since $R/\mathfrak{p}$ is an integral domain, then $a_0 = b_0 b_0' \in \mathfrak{p}^2$. This completes the proof of the contrapositive of the theorem, hence the theorem follows. □

Proof of Theorem 7.24. We have

$$\begin{aligned} 0 = f(a/b) &= a_n \left(\frac{a}{b}\right)^n + a_{n-1}\left(\frac{a}{b}\right)^{n-1} + \cdots + a_0 \\ &= a_n a^n + a_{n-1} b a^{n-1} + \cdots + b^n a_0, && \text{(multiplying through by } b^n) \end{aligned}$$

so $b^n a_0 = -(a_n a^n)(a_n a^n + \cdots + a b^{n-1} a_0)$. Thus $a \mid b^{n a_0}$, so since $(a, b) = 1$ we conclude $a \mid a_0$. □

[2] We will omit the factorization of d in the notation, since it adds nothing to the argument, but for clarity we have

$$d \cdot \prod_{i=1}^r q_i = f = c(f) p_1' \cdots p_r' = c(f) \underbrace{\left(\prod_{i=1}^r a_i\right)}_{\in A^\times} \left(\prod_{i=1}^r q_{\sigma(i)}\right),$$

so $f = d \prod_{i=1}^r q_i$ where $d = c(f) \cdot (\text{unit in } A)$.

Proof of Theorem 7.26. See Exercise 12.3. □

Solution to Exercise 7.29. (a) Fix $i \in \{1, \ldots, n\}$ and let $x_i \in \bigcap_{j\neq i} \mathfrak{q}_j$ be nonzero. To see $\operatorname{Ann}_A(x_i) \subset \mathfrak{p}_i$, first let $y \in \operatorname{Ann}_A(x_i)$ be given. Then

$$yx_i = 0 = \mathfrak{q}_1 \cap \cdots \mathfrak{q}_n \subset \mathfrak{q}_i,$$

so $yx_i \in \mathfrak{q}_i$. Note that $x_i \notin \mathfrak{q}_i$, since otherwise $x_i \in \mathfrak{q}_i \cap \bigcap_{j\neq i} \mathfrak{q}_j = \mathfrak{q}_1 \cap \cdots \mathfrak{q}_n = (0)$, contradicting $x_i \neq 0$. But $\mathfrak{q}_i$ is primary, so we obtain the desired result $y \in \sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$.

(b) A is Noetherian, so by Exercise 10.2(a) any ideal of A contains some power of its radical. Then in particular there exists $m \in \mathbb{Z}_{\geqslant 1}$ such that $\mathfrak{p}_i^m = (\sqrt{\mathfrak{q}_i})^m \subset \mathfrak{q}_i$. Then by taking the intersection with $\bigcap_{i\neq j} \mathfrak{q}_j$ and recalling $I \cdot J \subset I \cap J$ for any ideals I, J of a ring, we obtain

$$\left(\bigcap\nolimits_{i\neq j} \mathfrak{q}_i\right) \cdot \mathfrak{p}_i^m \subset \left(\bigcap\nolimits_{i\neq j} \mathfrak{q}_i\right) \cap \mathfrak{p}_i^m \subset \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n = (0).$$

Thus

$$\left(\bigcap\nolimits_{i\neq j} \mathfrak{q}_i\right) \cdot \mathfrak{p}_i^m = (0). \tag{11.12.2}$$

Now replace m with the least integer satisfying Equation (11.12.2), which we again denote by m. Then $(\bigcap_{j\neq i} \mathfrak{q}_j) \cdot \mathfrak{p}_i^{m-1}$ is nonzero, so it contains some nonzero x_i. Then for all $y \in \mathfrak{p}_i$,

$$x_i y \in \left(\bigcap\nolimits_{j\neq i} \mathfrak{q}_i\right) \cdot \mathfrak{p}_i^{m-1} \cdot \mathfrak{p}_i \subset \left(\bigcap\nolimits_{j\neq i} \cdot \mathfrak{q}_j\right)\mathfrak{p}_i^m = (0),$$

so $x_i y = 0$. Thus $y \in \operatorname{Ann}_A(x_i) = \mathfrak{p}_i$, so we conclude $\mathfrak{p} \subset \operatorname{Ann}_A(x_i)$.

(c)
- $\operatorname{Ass}((0)) \subset \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} = \operatorname{Ann}_A(x) \text{ for some } x \in A\}$: Fix $i \in \{1, \ldots, n\}$. Since the primary decomposition $(0) = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$ is reduced, the intersection $\bigcap_{j\neq i} \mathfrak{q}_j$ is nonzero. Where m is (as in part (b)) the least integer satisfying $(\bigcap_{j\neq i} \mathfrak{q}_j) \cdot \mathfrak{p}_i \neq 0$, we can choose some nonzero $x_i \in (\bigcap_{j\neq i} \mathfrak{q}_j) \cdot \mathfrak{p}_i$. Then by part (b), $\mathfrak{p}_i \subset \operatorname{Ann}_A(x_i)$. To see the reverse inclusion, note that x_i is also a nonzero element of $\bigcap_{j\neq i} \mathfrak{q}_j$ since

  $$x \in \left(\bigcap\nolimits_{j\neq i} \mathfrak{q}_j\right) \cdot \mathfrak{p}_i^{m-1} \subset \bigcap\nolimits_{j\neq i} \mathfrak{q}_j,$$

  so $\operatorname{Ann}_A(x_i) \subset \mathfrak{p}_i$ by part (a). Thus $\operatorname{Ann}_A(x_i) = \mathfrak{p}_i$, so any element of $\operatorname{Ass}((0)) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ is the the annihilator of some element of A, that is, each $\mathfrak{p}_j$ is associated with A.

- $\{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{p} = \operatorname{Ann}_A(x) \text{ for some } x \in A\} \subset \operatorname{Ass}((0))$: Suppose $\operatorname{Ann}_A(x)$ is prime for some $x \in A$. Thus

  $$\operatorname{Ann}_A(x) = \sqrt{\operatorname{Ann}_A(x)} = \sqrt{\{y \in A \mid yx = 0\}} = \sqrt{((0) : (x))},$$

  where the first equality is because $\operatorname{Ann}_A(x)$ is radical (as a prime) and the last equality is by definition of $((0) : (x))$. Thus $\operatorname{Ann}_A(x) \in \left\{\mathfrak{p} \in \operatorname{Spec} A \,\middle|\, \mathfrak{p} = \sqrt{((0) : (x))} \text{ for some } x \in A\right\}$. But in the proof of the uniqueness statement for primary decomposition, we showed that

  $$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} = \left\{\mathfrak{p} \in \operatorname{Spec} A \,\middle|\, \mathfrak{p} = \sqrt{((0) : (x))} \text{ for some } x \in A\right\},$$

  so $\operatorname{Ann}_A(x)$ must be among the $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. □

Solution to Exercise 7.30. Let A be a PID. Then A is a Noetherian integral domain, hence any nonzero $a \in A$ factors as a product of units and irreducible elements. It then suffices to show irreducible elements of A are prime.

Let a be an irreducible element of A. It is enough to show (a) is maximal. If (a) is not maximal, there exists some ideal I of A such that $(a) \subsetneq I \subsetneq A$. Since A is a PID, $I = (b)$ for some $b \in A$. Since $(a) \subset I = (b)$, there exists $r \in A$ such that $a = br$. Since b is not a unit (otherwise $I = (b) = A$) and a is irreducible, r is a unit. Then we can write $b = ar^{-1}$ and $(a) = aA = ar^{-1}A = (ar^{-1})$, so

$$(a) = (ar^{-1}) = (b) = I$$

contradicting $(a) \subsetneq I$. Thus (a) is maximal. We conclude that irreducible elements of A are prime.

Note that our argument also shows that any PID has (Krull) dimension at most 1. □

Solution to Exercise 7.31. Suppose $f(a_0) = 0$ in $\mathbb{Z}/(p)$ and $f'(a_0) \neq 0$ in $\mathbb{Z}/(p)$. For each $n \in \mathbb{Z}_{\geqslant 1}$, define $a_n \in \mathbb{Z}/(p^{n+1})$ by

$$a_n \coloneqq a_{n-1} - f(a_{n-1})q_n,$$

where $f'(a_{n-1})q_n \equiv 1$ in $\mathbb{Z}/(p^{n+1})$.

- *a_n is well-defined*: To see each a_n is well-defined, we need to show such a q_n exists and is unique. Uniqueness follows from the fact any unit has a unique inverse, so it suffices to show $f'(a_{n-1})$ is a unit in $\mathbb{Z}/(p^{n+1})$. Since

  $$(\mathbb{Z}/(p^{n+1}))^\times = \{u \in \mathbb{Z}/(p^{n+1}) \mid p \nmid u \text{ in } \mathbb{Z}\} = \{u \in \mathbb{Z}/(p^{n+1}) \mid u \neq 0 \text{ in } \mathbb{Z}/(p)\},$$

  it is enough to show $f'(a_{n-1}) \neq 0$ in $\mathbb{Z}/(p)$. This follows from the following induction argument on $n \in \mathbb{Z}_{\geqslant 1}$.

  If $n = 1$ then since $f'(a_0) \not\equiv 0 \pmod p$ by hypothesis, $p \nmid f'(a_0)$, hence the base case follows. Now suppose $n \in \mathbb{Z}_{\geqslant 2}$ and that for each $k \in \{0, 1, \ldots, n-2\}$ we have $f(a_k) = 0$ in $\mathbb{Z}/(p^{k+1})$ and $p \nmid f'(a_k)$ in $\mathbb{Z}$. Under this assumption, the existence and uniqueness of q_k are guaranteed, and we can write

  $$\begin{aligned} a_{n-1} &\equiv a_{n-2} - \cancelto{\equiv 0 \pmod p}{f(a_{n-2})}q_{n-1} \pmod p \equiv a_{n-2} \pmod p \\ &\equiv a_{n-3} - \cancelto{\equiv 0 \pmod p}{f(a_{n-3})}q_{n-2} \pmod p \equiv \cdots \equiv a_0 \pmod p. \end{aligned}$$

  Applying f' to both sides, we obtain

  $$f'(a_{n-1}) \equiv f'(a_0) \pmod p \not\equiv 0 \pmod p,$$

  where the last incongruence is by hypothesis. It follows that $p \nmid f'(a_{n-1})$, which completes the induction argument. By our previous comments, this shows q_n as defined exists and is unique for all $n \in \mathbb{Z}_{\geqslant 1}$.

- *a_n satisfies the desired properties*: We now show that for all $n \in \mathbb{Z}_{\geqslant 1}$, $f(a_n) = 0$ in $\mathbb{Z}/(p^{n+1})$ and that $a_n = a_{n-1}$ in $\mathbb{Z}/(p^n)$. We argue by induction on $n \in \mathbb{Z}_{\geqslant 1}$. The base case is just our hypothesis (that $f(a_0) = 0$ in $\mathbb{Z}/(p)$ and $f'(a_0) \neq 0$ in $\mathbb{Z}/(p)$), so let

$n \in \mathbb{Z}_{\geqslant 1}$ and assume the claim is true for all integers $1, \ldots, n-1$. Since $f(a_{n-1}) = 0$ in $\mathbb{Z}/(p^n)$, $f(a_{n-1}) = t_n p^n$ in $\mathbb{Z}$ for some $t_n \in \mathbb{Z}$.

We can then see $a_n = a_{n-1}$ in $\mathbb{Z}/(p^n)$, since in $\mathbb{Z}/(p^n)$ we have

$$a_n = a_{n-1} - f(a_{n-1})q_n = a_{n-1} - \cancelto{0}{t_n p^n} a_{n-1} = a_{n-1}$$

To see $f(a_n) = 0$ in $\mathbb{Z}/(p^{n+1})$, first write $f(x)$ as

$$f(x) = \sum\nolimits_{j=0}^{N} b_j x^j,$$

where $N = \deg f$ and $b_1, \ldots, b_N \in \mathbb{Z}$. Then we can compute $f(a_n)$ in the ring $\mathbb{Z}/(p^{n+1})$ as follows:

$$\begin{aligned}
f(a_n) &= \sum\nolimits_{j=0}^{N} b_j a_n^j = \sum\nolimits_{j=0}^{N} b_j (a_{n-1} - t_n p^n q_n)^j \\
&= \sum\nolimits_{j=0}^{N} b_j \left(\sum\nolimits_{k=0}^{j} \binom{j}{k} a_{n-1}^j (-1)^{j-k} p^{j-k} t_n^{j-k} q_n^{j-k} \right) \quad \text{(by the binomial theorem)} \\
&= \sum\nolimits_{j=0}^{N} b_j (a_{n-1}^j - a_{n-1}^{j-1} t_n p^n q_n) \qquad \text{(since } p^\ell \text{ for } \ell \geqslant n+1 \text{ vanishes in } \mathbb{Z}/(p^{n+1})\text{)} \\
&= \sum\nolimits_{j=0}^{N} b_j a_{n-1}^j - t_n p^n q_n \sum\nolimits_{j=0}^{N} j b_j a_{n-1}^{j-1} = f(a_{n-1}) - t_n p^n \cancelto{1}{q_n f'(a_{n-1})} \\
&= f(a_{n-1}) - f(a_{n-1}) = 0.
\end{aligned}$$

Hence $f(a_n) = 0$ in $\mathbb{Z}/(p^{n+1})$.

- *Uniqueness of a_n*: Suppose some $a_n' \in \mathbb{Z}/(p^{n+1})$ satisfies

  $$f(a_n') = 0 \text{ in } \mathbb{Z}/(p^{n+1}) \quad \text{and} \quad a_n' = a_{n-1} \text{ in } \mathbb{Z}/(p^n).$$

  Then a_n' and a_n are both equal to a_{n-1} in $\mathbb{Z}/(p^n)$, so there is some $t \in \mathbb{Z}$ such that $a_n' = a_n + tp^n$ in $\mathbb{Z}$. Then

  $$f(a_n') = f(a_n + tp^n) = f(a_n) + f'(a_n)tp^n \text{ in } \mathbb{Z}/(p^{n+1}),$$

  where the second equality by the. same calculation as in the proof of existence above. Since $f(a_n) = f(a_n') = 0$ in $\mathbb{Z}/(p^{n+1})$, it follows that

  $$f'(a_n)tp^n = 0 \text{ in } \mathbb{Z}/(p^{n+1}). \tag{11.12.3}$$

  But

  $$a_n \equiv a_{n-1} \pmod{p^n} \equiv a_{n-2} \pmod{p^{n-1}} \equiv \cdots \equiv a_0 \pmod{p},$$

  so $f(a_n) \neq 0$ in $\mathbb{Z}/(p)$. Then in particular $f(a_n) \neq 0$ in $\mathbb{Z}/(p^{n+1})$, so it follows from Equation (11.12.3) that $tp^n \equiv 0 \pmod{p^{n+1}}$. Thus t is divisible by p, so $a_n' = a_n + tp^n \equiv a_n$ in $\mathbb{Z}/(p^{n+1})$, proving uniqueness. □

Solution to Exercise 7.32. Let $f(x) = x^3 + 3x + 1$. It follows from a simple computation that the only simple root $a_0 \in \mathbb{Z}/(5)$ for f in $\mathbb{Z}/(5)$ is $a_0 \coloneqq 1$. By Hensel's lemma there exists a unique $a_1 \in \mathbb{Z}/(25)$ given by $a_1 = 1 - f(a_0)q_1 = 1 - 5q_1$, where $q_1 \in \mathbb{Z}/(25)$ satisfies the system

$$\begin{cases} f(1 - 5q_1) = 0 & \text{in } \mathbb{Z}/(25), \\ \quad 1 - 5q_1 = a_0 \ (= 1) & \text{in } \mathbb{Z}/(5). \end{cases}$$

By inspection $q_1 \coloneqq 1 \in \mathbb{Z}/(25)$ satisfies these conditions, so

$$a_1 = 1 - 5(1) = 21 \text{ in } \mathbb{Z}/(25).$$

Again by Hensel's lemma, there is a unique element $a_2 \in \mathbb{Z}/(125)$ given by $a_2 = a_1 - f(a_1)q_2 = 1 - 75q_2$, where $q_2 \in \mathbb{Z}/(125)$ satisfies the system

$$\begin{cases} f(a_1 - 75q_2) = 0 & \text{in } \mathbb{Z}/(125), \\ \quad a_1 - 75q_2 = a_1 \ (= 21) & \text{in } \mathbb{Z}/(25). \end{cases}$$

By checking the elements of $\mathbb{Z}/(125)$ that equal $a_1 = 21$ in $\mathbb{Z}/(25)$, we obtain $a_2 = 71$ in $\mathbb{Z}/(125)$. In particular, the equation $f(x) = 0$ has a solution $x = 71$ in $\mathbb{Z}/(125)$.

We claim there are no other solutions in $\mathbb{Z}/(125)$. To see this, suppose $f(b) = 0$ in $\mathbb{Z}/(125)$ for some $b \in \mathbb{Z}/(125)$. Then $f(b) = 0$ in $\mathbb{Z}/(5)$ (resp. $\mathbb{Z}/(25)$), since any integer k divisible of 125 must be divisible by 5 (resp. 25). There are two roots of f in $\mathbb{Z}/(5)$, namely 1 and 2, but the only simple root is 1. If we can show $b = 1$ in $\mathbb{Z}/(5)$, then by the uniqueness clause of Hensel's lemma we can conclude $b = 71$ in $\mathbb{Z}/(25)$. Suppose for a contradiction $b = 2$ in $\mathbb{Z}/(5)$. Then in $\mathbb{Z}/(25)$ we must have $b \in \{2, 7, 12, 17, 22\}$. But $f(2) = f(7) = f(12) = f(17) = f(22) = 15$ in $\mathbb{Z}/(25)$, contradicting $f(b) = 0$ in $\mathbb{Z}/(25)$. Thus $b \neq 2$, leaving $b = 1$ as the only possibility. Thus there are no other solutions in $\mathbb{Z}/(125)$. □

Solution to Exercise 7.33. (a) Note that $f(x) \coloneqq x^4 + 1$ satisfies $f(x+1) = x^4 + 4x^3 + 6x^2 + 4x + 2$, so $f(x+1)$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion for $p = 2$ since $p = 2$ divides all nonzero coefficients except the leading coefficient and $p^2 = 4$ does not divide the constant term 2. Thus $f(x+1)$ is irreducible in $\mathbb{Q}[x]$, so $f(x)$ must be too (since otherwise the irreducible polynomial $f(x+1)$ would factor by replacing x with $x+1$ in the factorization of $f(x)$).

To see $f(x) \coloneqq x^6 + x^3 + 1$ is irreducible in $\mathbb{Q}[x]$, note that we can apply Eisenstein's criterion to $f(x+1) = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3$ for $p = 3$. Indeed, the leading coefficient is not divisible by 3 and the constant term 3 is not divisible by $p^2 = 9$, while the rest of the coefficients of $f(x+1)$ are divisible by 3. Thus $f(x+1)$ is irreducible in $\mathbb{Q}[x]$. It follows that $f(x)$ is irreducible in $\mathbb{Q}[x]$ (since otherwise the irreducible polynomial $f(x+1)$ would factor by replacing x with $x+1$ in the factorization of $f(x)$).

(b) We claim $x^2 + y^2 - 1$ is irreducible over $\mathbb{Q}[x, y]$. We will use Eisenstein's criterion, viewing $f(x) \coloneqq x^2 + y^2 - 1$ as a polynomial in x over the integral domain $\mathbb{Q}[y]$. Then we can write

$$f(x) = a_2x^2 + a_1x + a_0,$$

where $a_2 = 1$, $a_1 = 0$, and $a_0 = y^2 - 1$. We want a prime ideal $\mathfrak{p}$ of $\mathbb{Q}[y]$ such that

- $1 = a_2 \notin \mathfrak{p}$,
- $0 = a_1 \in \mathfrak{p}$,
- $y^2 - 1 = a_0 \in \mathfrak{p}$, and
- $y^2 - 1 = a_0 \notin \mathfrak{p}^2$.

Consider the ideal $\mathfrak{p} = (y-1) \in \mathbb{Q}[x]$. Since the map $g(y) \mapsto g(1)$ induces an isomorphism

$\mathbb{Q}[y]/(y-1) \xrightarrow{\cong} \mathbb{Q}$ and $\mathbb{Q}$ is a field, $\mathfrak{p} := (y-1)$ is maximal in $\mathbb{Q}[y]$, hence prime. As $\mathfrak{p}$ is a proper ideal, $1 = a_0 \notin \mathfrak{p}$. Also, both $a_0 = y^2 - 1 = (y-1)(y+1)$ and $a_1 = 0$ are in $\mathfrak{p}$. To see the last point $a_0 = y^2 - 1 \notin \mathfrak{p}^2$, suppose the contrary. Then $(y-1)(y+1) = y^2 - 1 \in \mathfrak{p}^2$, and thus $y + 1 \in \mathfrak{p}$, forcing $y + 1 = (y-1)g(y)$ for some $g(y) \in \mathbb{Q}[y]$. But $y - 1$ is irreducible in $\mathbb{Q}[y]$, so $g(y) = q$ for some $q \in \mathbb{Q}$, which contradicts the fact $(y-1)q \neq y + 1$ for any $q \in \mathbb{Q}$. Thus by Eisenstein's criterion, $f(x, y) = x^2 + y^2 - 1$ is irreducible over $(\mathbb{Q}(y))[x]$. But $\mathbb{Q}[y]$ is itself a UFD (as a polynomial ring over a field), so the prime elements of $(\mathbb{Q}[y])[x]$ are the irreducible elements of $\mathbb{Q}[y]$ together with the primitive polynomials of $(\mathbb{Q}[y])(x)$ that are irreducible in $(\mathbb{Q}(y))[x]$. Since $f(x, y)$ is of the latter type, we conclude $f(x, y)$ is irreducible in $(\mathbb{Q}[y])(x_0) \cong \mathbb{Q}[x, y]$.

Notice that the above proof *verbatim* shows that $f(x) := x^2 + y^2 - 1$ is an irreducible element of $\mathbb{C}[x, y]$, after replacing any occurrence of "$\mathbb{Q}$" with "$\mathbb{C}$." □

Proof of Lemma 8.2. Assume for contradiction that there exists a nonzero element $m + \operatorname{Tor}(M)$ in $M/\operatorname{Tor}(M)$ that is a torsion element. This means there exists a nonzero $a \in A$ such that $am \in \operatorname{Tor}(M)$. If m were not in $\operatorname{Tor}(M)$, there would exist a nonzero $a' \in A$ with $a'(am) = 0$, implying $(a'a)m = 0$. However, $a'a \neq 0$ since A is an integral domain, which contradicts the assumption that $m \notin \operatorname{Tor}(M)$. Therefore, $m + \operatorname{Tor}(M)$ must be zero in $M/\operatorname{Tor}(M)$, contradicting our assumption. Hence, $M/\operatorname{Tor}(M)$ is torsion-free. □

Proof of Proposition 8.3. Let $\{v_1, \ldots, v_r\}$ be a maximal linearly independent subset of M. (Such a subset exists because if M is torsion-free, then even the singleton set $\{m_1\}$ is linearly independent, and adding more m_i's to this set can only change it from linearly dependent to linearly independent once. Since there are finitely many generators, there exists a maximal linearly independent subset of them.) Then, for each i, the set $\{m_i, v_1, \ldots, v_r\}$ is linearly dependent. Therefore, there exist $a^i_j \in A$ and $b_i \in A \setminus \{0\}$ such that

$$b_j m_j + \sum\nolimits_{j=1}^{r} a^i_j v_j = 0.$$

Now set $b := b_1 b_2 \cdots b_n$. Then bM is a submodule of the free submodule $\langle v_1, \ldots, v_r \rangle$, since if $m = a_1 m_1 + \cdots + a_n m_n$, then

$$\begin{aligned} bm &= a_1 \Big(\prod\nolimits_{i \neq 1} b_i\Big) b_1 m_1 + \cdots + a_n \Big(\prod\nolimits_{i \neq n} b_i\Big) b_n m_n \\ &= a_1 \Big(\prod\nolimits_{i \neq 1} b_i\Big) \Big(-\sum\nolimits_{j=1}^{r} a^1_j v_j\Big) + \cdots + a_n \Big(\prod\nolimits_{i \neq n} b_i\Big) \Big(-\sum\nolimits_{j=1}^{r} a^n_j v_j\Big) \\ &\in \langle v_1, \ldots, v_r \rangle. \end{aligned}$$

Since $\langle v_1, \ldots, v_r \rangle$ is free of rank r, and by Exercise 11.4, bM is free as well. Because M is torsion-free, the A-module map $M \to bM$ given by $m \mapsto bm$ has kernel zero (and is certainly surjective), so $bM \cong M$ as A-modules. But bM was free, so we conclude that M is free. □

Proof of Corollary 8.5. $M/\operatorname{Tor}(M)$ is torsion-free by Lemma 8.2, hence free by Proposition 8.3. Therefore, there exists a nonempty set I such that $M/\operatorname{Tor}(M) \cong \bigoplus_{i \in I} A$. Then by Exercise 11.5, the short exact sequence

$$0 \longrightarrow \operatorname{Tor}(M) \longrightarrow M \longrightarrow M/\operatorname{Tor}(M) \to\!\!\longrightarrow 0$$

admits a section $s\colon M/\operatorname{Tor}(M) \to M$, hence splits. It follows that

$$M \cong \underbrace{M/\operatorname{Tor}(M)}_{=:F} \oplus \underbrace{\operatorname{Tor}(M)}_{=:T}.$$

Since M is finitely generated, any generating set of F must be finite, so in particular F has finite rank $r \in \mathbb{Z}_{\geqslant 1}$. Since the rank is well-defined, there exists a unique $r \in \mathbb{Z}_{\geqslant 0}$ (where $r = 0$ corresponds to the case $F = 0$, or equivalently when $M = \operatorname{Tor}(M)$). The module T is a torsion module, since any $m \in T = \operatorname{Tor}(M)$ is a torsion element by definition of $\operatorname{Tor}(M)$. Hence, any finitely generated module M over a PID A can be written as $M \cong A^{\oplus r} \oplus T$. □

Proof of 8.10 (Lemma 8.10). Fix $(p) \in \operatorname{Spec} A$. If $a \in A$, then $M[(a)] \subset M[(a^2)]$ (since if $ra = 0$ then certainly $ra^2 = 0$). Thus the sequence

$$M[(p)] \subset M[(p^2)] \subset M[(p^3)] \subset \cdots$$

is an ascending chain in M, which is a Noetherian module as a finitely generated module over the Noetherian ring A. Thus there exists $n_p \in \mathbb{Z}_{\geqslant 1}$ such that for all $\ell \in \mathbb{Z}_{\geqslant 0}$, we have $M[(p^{n_p+\ell})] = M[(p^{n_p})]$. Hence $M_{p^\infty} = M[(p^{n_p})]$.

Now, let $\mathcal{P} = \{(p) \in \operatorname{Spec} A \mid M_{p^\infty} \neq 0\}$. If $\mathcal{P}$ were infinite, then choose distinct $(p_1), (p_2), (p_3), \dots \in \mathcal{P}$ and observe that

$$M[(p_1)] \subset M[(p_1^{n_1} p_2^{n_2})] \subset M[(p_1^{n_1} p_2^{n_2} p_3^{n_3})] \subset \cdots$$

is an increasing chain of submodules of M, which must stabilize. That is, there exists $k \in \mathbb{Z}_{\geqslant 0}$ such that for all $\ell \in \mathbb{Z}_{\geqslant 0}$,

$$M\Big[\prod\nolimits_{i=1}^{k} p_i^{n_i}\Big] = M\Big[\prod\nolimits_{i=1}^{k+\ell} p_i^{n_i}\Big].$$

Set $m \coloneqq \prod_{i=1}^{k} p_i^{n_i}$. Then for all $x \in M_{p_{k+1}^\infty}$, we have $x \in M[(p_{k+1}^{n_{p_{k+1}}})] \subset M[mp_{k+1}^{n_{p_{k+1}}}] = M[m]$. Hence $p_{k+1}^{n_{k+1}} x = 0$ implies $p_{k+1}x = 0$ and $mx = 0$. But A is a PID, so $(m, p_{k+1}^{n_{k+1}}) = A$, and thus $ax = 0$ for all $a \in A$. We conclude that $x = 0$. Thus $M_{p_{k+1}^\infty} = 0$, and similarly, $M_{p_{k+i}^\infty} = 0$ for all $i \geqslant 1$. □

Proof of 8.11 (Theorem 8.11). We will show existence in (2), then existence in (1), then uniqueness in (1), then uniqueness in (2).

- *Existence in (2)*: Consider the set Σ defined as $\Sigma \coloneqq \{\lambda(N) \mid \lambda \in \operatorname{Hom}_A(M, A)\}$, the collection of ideals of A given by A-linear functionals on M. Since $\Sigma \neq \varnothing$ (as $\lambda = 0 \in \Sigma$), and since A is Noetherian (being a PID), there exists a maximal element in Σ, say $(q_1) = \lambda_1(N)$ for some $\lambda_1 \in \operatorname{Hom}_A(M, A)$.

  Note $q_1 \neq 0$: if $N \neq (0)$, for any basis $v_1, \dots, v_n$ of M and any nonzero $n \in N$, we can write $n = \sum_{i=1}^{n} a_i v_i$ for some nonzero $a_i \in A$. Thus, the map $\lambda \coloneqq \operatorname{pr}_i \in \operatorname{Hom}_A(M, A)$ that projects onto the i-th coordinate sends n to a nonzero element. Hence, $(q_1) = \lambda(N)$ is nonzero, implying $q_1 \neq 0$.

  Choose $f_1 \in N$ such that $\lambda_1(f_1) = q_1$. Then, for all $\lambda \in \operatorname{Hom}_A(M, A)$, $\lambda(f_1) \in (q_1)$. Otherwise, a suitable linear combination

  $$(a\lambda + b\lambda_1)(f_1) = \gcd(q_1, \lambda(f_1))$$

would contradict the maximality of (q_1). Thus, $f_1 = q_1 e_1$ for some $e_1 \in M$, writing f_1 in any basis of M as $f_1 = \sum_{i=1}^n a_i v_i$; the projections to the ith coordinate p_i give $p_i f_1 = a_i \in (q_1)$.

We observe:

- $M = Ae_1 \oplus \ker(\lambda_1)$: For all $m \in M$, $m = \lambda_1(m)e_1 + (m - \lambda_1(m)e_1)$, where the latter is in $\ker(\lambda_1)$ since $\lambda_1(e_1) = 1$. Thus, $M = Ae_1 + \ker(\lambda_1)$. If $\lambda_1(ae_1) = 0$, then $a \cdot 1 = 0$, so $Ae_1 \cap \ker(\lambda_1) = (0)$.
- $\ker(\lambda_1)$ is free (of rank $n-1$): Indeed, as A is a PID, and $N = Af_1 \oplus \ker(\lambda_1|_N)$, we find that $\ker(\lambda_1|_N)$ is free.

For the inductive step, assume that there exists a basis $e_2, \ldots, e_r$ of $\ker(\lambda_1)$ and ideals $(q_2) \supset (q_3) \supset \cdots \supset (q_r)$ of A such that $q_2e_2, \ldots, q_re_r$ is a basis of $\ker(\lambda_1|_N) = N \cap \ker(\lambda_1)$. We may further assume that our induction hypothesis says (q_2) is maximal in the set

$$\{\lambda(\ker(\lambda_1|_N)) \mid \lambda \in \mathrm{Hom}_A(\ker \lambda_1, A)\}.$$

We must check $q_1 \mid q_2$. For all $\lambda \in \mathrm{Hom}_A(M, A)$, $\lambda(N_1) \subset (q_1)$. If not, extend λ to M by setting $\lambda(e_1) = 0$, and then for some $n_1 \in N_1$ with $\lambda(n_1) \notin (q_1)$, a linear combination

$$(a\lambda_1 + b\lambda)(f_1 + n_1) = aq_1 + b\lambda(n_1)$$

equals $\gcd(q_1, \lambda(n_1))$, contradicting the maximality of (q_1). Thus, $(q_2) \subset (q_1)$, that is, $q_1 \mid q_2$. This proves existence in (2).

- *Existence in (1)*: Let $m_1, \ldots, m_n$ be generators of M. Consider an exact sequence $0 \to G \to A^n \xrightarrow{\pi} M \to 0$, where $G = \ker(\pi)$ and $\pi(a_1, \ldots, a_n) = \sum_{i=1}^n a_i m_i$. Applying the existence of (2) to the inclusion $G \subset A^n$, we get a basis $e_1, \ldots, e_n$ of A^n and $q_1 \mid q_2 \mid \cdots \mid q_n$ such that for some r, s with $r + s = n$, $q_1e_1, \ldots, q_se_s$ is a basis of G and $q_{r+1} = \cdots = q_{r+s} = 0$. Thus
$$M \cong A^{\oplus r} \oplus \bigoplus\nolimits_{j=1}^s A/(q_j).$$

- *Uniqueness in (1)*: let M be a finitely generated A-module. From existence, we know $M \cong A^{\oplus r} \bigoplus_{j=1}^s A/(q_j)$ for some $r, s \in \mathbb{Z}_{\geqslant 0}$. We want to show $r, s, q_1, \ldots, q_s$ (with all $q_j \neq 0$ and non-units) are uniquely determined by M. Uniqueness of r is just because $r = \mathrm{rk}(M/\mathrm{Tor}(M))$. It remains to show uniqueness of the torsion submodule of M. We may assume $r = 0$ (since otherwise we can consider $M/A^{\oplus r}$). Let p be any prime of A such that $p \mid q_i$. Set $M[p] = \{x \in M \mid px = 0\}$. In the decomposition $M = \bigoplus_{j=1}^s A/(q_j)$, an $m \in M$ lies in $M[p]$ if and only if when we write $m = m_1 + \cdots + m_s$, $m_j \in A/q_j$, each
$$m_j \in A/(q_i)[p] = \begin{cases} (0) & \text{if } p \nmid q_i, \\ \frac{q_i/pA}{q_iA} & \text{if } p \mid q_i. \end{cases}$$
In this latter case where $p \mid q_i$, $\frac{(q_i/p)\cdot A}{q_iA} \cong A/p$ via $\frac{q_i}{p}x \mapsfrom x$. Consequently, $|\{j \mid p \text{ divides } q_j\}| = \dim_{A/p}(M[p])$ (dimension as a vector space). In particular, for any p such that $p \mid q_1$, we deduce that $s = \dim_{A/p} M[p]$. For any other decomposition $M = \bigoplus_{i=1}^{s'} A/(q_i')$ (with q_j nonzero non-units) such that $(q_i') \mid (q_2') \mid \cdots \mid (q_s')$, $\dim_{A/p} M[p] = |\{j \mid p \text{ divides } q_j'\}| \leqslant s'$. The argument here is symmetric with respect to s and s', so we also obtain the other inequality $s' \leqslant s$. Hence $s = s'$, so s is independent of the choice of decomposition with the divisibility property.

And moreover, for any p dividing q_1, p also divides each q'_j. So, for any two decompositions like this, they have the same number of terms, and any prime appearing in the first layer of one must appear in the first layer of the other, hence in all other terms.

We can now finish the proof of uniqueness by inducting on the number of prime factors of $\prod_{j=1}^{s} q_j$. Namely, look at t submodule pM of M. Still with $p \mid q_1$, we have

$$pM \cong \bigoplus_{j=1}^{s} \frac{pA}{q_jA} \cong \bigoplus_{j=1}^{s} A/(q_j/p).$$

Then by induction, since $\frac{q_1}{p} \mid \frac{q_2}{p} \mid \cdots \mid \frac{q_s}{p}$, we see that the q_j/p are uniquely determined (by the IH), so by multiplying by p we obtain uniqueness of the q_j. This proves uniqueness of (1).

- Uniqueness of (2): This follows directly from the uniqueness of (1) as follows. Choose a basis $\{e_1, \ldots, e_n\}$ of M with $\{q_1e_1, \ldots, q_ne_n\}$ (discarding those i such that $q_ie_i = 0$) as a basis of $N \subseteq M$ and $q_1 \mid q_2 \mid \cdots \mid q_n$. Then, for some t, s, r,

$$\underbrace{q_1, \ldots, q_t}_{\in A^\times}, \underbrace{q_{t+1}, \ldots, q_{t+s}, q_{t+s+1}}_{\neq 0 \text{ and } \notin A^\times}, \underbrace{q_{n=t+s+r}}_{=0}.$$

Then

$$M/N \simeq A^r \oplus \bigoplus_{j=1}^{s} A/(q_{t+j}),$$

and by uniqueness in (1), N and the sequence $(q_{t+1}), \ldots, (q_{t+s})$ are uniquely determined. But then so is $t = n - r - s$ and necessarily $(q_1) = \cdots = (q_t) = A$. □

Proof of Corollary 8.13. By Lemma 8.10 $M_{p^\infty} = 0$ for all but finitely many $(p) \in \operatorname{Spec} A$. Let $\mathcal{P} = \{(p) \in \operatorname{Spec} A \mid M_{p^\infty} \neq 0\}$. Since $\mathcal{P}$ is finite, we can write M as a direct sum of its p^∞-torsion submodules for each $(p) \in \mathcal{P}$, and a direct summand that is torsion-free. Formally,

$$M \cong \left(\bigoplus_{(p)\in\mathcal{P}} M_{p^\infty}\right) \oplus T,$$

where T is a torsion-free A-module.

By part (1) of Theorem 8.11, T is isomorphic to a direct sum of a free A-module and a direct sum of cyclic modules of the form $A/(q_i)$ for some $q_i \in A$, which gives us the desired decomposition. □

Proof that 8.13 and 8.11 together imply 8.14 (Corollary 8.14). By Corollary 8.5 we can write $M \cong A^{\oplus r} \oplus \operatorname{Tor}(M)$ for some $r \in \mathbb{Z}_{\geqslant 0}$. Since $M_{p^\infty} \subset \operatorname{Tor}(M)$ by definition of M_{p^∞}, we define a map

$$\begin{aligned} \varphi\colon \bigoplus_{(p)\in\operatorname{Spec} A} M_{p^\infty} &\longrightarrow \operatorname{Tor}(M), \\ \{m_{(p)}\}_{(p)\in\operatorname{Spec} A} &\longmapsto \sum_{(p)\in\operatorname{Spec} A} m_{(p)}. \end{aligned}$$

This map is a module homomorphism by the universal mapping property of direct sums, so it remains to show that it is injective and surjective.

- *φ is surjective*: Let $x \in \operatorname{Tor}(M)$. By definition, $\operatorname{Ann}_A(x) \neq 0$. Since A is a PID, we have $\operatorname{Ann}_A(x) = (a)$ for some nonzero $a \in A$. As A is a PID, a can be factored, so $a = up_1^{n_1} \cdots p_k^{n_k}$ for some unit $u \in A^\times$ and distinct prime elements $p_i \in A$, $n_i \in \mathbb{Z}_{\geqslant 0}$. For each $i \in \{1, \ldots, k\}$, define

$$a_i := \frac{a}{p_i^{n_i}} = u \prod_{\substack{j=1 \\ j \neq i}}^{k} p_j^{n_j}.$$

Then $(a_1, \ldots, a_k) = A$. Hence, we can write

$$1 = \sum_{i=1}^{k} r_i a_i.$$

In particular, $x = \sum_{i=1}^{k} r_i a_i x$. Observe that $r_i a_i x \in M_{p_i^\infty}$, since $p_i^{n_i}(r_i a_i x) = r_i a x = 0$. Thus, φ is surjective.

- *φ is injective*: Suppose $\{m_i\}_{i=1}^{k} \in \ker(\varphi)$, where $m_i \in M_{p_i^\infty} = M[(p_i^{n_i})]$. Then $\sum_{i=1}^{k} m_i = 0$, with k minimal. Consequently, $-m_1 = m_2 + \cdots + m_k$. Since $p_1^{n_1} m_1 = 0$, we have $p_1^{n_1}(m_2 + \cdots + m_k) = 0$. Also,

$$p_2^{n_2} p_3^{n_3} \cdots p_k^{n_k}(m_2 + \cdots + m_k) = 0,$$

which implies

$$\operatorname{Ann}_A(m_1) = \operatorname{Ann}_A(m_2 + \cdots + m_k) \supset (p_1^{n_1}, p_2^{n_2} \cdots p_k^{n_k}) = A,$$

so $\operatorname{Ann}_A(m_1) = A$. This means $m_1 = 0$, which contradicts the minimality of k. Thus φ is injective, which completes the proof. □

Proof of Theorem 8.17. (1) As $m_T = \operatorname{Ann}_{k[x]}(V_T)$ and $V_T \cong \bigoplus k[x]/(q_i(x))$, we have $m_T(x) = q_s(x)$, where each q_j divides q_s. Since m_T and q_s are monic, $m_T = q_s$.

(2) The decomposition of V_T guides our choice of basis: in the i-th summand, choose the basis $(1, x, \ldots, x^{\deg q_i - 1})$. Then, with respect to this basis, T has the form of a block diagonal matrix with each block being a companion matrix $\mathscr{C}_{q_i}$. Thus RCF is unique.

(3) A and B are conjugate in $\mathrm{GL}_n(k)$ if they represent the same linear transformation. Hence, if $\mathrm{RCF}(A) = \mathrm{RCF}(B)$, they are conjugate. For the second part, consider L extending k. If A and B are conjugate in $\mathrm{GL}_n(L)$, then their RCFs are the same in $L[x]$. Since the q_is are in $k[x]$, it follows that A and B are conjugate in $\mathrm{GL}_n(k)$.

(4) $p_T(x) := \det(xI_n - T)$, where $A = \mathrm{RCF}(T)$. Then $p_T(x) = \prod \det(xI_{\deg q_i} - \mathscr{C}_{q_i}) = q_1(x) q_2(x) \cdots q_s(x)$. Since $q_1 \mid q_2 \mid \cdots \mid q_s = m_T(x)$, $m_T(x) \mid p_T(x)$, and they share the same roots, considering multiplicity. □

Proof of Theorem 8.19. As a $k[x]$-module, there exists an isomorphism $V \cong \bigoplus_{i=1}^{r} k[x]/(x - \lambda_i)^{d_i}$ for some d_i and λ_is. The matrix of multiplication by x on $k[x]/(x-\lambda)^d$, in the basis $(1, x - \lambda, \ldots, (x-\lambda)^{d-1})$, is the Jordan block $J_{\lambda,d}$. □

Proof of Corollary 8.20. If A is diagonalizable, say $PAP^{-1} = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$, then the minimal polynomial $m_A(x) = \prod_{\text{distinct } \lambda_i}(x - \lambda_i)$. Conversely, if m_A has distinct roots, then each Jordan block J_{λ_i, d_i} of A satisfies $m_{J_{\lambda_i,d_i}}(x) = (x - \lambda_i)^{d_i}$, and since m_A has distinct roots, we have $d_i = 1$ for all i. Hence, A is diagonalizable. We now make this precise:

($\Rightarrow$) Suppose $P^{-1}AP = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$ for some $P \in \mathrm{GL}_n(k)$. Then A satisfies $m(A) = 0$ for $m(x) = \prod_{i \in S}(x - \lambda_i)$ where $S \subset \{1, \ldots, n\}$ is a subset such that $\lambda_i \neq \lambda_j$ for $i, j \in S$ and

$\{\lambda_i \mid i \in \{1, \ldots, n\}\} = \{\lambda_i \mid i \in S\}$. By definition, $m_A(x) \mid m(x)$, so $m_A(x)$ has distinct roots. (As easily checked, $m_A(x) = m(x)$).

($\Leftarrow$) We know there exists some $P \in \mathrm{GL}_n(k)$ such that

$$P^{-1}AP = \begin{pmatrix} J_1 & & \\ & \ddots & \\ & & J_r \end{pmatrix}$$

where we are writing J_i to mean J_{λ_i, d_i} for each $i \in \{1, \ldots, r\}$ The minimal polynomial of each J_i is $(x - \lambda_i)^{d_i}$: this follows quickly from a direct calculation, or from the fact that the invariant factor decomposition of k^{d_i} as a $k[x]$-module, with x acting via J_i, is given by $k^{d_i} = k[x]/(x - \lambda_i)^{d_i}$. Thus $m_A(x) = \mathrm{lcm}_{i=1,\ldots,r}((x - \lambda_i)^{d_i})$, and the assumption that m_A has distinct roots forces all $d_i = 1$, that is, $P^{-1}AP$ is diagonal. □

Proof of Proposition 8.31. $V = M$ as a $\mathbb{C}$-vector space, $Tv = xv$. So $v \in E_\lambda \iff (T - \lambda I)^n v = 0 \iff v \in M_{(x-\lambda)^\infty}$. □

Solution to Exercise 8.33. (a) Any $\mathbb{F}_2[x]$-module M of order 8 is finite, and hence finite-dimensional as an $\mathbb{F}_2$-vector space. Thus $M \cong \mathbb{F}_2^n$ for some $n \in \mathbb{Z}_{\geqslant 0}$. Thus $8 = |M| = |\mathbb{F}_2^n| = 2^n$, so $n = 3$; it follows that M is 3-dimensional as an $\mathbb{F}_2$-vector space.

It follows from the corollary to the structure theorem that we can write isomorphism classes of $\mathbb{F}_2[x]$-modules of order 8 take the form $M \cong \bigoplus_{i=1}^k \mathbb{F}_2[x]/(p_i(x)^{r_i})$ for $k \in \mathbb{Z}_{\geqslant 1}$ such that $p_i \in \mathbb{F}_2[x], r_i \in \mathbb{Z}_{\geqslant 1}$ are not necessarily distinct and the p_i are irreducible, and $\sum_{i=1}^k r_i \deg p_i = 3$.

First note that the following are all irreducible polynomials of degree at most 3 in $\mathbb{F}_2[x]$: $x^3 + x^2 + 1, x^3 + x + 1, x^2 + x + 1, x + 1, x$. Indeed, if any of these were reducible they would have a root in $\mathbb{F}_2$ but none of these do. And there are no more irreducibles, because the rest of the polynomials of degree at most 3 are $x^3 + 1 = (x + 1)(x^2 + x + 1)$, $x^3 + x^2 + x = x(x^2 + x + 1)$, $x^3 + x^2 + x + 1 = (x + 1)^3$, $x^2 + 1 = (x + 1)^2$, $x^2 + x = x(x + 1)$, which are all reducible.

We break into cases depending on the integer k. By the structure theorem any two isomorphism classes from different k are distinct, so when listing all possible isomorphism classes for a given k we only need to check that multiplication by x is a distinct linear transformation.

- $k = 1$: The possibilities and the corresponding action of multiplication by x in the basis $(1, x, x^2)$ are as follows:

  (1) $\frac{\mathbb{F}_2[x]}{(x^3+x+1)}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix};$

  (2) $\frac{\mathbb{F}[x]}{(x^3+x^2+1)}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix};$

(3) $\frac{\mathbb{F}_2[x]}{(x^3)}$, $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$;

(4) $\frac{\mathbb{F}[x]}{((x+1)^3)}$, $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$;

- $k = 2$: The possibilities and the corresponding action of multiplication by x in the basis $(1, x) \oplus (1)$, respectively, are as follows:

(5) $\frac{\mathbb{F}_2[x]}{(x^2+x+1)} \oplus \frac{\mathbb{F}_2[x]}{(x+1)}$, $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$;

(6) $\frac{\mathbb{F}_2[x]}{(x^2+x+1)} \oplus \frac{\mathbb{F}_2[x]}{(x)}$, $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$;

(7) $\frac{\mathbb{F}_2[x]}{(x^2)} \oplus \frac{\mathbb{F}_2[x]}{(x)}$, $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$;

(8) $\frac{\mathbb{F}_2[x]}{((x+1)^2)} \oplus \frac{\mathbb{F}_2[x]}{(x+1)}$, $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$;

(9) $\frac{\mathbb{F}_2[x]}{((x+1)^2)} \oplus \frac{\mathbb{F}_2[x]}{(x)}$, $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$;

(10) $\frac{\mathbb{F}_2[x]}{(x^2)} \oplus \frac{\mathbb{F}_2[x]}{(x+1)}$, $\begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$;

- $k = 3$: The possibilities and the corresponding action of multiplication by x in the basis $(1) \oplus (1) \oplus (1)$ are as follows:

(11) $\frac{\mathbb{F}_2[x]}{(x+1)} \oplus \frac{\mathbb{F}_2[x]}{(x+1)} \oplus \frac{\mathbb{F}_2[x]}{(x+1)}$, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$;

(12) $\frac{\mathbb{F}_2[x]}{(x)} \oplus \frac{\mathbb{F}_2[x]}{(x)} \oplus \frac{\mathbb{F}_2[x]}{(x)}$, $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$;

(13) $\frac{\mathbb{F}_2[x]}{(x)} \oplus \frac{\mathbb{F}_2[x]}{(x+1)} \oplus \frac{\mathbb{F}_2[x]}{(x+1)}$, $\begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$;

(14) $\frac{\mathbb{F}_2[x]}{(x+1)} \oplus \frac{\mathbb{F}_2[x]}{(x)} \oplus \frac{\mathbb{F}_2[x]}{(x)}$, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. □

(b) By Corollary 8.22, we have the following possibilities:

(1) $\mathbb{F}_2[x]/(q(x))$ for $q(x) = x^3 + ax + bx + 1$ for some $a, b \in \mathbb{F}_2$ (where the nonzero constant term is equivalent to the condition $\mathscr{C}_q$ is invertible). Breaking into irreducibles and consulting our list of irreducibles in part (a), we have the following cases, where the RCF is in the basis $(1, x, x^2)$:

(1a) $\mathbb{F}_2[x]/(x^3 + x + 1)$, whose RCF is $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$,

(1b) $\mathbb{F}_2[x]/(x^3 + x^2 + 1)$, $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$,

(1c) $\mathbb{F}_2[x]/((x-1)(x^2 + x + 1)) \cong \frac{\mathbb{F}_2[x]}{(x-1)} \oplus \frac{\mathbb{F}_2[x]}{(x^2+x+1)}$, $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$, and

(1d) $\mathbb{F}_2[x]/((x-1)^3)$, $\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$.

(2) $\mathbb{F}_2[x]/(x-1) \oplus \mathbb{F}_2[x]/((x-1)^2)$, where the RCF is $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$, in the basis $(1) \oplus (1, x)$.

(3) $\mathbb{F}_2[x]/(x-1) \oplus \mathbb{F}_2[x]/(x-1) \oplus \mathbb{F}_2[x]/(x-1)$, where the RCF is $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ in the basis $(1) \oplus (1) \oplus (1)$.

Solution to Exercise 8.34. (a) Note that $\mathrm{im}(f)$ is a submodule of the free $\mathbb{Z}$-module $\mathbb{Z}^m$, so by the second clause of the structure theorem for finitely generated modules over a PID there exists a basis $(e'_1, \ldots, e'_m)$ for $\mathbb{Z}^m$ for which there are unique $q_1, \ldots, q_s \in \mathbb{Z}$ satisfying $q_1 \mid q_2 \mid \cdots \mid q_s$ and the nonzero elements of the ordered set $(q_1e'_1, \ldots, q_se'_s)$, say $(q_{i_1}e'_{i_1}, \ldots, q_{i_r}e'_{i_r})$ for $i_1 < \cdots < i_r$, is a basis for $\mathrm{im}(f)$. (Of course, since $q_1 \mid q_2 \mid \cdots \mid q_n$, our only choice for $i_1, \ldots, i_r$ is $i_1 = 1, i_2 = 2, \ldots, i_r = r$.)

For each $j \in \{1, \ldots, r\}$, since $q_{i_j}e'_{i_j} \in \mathrm{im}(f)$, there exists some nonzero $e_j \in \mathbb{Z}^m$ such that $f(e_j) = q_{i_j}e'_{i_j}$. Observe that $\{e_1, \ldots, e_r\}$ is linearly independent in $\mathbb{Z}^n$. To see this, suppose the contrary. Then (without loss of generality) e_1 can be expressed as a linear combination $e_1 = \sum_{j=1}^r n_je_j$ for some $n_1, \ldots, n_r \in \mathbb{Z}$. But then

$$q_{i_1}e'_{i_1} = f(e_1) = f\Big(\sum\nolimits_{j=1}^r n_je_j\Big) = \sum\nolimits_{j=1}^r n_jf(e_j) = \sum\nolimits_{j=1}^r n_j(q_{i_j}e'_{i_j}),$$

which contradicts the linear independence of $\{q_1e'_1, \ldots, q_re'_r\}$ in $\mathbb{Z}^m$. Thus $\{e_1, \ldots, e_r\}$ is linearly independent in $\mathbb{Z}^m$.

The short exact sequence $0 \to \ker f \to \mathbb{Z}^n \to \mathrm{im}\, f \to 0$ splits by Exercise 11.5(a) , so $\mathbb{Z}^n \cong \ker f \oplus \mathrm{im}\, f$. Since $\ker f$ is a free submodule of the free $\mathbb{Z}$-module, we can pick a basis $\{e_{r+1}, \ldots, e_n\}$ for $\ker f$. Then $(e_1, \ldots, e_n)$ is a basis of $\mathbb{Z}^n$. Because $(q_{i_1}, \ldots, q_{i_r})$ is a basis for the image, for each $j \in \{r+1, \ldots, n\}$ we can write $f(e_j)$ as a linear combination $f(e_j) = \sum_{k=1}^{r} a_{kj} q_{i_k} e'_{i_k}$ for some $a_{i_k} \in \mathbb{Z}$.

We now write the $\mathbb{Z}$-linear combination f as a matrix with respect to the ordered bases $(e_1, \ldots, e_n)$ for the source $\mathbb{Z}^n$ and $(e'_{i_1}, \ldots, e'_{i_m})$ for the target $\mathbb{Z}^m$, where the $e'_{i_1}, \ldots, e'_{i_r}$ are as before and $e'_{i_{r+1}}, \ldots, e'_{i_m}$ is any indexing of $\{e'_1, \ldots, e'_m\} \smallsetminus \{e'_{i_1}, \ldots, e'_{i_r}\}$. Then

$$f(e_j) = \begin{cases} q_{i_j} e'_{i_j} & \text{if } j \in \{1, \ldots, r\}, \\ \sum_{k=1}^{r} a_{kj} q_{i_k} e'_{i_k} \text{ for some } a_{jk} \in \mathbb{Z} & \text{if } j \in \{r+1, \ldots, m\}. \end{cases}$$

Thus the matrix A of f in these bases is

$$A = \left(\begin{array}{ccc|ccc} q_{i_1} & & & q_{i_1} a_{1,r+1} & \cdots & q_{i_1} a_{1,n} \\ & \ddots & & \vdots & \ddots & \vdots \\ & & q_{i_r} & q_{i_r} a_{r,r+1} & \cdots & q_{i_r} a_{r,n} \\ \hline & 0 & & & 0 & \end{array}\right).$$

The column operation that takes a column and subtracts an integer multiple of some other column is invertible, so by subtracting appropriate multiples of the first r columns from the last $n-r$ columns and transforming our ordered basis vectors $e_{r+1}, \ldots, e_n$ accordingly, we obtain bases in which f is written as

$$A' = \begin{pmatrix} q_{i_1} & & & & & \\ & \ddots & & & & \\ & & q_{i_r} & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

Since $q_{i_1} \mid q_{i_2} \mid \cdots \mid q_{i_r}$, this matrix takes the desired form. This completes the proof.

(b) Let A be the matrix representing $f \colon \mathbb{Z}^n \to \mathbb{Z}^n$ with respect to the standard ordered basis. Before we begin, first note that by part (a) A is similar (in $M_n(\mathbb{Z})$) to some $A' = \operatorname{diag}(q_1, \ldots, q_n)$ with each of $q_1, q_2, \ldots, q_n$ nonzero, so $\det A = \det A' = q_1 q_2 \cdots q_n$.

If A is singular then $\det A = q_1 q_2 \cdots q_n = 0$, so because $\mathbb{Z}$ is an integral domain one of the q_js is zero. Thus, by the divisibility condition, $q_s = 0$. Since $\mathbb{Z}^n \cong \ker f \oplus \operatorname{im} f$, at least the direct summand corresponding to $\mathbb{Z}/(q_s)$ in the decomposition of $\operatorname{im} f$ is $\mathbb{Z}/(q_s) = \mathbb{Z}/(0) \cong \mathbb{Z}$, which is infinite, so the cokernel $\mathbb{Z}^n/\operatorname{im}(f) \cong \ker f$ has an infinite direct summand. Since the index of $\operatorname{im}(f)$ in $\mathbb{Z}^n$ is the cardinality of this cokernel by definition, we have $[\mathbb{Z}^n \colon \operatorname{im}(f)] = \infty$.

On the other hand, suppose A is nonsingular. Then $\det A = \det A' = q_1 q_2 \cdots q_n \neq 0$, so each q_i is nonzero. Then

$$\frac{\mathbb{Z}^n}{\operatorname{im}(f)} \cong \frac{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}{q_1\mathbb{Z} \oplus \cdots \oplus q_n\mathbb{Z}} \cong \frac{\mathbb{Z}}{q_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{q_n\mathbb{Z}} \tag{11.12.4}$$

is a finite set since each direct summand is finite. (Here we used that if $\{M_i\}_{i \in I}$ are R-modules and $N_i \subset M_i$ is a submodule for each $i \in I$, then the natural map $\bigoplus_{i \in I} M_i \to$

$\bigoplus_{i\in I}\frac{RM_i}{N_i}$ is a surjective module homomorphism with kernel $\bigoplus_{i\in I} N_i$, and thus induces a natural isomorphism $\frac{\bigoplus_{i\in I} M_i}{\bigoplus_{i\in I} N_i} \xrightarrow{\cong} \bigoplus_{i\in I}\frac{M_i}{N_i}$.) Taking cardinalities in Equation (11.12.4), we conclude

$$[\mathbb{Z}^n : \operatorname{im}(f)] = \left|\frac{\mathbb{Z}}{q_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{q_n\mathbb{Z}}\right| = q_1 q_2 \cdots q_n < \infty,$$

as desired. Since $q_1 q_2 \cdots q_s = \det A' = \det A$, we conclude in this situation that $[\mathbb{Z}^n : \operatorname{im}(f)] = \det A$. □

Solution to Exercise 8.35. Write

$$A = \begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{pmatrix} \xrightarrow{R_2 -= 4R_1} \begin{pmatrix}1 & 2 & 3\\ 0 & -3 & -6\\ 7 & 8 & 9\end{pmatrix} \xrightarrow{R_3 -= 7R_1} \begin{pmatrix}1 & 2 & 3\\ 0 & -3 & -6\\ 0 & -6 & -12\end{pmatrix}$$

$$\xrightarrow{R_3 -= 2R_2} \begin{pmatrix}1 & 2 & 3\\ 0 & -3 & -6\\ 0 & 0 & 0\end{pmatrix} \xrightarrow{C_3 += 2C_2} \begin{pmatrix}1 & 2 & 7\\ 0 & -3 & 0\\ 0 & 0 & 0\end{pmatrix}$$

$$\xrightarrow{C_2 -= 2C_1} \begin{pmatrix}1 & 0 & 7\\ 0 & -3 & 0\\ 0 & 0 & 0\end{pmatrix} \xrightarrow{C_3 -= 7C_1} \begin{pmatrix}1 & 0 & 0\\ 0 & -3 & 0\\ 0 & 0 & 0\end{pmatrix}$$

$$\xrightarrow{C_2 \times = -1} \begin{pmatrix}1 & 0 & 0\\ 0 & 3 & 0\\ 0 & 0 & 0\end{pmatrix},$$

which is in the desired form. This is equivalent to obtaining bases of the source and target in which the matrix f has the desired form (since one can trace backward the sequence of invertible transformations and then apply them to the standard basis to obtain the desired basis), and after doing so we obtain $A = Q^{-1}AP$, where

$$Q = \begin{pmatrix}1 & 0 & 0\\ 4 & -1 & 0\\ 1 & -2 & 1\end{pmatrix} \qquad \text{and} \qquad P = \begin{pmatrix}1 & 2 & 3\\ 0 & 1 & 2\\ 0 & 0 & 1\end{pmatrix}.$$ □

Solution to Exercise 8.36. We first assume the finite case holds and prove the infinite case. Since $\operatorname{span}\{T_i\}_{i\in I}$ is a vector subspace of the k-vector space $\operatorname{End}_k(V)$ and $\dim(\operatorname{End}_k(V)) = \dim(V)^2$ is finite, $\operatorname{span}\{T_i\}_{i\in I}$ has some finite basis $(T_{i_1}, \ldots, T_{i_r})$ for some $r \leqslant n^2$. By the finite case, there exists a basis of V simultaneously diagonalizing each T_{i_j}. Any k-linear combination of finitely many simultaneously diagonalized maps is itself simultaneously diagonalized by linearity, so we are done because each $T \in \operatorname{span}\{T_i\}_{i\in I}$ is a k-linear combination of the T_i.

We now prove the finite case by induction on $|I| =: k \in \mathbb{Z}_{\geqslant 1}$. The base case is immediate by point (i) of the hypothesis, so suppose the claim is true for all integers in $\{1, \ldots, k-1\}$ and let $\{T_i\}_{i=1}^k$ be a collection of pairwise commuting diagonalizable matrices. For each eigenvalue λ of T_k, let

$$E_\lambda = \{v \in V \mid T_k v = \lambda v\}.$$

Then for each $v \in E_\lambda$, we have $T_i v \in E_\lambda$: indeed,

$$T_k(T_i v) = T_i(T_k v) = T_i(\lambda v) = \lambda(T_i v),$$

so $T_i v$ is an eigenvector of T_k with eigenvalue λ. Thus the linear maps $T_1, \ldots, T_{k-1}$ can be be viewed as linear maps $T_i|_{E_\lambda} \colon E_\lambda \to E_\lambda$. Then by the induction hypothesis (which we can apply because the subspace E_λ is itself finite-dimensional), there exists a basis, call it $\mathscr{B}$, of E_λ simultaneously diagonalizing the $T_1, \ldots, T_{k-1}$. And all elements of the basis $\mathscr{B}$ are eigenvectors for $T_k|_{E_\lambda}$ as well, as all (nonzero) elements of E_λ are eigenvectors of T_k (by definition of E_λ). Since T_k is diagonalizable, V is the direct sum of all such E_λ, so obtaining a basis for each direct summand E_λ as above we obtain a basis for V that simultaneously diagonalizes all $T_1, \ldots, T_k$, as desired. This completes the proof. □

Solution to Exercise 8.37. (a) By definition, $T^* w_j^* = w_j^* \circ T$, so for all $i, j \in \{1, \ldots, n\}$,

$$(T^* w_j^*) v_i = v_j^* \circ T(v_i) = w_j^* \circ \left(\sum\nolimits_k a_{ki} w_k\right) = \sum\nolimits_k a_{ki} \underbrace{w_j^* w_k}_{=\delta_{jk}} = a_{ji},$$

so $T^* w_j^*$ is the column vector corresponding to the linear functional $V \to K$ sending v_i to a_{ji}. Thus the matrix A^* of the linear transformation T^* in the bases $\{v_i\}_i$ and $\{w_j\}_j$ is

$$A^* = (a_{ji})_{i,j=1}^n = A^t,$$

the transpose of A.

(b) Suppose V is a K-vector space, $\{v_i\}_{i \in I}$ is a basis for V, and $v \in V, f \in V^*$, and $\operatorname{ev}(v)(f) = 0$. Then $0 = \operatorname{ev}(v)(f) = f(v)$, so $v \in \ker f$. But f was arbitrary, so in particular $v_i^*(v) = 0$ for all $i \in I$. But i was arbitrary, so

$$v = \{v_i\}_{i \in I} = \{v_i^*(v)\}_{i \in I} = \{0\}_{i \in I} = 0.$$

Thus ev is injective.

Now suppose $\dim V < \infty$, let $\{v_1, \ldots, v_n\}$ be a basis for V, and let $q \in (V^*)^*$. Since $\dim V < \infty$ and $\{v_1^*, \ldots, v_n^*\}$ is a basis for V^*, $\dim V^* < \infty$. Similarly, $\{\widehat{v}_1, \ldots, \widehat{v}_n\}$ is a finite basis for $(V^*)^*$, where $\widehat{v}_i \coloneqq (v^*)^*$. To see ev is surjective, it thus suffices to show each basis vector $\widehat{v}_i$ is in the image of ev. It is thus enough to show $\operatorname{ev}(v_i) = \widehat{v}_i$, which we justify as follows. Since $\operatorname{ev}(v_i)(v_j^*) = v_j^*(v_i) = \delta_{ij}$ for all i, j and this property characterizes the basis $\{\widehat{x}_1, \ldots, \widehat{x}_n\}$ dual to $\{v_1^*, \ldots, v_n^*\}$, we conclude $\operatorname{ev}(v_i) = \widehat{v}_i$. Thus ev is surjective, hence an isomorphism. □

Proof of Lemma 9.1. Define $\varphi \colon V^* \to \prod_{i \in I} k$ by

$$\varphi(\lambda) \coloneqq \{x_i\}_{i \in I} \in \prod\nolimits_{i \in I} k,$$

where $x_i = \lambda(v_i)$. It is straightforward that φ is a homomorphism of k-vector spaces.

We claim the map $\psi \colon \prod_{i \in I} k \to V^*$ defined by

$$\psi(\{x_i\}_{i \in I}) \coloneqq \left(\sum\nolimits_{i \in I} a_i v_i\right) = \sum\nolimits_{i \in I} a_i x_i$$

(the sums $\sum_{i \in I} a_i v_i$ are finite since $a_i = 0$ for almost every i) is an inverse for φ. One can check that $\{x_i\}_{i \in I} \in \prod_{i \in I} k$, $\psi(\{x_i\}_{i \in I}) \in V^*$, and ψ is a homomorphism of k-vector spaces.

(These are simple checks best left as an exercise.)

To see φ and ψ are inverses, we need to show $\varphi \circ \psi = \mathrm{id}_{\pi_k}$ and $\psi \circ \varphi = \mathrm{id}_{V^*}$. We have $\psi(\varphi(\lambda))(\sum a_i v_i) = \sum a_i x_i$ where $x_i = \lambda(v_i) = \sum a_i \lambda(v_i) = \lambda(\sum a_i v_i)$, that is, $\psi \circ \varphi = \mathrm{id}$, and $(\varphi \circ \psi)(\{x_i\}_{i\in I}) = \varphi(\psi(\{x_i\}_{i\in I})) = (y_i)$ where $y_i = \psi(\{x_i\}_{i\in I})(v_i) = x_i$, so $\varphi \circ \psi = \mathrm{id}$. Thus, $\varphi\colon V^* \to \prod_{i\in I} k$ is an isomorphism. □

Proof of Corollary 9.2. For I finite, $\prod_{i\in I} k = \bigoplus_{i\in I} k$. Then where φ, ψ are as in the proof of Lemma 9.1, we obtain an isomorphism

$$\begin{tikzcd}
V \arrow[r, "\cong"] & \bigoplus_{i\in I} k \arrow[r, equal] & \prod_{i\in I} k \arrow[r, "\cong", "\psi"'] & V^* \\
v_i \arrow[r, mapsto] & e_i \arrow[r] & e_i \arrow[r, mapsto] & \psi(e_i)
\end{tikzcd}$$

and $\psi(e_i)(v_j) = \delta_{ij}$, that is, $\psi(e_i) = v_i^*$, as desired.

We omit the general proof of the second point, but we do give some remarks in the case $\dim_k V = \infty$. For $V = \bigoplus_{i\in I} k$, we have $\dim_k V^* = |\{\text{set maps } I \to k\}|$, which is a strictly larger cardinal than $|I|$ by an argument similar to Cantor's diagonalization argument. We omit the general proof of this, but we do note that in some cases we can easily see that $\bigoplus k \not\cong \prod k$. For example, where p is a prime, $|V| = |\bigoplus_{i\in \mathbb{Z}_{\geqslant 1}} \mathbb{Z}/(p)|$ is countable, but for $k = \mathbb{Z}/p\mathbb{Z}$ and $I = \mathbb{Z}_{\geqslant 1}$ we have $|V^*| = \prod_{i\in\mathbb{Z}_{\geqslant 1}} \mathbb{Z}/(p)$ is uncountable (since it contains countably infinite strings of 0s and 1s, which covers all real numbers when written in binary, and the real numbers are uncountable). □

Proof of Definition 9.11. Define $\varphi\colon V \times W \to V \otimes_k W$ by

$$\varphi(v, w) \coloneqq (v, w) \pmod X.$$

Then φ is K-bilinear by the construction of X. Given any K-bilinear $f\colon V \times W \to U$, define the K-linear $\widetilde{\varphi}\colon \bigoplus_{(v,w)\in V\times W} K(v, w) \to U$ first for generators by $\widetilde{\varphi}((v, w)) = f(v, w)$, then extending uniquely to $\widetilde{\varphi}\colon \bigoplus_{(v,w)} K(v, w) \to U$ by the universal property of the direct sum.

Note that $\widetilde{\varphi}(X) = 0$: it suffices to show $\widetilde{\varphi}$ vanishes on a spanning set of X. And indeed,

$$\begin{aligned}
\widetilde{\varphi}((av + bv', w) - a(v, w) - b(v', w)) &= \widetilde{\varphi}(av + bv', w) - a\widetilde{\varphi}(v, w) - b\widetilde{\varphi}(v', w) \\
&= f(av + bv', w) - af((v, w)) - bf((v', w)) \\
&= f((av + bv', w)) - af((v, w)) - bf((v', w)) \\
&= 0.
\end{aligned}$$

and likewise for the other generators. Since $\widetilde{\varphi}(X) = 0$ (that is, $X \subset \ker \widetilde{\varphi}$), $\widetilde{\varphi}$ factors uniquely through the desired K-linear φ by the universal property of the quotient.

Conversely, given a K-linear map $\varphi\colon V \otimes_k W \to U$, it is immediate that the map $\varphi \circ \otimes$ is bilinear (since lin∘bilin=bilin). The maps $\varphi \mapsto \varphi \circ \otimes$, and the map sending f to its induced map, are easily seen to define inverse isomorphisms of K-vector spaces. (The details are left as an exercise.) □

Proof of Lemma 9.14. Let $\{e_i\}_{i\in I}$ and $\{f_j\}_{j\in J}$ be bases of V and W, respectively. We claim $\{e_i \otimes f_j\}_{(i,j)\in I\times J}$ forms a basis for $V \otimes_k W$.

- $\{e_i \otimes f_j\}_{(i,j)\in I\times J}$ is a spanning set: For any $v \in V$, $w \in W$, we can write $v = \sum_{i\in I} a_i e_i$ (where finitely many a_i are nonzero), and likewise $w = \sum_{j\in J} b_j f_j$ (where finitely many a_i are nonzero). Then
$$\begin{aligned} v \otimes w &= \left(\sum\nolimits_{i\in I} a_i e_i\right) \otimes \left(\sum\nolimits_{j\in J} b_j f_j\right) = \sum\nolimits_{i\in I} a_i (e_i \otimes w) \\ &= \sum\nolimits_{i\in I} a_i \left(\sum\nolimits_{j\in J} b_j (e_i \otimes f_j)\right) = \sum\nolimits_{(i,j)\in I\times J} a_i b_j (e_i \otimes f_j). \end{aligned}$$
Any element of $V \otimes_k W$ is a finite k-linear combination of simple tensors of the form $v\otimes w$, hence can be written as a linear combination of the above form. Thus $\{e_i \otimes f_j\}_{(i,j)\in I\times J}$.
- $\{e_i \otimes f_j\}_{(i,j)\in I\times J}$ is a linearly independent set: Suppose there is a k-linear relation
$$\sum\nolimits_{(i,j)\in I\times J} c_{ij}(e_i \otimes f_j) = 0 \text{ where finitely many } c_{ij} \text{ are nonzero.}$$
Suppose some $c_{i_0 j_0} \neq 0$. Then
$$e_{i_0} \otimes f_{j_0} = \frac{-1}{c_{i_0 j_0}} \sum\nolimits_{\substack{(i,j)\in I\times J \\ (i,j)\neq(i_0,j_0)}} c_{ij}(e_i \otimes f_j). \tag{11.12.5}$$

Now define a k-bilinear map $\lambda\colon V \times W \to k$ by the unique k-bilinear extension of the function
$$H(e_i, f_j) = \begin{cases} 1 & \text{if } (i,j) = (i_0, j_0), \\ 0 & \text{otherwise,} \end{cases}$$
(Such an extension exists and is unique because $\{e_i\}_{i\in I}$ and $\{f_j\}_{j\in J}$ are bases.) This assignment induces a map $\mathrm{Hom}_k(V \otimes_k W, k) \xrightarrow{\cong} \mathrm{Bilin}_k(V \times W, k)$, so by the universal mapping property in Theorem 9.10 there exists a unique $\varphi \in \mathrm{Hom}_k(V \otimes_k W, k)$ such that $H = \varphi \circ \otimes$. Applying φ to Equation (11.12.5), we obtain $\varphi(e_{i_0} \otimes f_{j_0}) = 1$. But for all $(i,j) \neq (i_0, j_0)$ we have $\varphi(e_i \otimes f_j) = H(e_i, f_j) = 0$, so
$$1 = \varphi(\text{LHS of Equation (11.12.5)}) = \varphi(\text{RHS of Equation (11.12.5)}) = 0,$$
a contradiction. □

Proof of Theorem 9.17. We have the commutative diagram
$$\begin{tikzcd}
\mathrm{Hom}_k(V \otimes W, U) \arrow[r, "\cong"] \arrow[d, dash, "\cong"] & \mathrm{Hom}_k(V, \mathrm{Hom}_k(W, U)) \arrow[dl, shift left, "\Psi"] \\
\mathrm{Bilin}_k(V \times W, U) \arrow[ur, shift left, "\Phi"] \arrow[ur, phantom, "\simeq"] &
\end{tikzcd}$$
with $\Phi(f)(v)(w) = f(v,w)$ for any $f \in \mathrm{Bilin}_k(V\times W, U)$, $v \in V$, and $w \in W$ and $\Psi(\varphi)((v,w)) = \varphi(v)(w)$, where $(v,w) \in V \times W$. □

Proof of Corollary 9.26. $\Lambda^n T\colon \Lambda^n V \to \Lambda^n V$ is an endomorphism of a K-vector of rank 1, hence is multiplication by a scalar. (This is intrinsic in the sense that no choice of basis of V is needed.)

The determinant of a linear transformation is axiomatically characterized by being the unique multilinear alternating function on the columns of an $n\times n$ matrix (that is, $\det \in \mathrm{Alt}^n(V^*, K)$ where $V = K^n$ is the space of column vectors & we picture V^n as $M_n(K)$ such that $\det(I) = 1$).

Fix a basis of V, so $V = K^n$ and $\mathrm{End}_K(V) = M_n(K)$. For any $A \in M_n(K)$, define $D(A) = \Lambda^n A$, that is, $Ae_1 \wedge \ldots \wedge Ae_n = D(A)e_1 \wedge \ldots \wedge e_n$. Then $D(I) = 1$, and D is clearly a multilinear function on the columns $Ae_1, \ldots, Ae_n$ of A. □

Solution to Exercise 10.1. Let $P \in \mathrm{Syl}_p(G)$. Then $PH/H \in \mathrm{Syl}_p(G/H)$: indeed, $[G/H : PH/H] = [G : PH] \mid [G : P]$ is coprime to P, and $PH/H \cong P/(P \cap H)$ is a p-group—combining these observations yields $PH/H \in \mathrm{Syl}_p(G/H)$.

The orbit of PH/H under the action of conjugation by G/H is (by the orbit-stabilizer theorem) the index $[G/H : \mathrm{Stab}_{G/H}(PH/H)]$, which has cardinality $|G/H| = [G/H : \mathrm{Stab}_{G/H}(PH/H)]$ and $\mathrm{Stab}_{G/H}(PH/H) > \mathrm{Stab}_G(P)H/H$ (because if $nPn^{-1} = P$, then for all $h \in H$, $hnPHn^{-1}h^{-1} = hnPn^{-1}Hh^{-1} = hPH = hHP = HP = PH$, since $H \lhd G$). Thus

$$\begin{aligned}\mathrm{Syl}_p(G/H) = [G/H : N_{G/H}(PH/H)] \mid [G/H : N_G(P)H/H]\\ = [G : N_G(P) \cdot H] \mid [G : N_G(P)] = |\mathrm{Syl}_p(G)|,\end{aligned}$$

as desired. □

Solution to Exercise 10.2. Let $S = \{\text{maximal proper subgroups of } G\}$. Recall G is not a union of the conjugates of proper subgroups, so in particular $G \neq \bigcup_{H \in S} H$. Hence there exists some $g \in G \smallsetminus (\bigcup_{H \in S} H)$.

Every element of a finite *non-cyclic* group is contained in a maximal proper subgroup, but all maximal proper subgroups have the same size by our hypothesis (since they are all conjugate, hence isomorphic to each other).

But this means g cannot be contained in some maximal proper subgroup (otherwise, it would be in the chain $\bigcup_{H \in S} H$), so G cannot be non-cyclic. □

Solution to Exercise 10.3. ($\Rightarrow$) Suppose M is finitely generated. Then there exists an R-module surjection $R^n \to M \to 0$ for some $n \in \mathbb{Z}$. Since localization is exact, for all i, the induced map $R^n_{f_i} \to M_{f_i}$ is also a surjection, that is, M_{f_i} is finitely generated as an R_{f_i}-module.

($\Leftarrow$) Suppose M_{f_i} is finitely generated as an R_{f_i}-module for each i. Thus, for each i, there exists a finite set of generators $\{m_{i1}, \ldots, m_{in_i}\}$ of M_{f_i}, where each $m_{ij} \in M$ and $n_i \in \mathbb{Z}_{\geqslant 1}$. These generators can be expressed as $\left\{\frac{m_{ij}}{f_i^{r_{ij}}}\right\}_{j=1}^{n_i}$ for M_{f_i}, where $r_{ij} \in \mathbb{Z}$. We claim that

$$\{m_{ij}\}_{i \in \{1,\ldots,r\}, j \in \{1,\ldots,n_i\}}$$

generates M as an R-module. Let $m \in M$. Expressing m in terms of the generators of M_{f_i} (as an R_{f_i}-module), we obtain a relation

$$\left(m - \sum\nolimits_{j=1}^{n_i} \frac{a_{ij}}{f_i^{r_{ij}}} m_{ij}\right) f_i^{t_i} = 0 \text{ in } M,$$

for some $t_i \in \mathbb{Z}$ and $a_{ij} \in R$. Choosing N large enough, for all i, we have

$$f_i^N \cdot m \in \sum\nolimits_{j=1}^{n_i} R \cdot m_{ij} \quad (i = 1, \ldots, r).$$

Since $(f_1, \ldots, f_r) = R$, it implies that $(f_1^N, \ldots, f_r^N) = R$. The relation $\sum_{i=1}^r a_i f_i = 1$ with $a_i \in R$, raised to the Nth power, gives $1 \in (f_1^N, \ldots, f_r^N)$. Thus,

$$1 = \sum\nolimits_{i=1}^{r} b_i f_i^N \quad \text{for some } b_i \in R.$$

Therefore,

$$m = \sum\nolimits_{i=1}^{r} b_i f_i^N \cdot m \in \sum\nolimits_{i=1}^{r} \sum\nolimits_{j=1}^{n_i} R \cdot m_{ij},$$

and we conclude that $\{m_{ij}\}_{\substack{i\in\{1,\ldots,r\} \\ j\in\{1,\ldots,n_i\}}}$ generates M as an R-module. □

Solution to Exercise 10.4. In a UFD, $f \in D[x]$ is primitive means $C(f) = 1$, where

$$C(f) = \prod\nolimits_{\substack{\text{principal} \\ (p)\in Spec(D)}} p^{\operatorname{ord}_p(f)}$$

where $\operatorname{ord}_p(f) = \min\{\operatorname{ord}(a_j) \mid a_j \text{ is a coefficient of } f\}$, and $\operatorname{ord}_p(a) = r$ such that $a = p^r \frac{b}{c}$ for $b, c \in D$ such that $p \mid bc$.

Now, suppose f and g are primitive. We claim that $C(fg) = 1$, which follows from Gauss' lemma. We have $C(fg) = \prod_{\substack{\text{prime} \\ (p)\in Spec(D)}} p^{\operatorname{ord}(fg)}$, and $\operatorname{ord}_p(fg) = \min\{\operatorname{ord}_p(c_k) \mid c_k \text{ is a coefficient of } fg\}$. Coefficients of fg are $c_k = \sum_{i+j=k} a_i b_j$, so $\operatorname{ord}_p(c_k) = r$ such that

$$\sum\nolimits_{i+j=k} a_i b_j = c_k = p^r \frac{b}{c} \text{ where } p \nmid bc.$$

As $\operatorname{ord}_p(a_i b_j) = 0$ (since $\operatorname{ord}_p(a_i) = 0$ and $\operatorname{ord}_p(b_j) = 0$), and indeed, $\operatorname{ord}_p(a_i b_j) = r$ such that $a_i b_j = p^0 \frac{b}{c} p^0 \frac{b'}{c'} = p^0 \frac{bb'}{cc'}$ and $p \nmid c_1 c'$. Thus, $\operatorname{ord}_p(c_k) = 0$, so $\operatorname{ord}_p(fg) = 1$ by arithmetic, hence fg is primitive if f and g are primitive. □

Alternate Solution to 10.4 (Exercise 10.4). $f(x)$ is primitive if for all prime elements $p \in R$, p does not divide every coefficient of $f(x)$. Suppose

$$f(x) = a_n x^n + \ldots + a_0 \in \mathbb{R}[x] \quad \text{and} \quad g(x) = b_m x^m + \ldots + b_0 \in \mathbb{R}[x]$$

are primitive. Let $p \in R$ be a prime element. Let r and s be the largest indices such that $p \nmid a_r$ and $p \nmid b_s$. Let

$$f(x) \cdot g(x) = \sum\nolimits_{i=0}^{m+n} c_i x^i.$$

Then

$$c_{r+s} = \sum\nolimits_{i+j=r+s} a_i \cdot b_j = a_r \cdot b_s + T,$$

where T is a sum of terms $a_i \cdot b_j$ such that $i > r$ or $j > s$, hence $p \mid T$. As p is prime, $p \nmid a_r \cdot b_s$, so $p \nmid c_{r+s}$. We conclude that $f(x) \cdot g(x)$ is primitive. □

Solution to Exercise 10.5. We have $A \cdot \operatorname{adj}(A) = \det(A) \cdot I_n$. If A is invertible, then $\det(A) \neq 0$, $\operatorname{adj}(A)$ is invertible, and $\operatorname{rk}(\operatorname{adj}(A)) = n$.

Otherwise, if $\operatorname{rk}(A) < n - 1$, then all $(n-1) \times (n-1)$ minors of A are 0, so $\operatorname{adj}(A) = 0$ and has rank 0.

If $\operatorname{rk}(A) = n-1$, then $\operatorname{adj}(A) \neq 0$, so $\operatorname{rk}(\operatorname{adj}(A)) \geqslant 1$. However, $\operatorname{im}(\operatorname{adj}(A)) \subset \ker(A)$, which is 1-dimensional, so $\operatorname{rk}(\operatorname{adj}(A)) = 1$. □

Solution to Exercise 10.6. We have $245 = 5 \cdot 7^2 \cdot n_7(G) \equiv 1 \pmod 7$ and $n_7(G) \mid 5$ (by Sylow's), so $n_7(G) = 1$. Likewise, $n_5(G) \equiv 1 \pmod 5$ and $n_5(G) \mid 7^2$, so $n_5(G) = 1$. By the conjugacy of Sylow p-subgroups, the unique Sylow 5-subgroup P and Sylow 7-subgroup Q are both normal in G. Since $P \cap Q = \{1\}$ (by Lagrange's theorem), we have $|P \cdot Q| = |P| \cdot |Q| = |G|$. Then since both $P, Q \lhd G$, it follows that $G \cong P \times Q$.

Now, up to isomorphism, P is unique, $P \simeq C_5$, and for Q there are two possibilities: $Q \simeq C_{49}$ or $Q \simeq C_7 \times C_7$. So by Exercise 4.1 G is isomorphic to exactly one of the following: $C_5 \times C_{49} (= C_{245})$ or $C_5 \times C_7 \times C_7$. □

Solution to Exercise 10.7. Let X be the finite set G/H of left cosets of H in G, and let $G\times$ act by $g \cdot (aH) = gaH$. This induces a group map $\alpha \colon G \to Aut_{set}(X)$ with kernel $\ker \alpha = \bigcap_{a \in X} \operatorname{Stab}_G(aH) = \bigcap_{aH \in G} aHa^{-1} \subset H$. Thus here $\alpha \subset H$, so we only need to show $|G/\alpha| < \infty$. And indeed, $G/\alpha \cong \operatorname{im} \alpha < S_{[G:H]}$, and $S_{[G:H]}$ is a finite group since $[G : H]$ is finite, so $|G/\ker \alpha| < \infty$. □

Solution to Exercise 10.8. $H = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ with the unique associative $\mathbb{R}$-algebra structure such that $\mathbb{R}$ is central, $i^2 = j^2 = k^2 = -1$, $ij = k$, $ji = -k$. Define $H \xrightarrow{\varphi} M_2(\mathbb{C})$ by the unique $\mathbb{R}$-linear extension of $1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $i \to \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $j \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, and $k \to \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. The images $\varphi(i)$, $\varphi(j)$, $\varphi(k)$, $\varphi(\mathbb{R})$ satisfy the relations, so such a φ exists.

More formally, H is presented as the quotient of the non-commutative polynomial ring $\mathbb{R}\langle i, j \rangle$ in two variables modulo the two-sided ideal generated by $i^2 + 1$, $j^2 + 1$, $ij + ji$, and φ comes from the universal mapping property of this quotient. □

Solution to Exercise 10.9. (a) Let $A = (\mathbb{Z}/6\mathbb{Z})$ and set $e = 3$ in A. . Then $e^2 = 3^2 = 9 \equiv 3 \pmod 6 = e$ but $e \neq 0, 1$.

(b) Suppose $e^2 = e$. Then $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$, so $1 - e$ is idempotent.

(c) For the reverse implication, take $e = (1, 0) \in A_1 \times A_2$. For the forward implication, suppose an element $e \in A$ satisfies. Then $e(1-e) = e - e^2 = 0$, so because e and $(1-e)$ are coprime (as $1 = (1-e) + e$, hence $A = (e) + (1-e)$) we have by the Chinese remainder theorem that

$$A \cong \frac{A}{(0)} \cong \frac{A}{(e(1-e))} = \frac{A}{(e)(1-e)} \cong \frac{A}{(e)} \times \frac{A}{(1-e)},$$

which is a direct product of two nonzero rings. □

Solution to Exercise 10.10. (a) The polynomial $x^7 + 48x - 24$ is a primitive polynomial in $\mathbb{Z}[x]$, so it is irreducible in $\mathbb{Q}[x]$ if it is irreducible in $\mathbb{Z}[x]$ (by Gauss's lemma). By Eisenstein's criterion for $p = 3$, it is irreducible in $\mathbb{Z}[x]$. The same argument works to prove irreducibility in $\mathbb{Q}(i)[x]$, where $\mathbb{Q}(i)$ is the fraction field of $\mathbb{Z}[i]$, and $\mathbb{C}[i]$ is a UFD and 3 is a prime element in $\mathbb{Z}[i]$ (to prove 3 irreducible; if $3 = \alpha\beta$, then $9 = N(\alpha) \cdot N(\beta)$ where $N(a+bi) = a^2+b^2$, $a, b \in \mathbb{Z}$. Then either one of α, β is a unit or $3 = N(\alpha) = N(\beta)$; but $3 = a^2 + b^2$ has no integer solutions.)

(b) Let $f(x, y) = x^3 + y + y^5$ in $\mathbb{C}[x, y]$. Then as a polynomial in $(\mathbb{C}[y])[x]$, we have $f(x) = x^3 + a_0$, where $a_0 = y + y^5$. Then $f(x)$ is irreducible in $(\mathrm{Frac}(\mathbb{C}[y]))[x] = (\mathbb{C}(y))[x]$; $a_0 = y(y+1)(y-1)(y+i)(y-i)$ satisfies for $\mathfrak{p} := (y)$ that $a_0 \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$, and then applying Eisenstein.

In addition, $\mathbb{C}[y]$ is a UFD (since $\mathbb{C}$ is), so by Gauss's lemma the irreducibles of $\mathbb{C}[y]$ are the irreducibles of $\mathbb{C}$ together with the irreducibles of $(\mathrm{Frac}(\mathbb{C}[y]))[x] = \mathbb{C}(y)[x]$ that are prime as elements of $\mathbb{C}[y][x]$; so, since $g(x) = x^4 + a_0$ is certainly primitive as an element of $(\mathbb{C}[y])[x]$, we conclude it is irreducible in $\mathbb{C}[x, y]$. □

Solution to Exercise 10.11. (a) $\mathbb{Q}$ is *not* finitely generated, since for all $x_1, \ldots, x_n \in \mathbb{Q}$, $\sum_{i=1}^n \mathbb{Z}x_i$ only contains elements α with $\mathrm{ord}_p(\alpha) \geqslant 0$ for all primes p such that $\mathrm{ord}_p(x_i) \geqslant 0$ for all i, which is all but finitely many p. $\mathbb{Q}$ is torsion-free (as $\mathbb{Q}$ is a domain containing $\mathbb{Z}$ as a subring), and $\mathbb{Q}$ is not free because if $\mathbb{Q} = \bigoplus_{i \in I} \mathbb{Z}x_i$ for some set I and rational numbers x_i (that is, for $x_i \in \mathbb{Q}$), then we see $|I| = 1$ since any two x_i, x_j satisfy $ax_i + bx_j = 0$ for some $a, b \in \mathbb{Z}\backslash\{0\}$ (namely, if $x_i = a_i/b_i$ and $x_j = a_j/b_j$, then $b_j a_i x_i - b_i a_j x_j = 0$ works if $x_i x_j \neq 0$). But clearly $\mathbb{Q} \neq \mathbb{Z}x$ for some x (since $\mathbb{Q}$ is not finitely generated).

(b) $\mathbb{Q}/\mathbb{Z}$ is not finitely generated (similar to (a)), is not torsion-free ($2 \cdot \frac{1}{2} = 0$), and is not free (since it is not torsion-free).

(c) Let $\omega = (-1 + \sqrt{-3})/2$. Note $\omega^2 + \omega + 1 = 0$ ($\omega^3 = 1, \omega \neq 1$). $\mathbb{Z}[\omega] = \{\sum_{n=0}^N a_n\omega^n \mid a_n \in \mathbb{Z}\}$. Since $\omega^2 = -\omega - 1$, any $\sum_{n=0}^N a_n\omega^n$ equals $a + b\omega$ for some $a, b \in \mathbb{Z}$, so $\mathbb{Z}[\omega]$ is finitely generated and free with basis $\{1, \omega\}$. (The freeness follows since $a + b\omega = 0 \Rightarrow a = 0$ and $b = 0$ by consideration of real and imaginary parts, or since $\mathbb{Z}[x]/(x^2 + 1)$ is free with basis $\{1, x\}$.) So, $\mathbb{Z}[\omega]$ is torsion-free because it is free. □

Solution to Exercise 10.12. Let A be a PID. We will show that the primary ideals of A are precisely (0) and $\mathfrak{m}^n$ for any $\mathfrak{m} \in \mathrm{Max}(A)$ and $n \in \mathbb{Z}_{\geqslant 1}$.

Let $\mathfrak{q}$ be a primary ideal. Then $\sqrt{\mathfrak{q}}$ is prime, so (since A is a PID) it is either (0) or a maximal ideal $\mathfrak{m}$. If $\sqrt{\mathfrak{q}} = (0)$, then $\mathfrak{q} = (0)$. If $\sqrt{\mathfrak{q}} = \mathfrak{m}$ is maximal, then $\sqrt{\mathfrak{q}} = (\mathfrak{p})$ for a nonzero prime element $\mathfrak{p} \in A$ (again, since A is a PID). In this situation, $\mathfrak{p}^n \in \mathfrak{q}$, and we may assume $\mathfrak{p}^n \in \mathfrak{q}$ but $\mathfrak{p}^{n-1} \notin \mathfrak{q}$. Then $\mathfrak{q} = (\mathfrak{p}^n)$. Since $\mathfrak{q} = (y)$ for some $y \in A$, we have $\mathfrak{p}^n = y \times x$ for some $x \in A$. By unique factorization, $y = \mathfrak{p}^k$ for some $k \leqslant n$. Since $\mathfrak{p}^{n-1} \notin \mathfrak{q}$, in fact $k = n$.

On the other hand, (0) is prime, hence primary, and we have seen that $\mathfrak{m}^n$ is primary for any maximal ideal $\mathfrak{m}$. □

Solution to Exercise 10.13. Conjugacy classes on $M_n(k)$ correspond to $\mathscr{C}_{q_1} \oplus \cdots \oplus \mathscr{C}_{q_s}$ where q_i is as in the structure theorem and $\mathscr{C}_{q_i}$ is the companion matrix of q_i for all $i \in \{1, \ldots, s\}$ and $\sum_{i=1}^s \deg q_i = 2$. We may assume the q_i's are monic since the q_is are unique up to units (that is, since the chain $(q_1) \supset (q_2) \supset \cdots \supset (q_s)$ is what is unique in the structure theorem).

And we need conjugacy classes in $\mathrm{GL}_2(\mathbb{Z}/(p))$ (not $M_2(\mathbb{Z}/(p))$), so the $\mathscr{C}_{q_i}$ must each be invertible, or equivalently the q_is must have nonzero constant term. This gives two cases:

- $s = 1$: $q_1(x) = x^2 + ax + b$ where $a \in \mathbb{Z}/(p), b \in \mathbb{Z}/(p) \smallsetminus \{0\}$. There are exactly $p(p-1)$ ways to have this.
- $s = 2$: $q_1(x) = x - a, q_2(x) = x - b, q_1 \mid q_2 \Rightarrow a = b$, and here $a \in \mathbb{Z}/(p) \smallsetminus \{0\}$. There are exactly $p - 1$ ways to have this.

Thus, there are exactly $p(p-1) + (p-1) = p^2 - 1$ conjugacy classes in $\mathrm{GL}_2(\mathbb{Z}/(p))$. □

Solution to Exercise 10.14. ($\Leftarrow$) Suppose $\gcd(a_1, \ldots, a_n) = 1$. Then $\mathbb{Z}/\mathbb{Z}v$ is torsion-free: suppose instead there exists $w \in \mathbb{Z}^n \smallsetminus \{0\}$ and some $k \in \mathbb{Z} \smallsetminus \{0\}$ such that $k(w + \mathbb{Z}v) = 0 + \mathbb{Z}r$. Without loss of generality, we may assume k is a prime p. Then $pw = c\mathbb{Z}$ for some $c \in \mathbb{Z}$, so either p divides a_j for all j or p divides c. If p divides c, then $w = c'v$ for some $d \in \mathbb{Z}$, contradicting $w \notin \mathbb{Z}$ so p divides a_j for all j. But then $p \nmid \gcd(a_1, \ldots, a_n) = 1$, contradicting our hypothesis. Thus $\mathbb{Z}/\mathbb{Z}v$ is torsion-free.

Now $\mathbb{Z}^n/\mathbb{Z}v$ is torsion-free, hence free. Then, by Exercise 11.5 (since π is a surjection in the short exact sequence $0 \to \mathbb{Z}v \to \mathbb{Z}^n \to \mathbb{Z}^n/\mathbb{Z}v \to 0$ and $\mathbb{Z}^n/\mathbb{Z}v$ is free), the short exact sequence splits, so $\mathbb{Z}^n \cong \mathbb{Z}v \oplus \mathbb{Z}^n/\mathbb{Z}v$.

As $\mathbb{Z}^n/\mathbb{Z}v$ is a free submodule of the free module $\mathbb{Z}^n$, we can choose a basis B for $\mathbb{Z}^n/\mathbb{Z}v$. Then $\{v\} \cup B$ is a basis for $\mathbb{Z}v \oplus (\mathbb{Z}^n/\mathbb{Z}v) \cong \mathbb{Z}^n$, as desired.

($\Rightarrow$) Conversely, suppose for a contradiction we can extend v to a basis $(v_1, w_2, \ldots, w_n)$ of $\mathbb{Z}^n$ but that $\gcd(a_1, a_2, \ldots, a_n) = d > 1$. Then $\mathbb{Z}^n \cong \mathbb{Z}v \oplus \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$, so $\mathbb{Z}^n/\mathbb{Z}v \cong \mathbb{Z}w_1 \oplus \cdots \oplus \mathbb{Z}w_n$ is free, hence torsion-free. But $\gcd(a_1, \ldots, a_n) = d > 1$, so $\frac{1}{d} \cdot v \neq 0$ in $\mathbb{Z}/\mathbb{Z}v$. Thus $\frac{1}{d}v$ is a nonzero torsion element of $\mathbb{Z}/\mathbb{Z}v$, a contradiction. □

Solution to Exercise 10.15. (a) Since $Q \lhd P$, P acts on Q by conjugation, yielding a group homomorphism $\alpha\colon P \to \mathrm{Aut}(C_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. By Lagrange's theorem, $\alpha(P) = \{1\}$.

(b) Let $P = C_{p^2} \rtimes_\alpha C_p$, where the homomorphism $\alpha\colon C_p \to \mathrm{Aut}_{\mathrm{Grp}}(C_{p^2}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times$ giving the conjugation sends a generator of C_p to an element of order p. (Such a p exists by Sylow I). □

Solution to Exercise 10.16. (a) $M = N + J(A) \cdot M$. Then $M/N = J(A) \cdot M/N$ (and M/N is again a finitely generated R-module with generators the equivalence classes of the original finite generating set of M), so by Nakayama $M/N = 0$, that is, $M = N$.

(b) Consider $\mathfrak{m}_A \cdot B \subset \mathfrak{m}_B$. Since B is Noetherian, we have $\mathfrak{m}_B = \mathfrak{m}_A \cdot B + \mathfrak{m}_B \cdot \mathfrak{m}_B$. By part (a), $\mathfrak{m}_A \cdot B = \mathfrak{m}_B \cdot B$. Since B is a finitely generated A-module, we can conclude $N = M$, where $\varphi(A) = B$. Hence φ is surjective. □

Solution to Exercise 10.17. As M is finitely generated, we can write $M = Am_1 + \cdots + Am_n$ for some $n \in \mathbb{Z}_{\geqslant 1}$ and some $m_1, \ldots, m_n \in M$.

($\subset$) First suppose $\mathfrak{p} \in V(\mathrm{Ann}_A(M))$, that is, $\mathfrak{p} \supset \mathrm{Ann}_A(M)$. Now suppose for a contradiction $M_\mathfrak{p} = 0$. Then for each i there exists $s_i \in A \smallsetminus \mathfrak{p}$ such that $s_i m_i = 0$. Then for

$s = s_1 s_2 \cdots s_n$, we have $sm_i = 0$ for all i, so $sM = 0$. But s is also in $A \smallsetminus \mathfrak{p}$ since $A \smallsetminus \mathfrak{p}$ is multiplicatively closed, so $s \in \operatorname{Ann}_A(M) \subset \mathfrak{p}$, a contradiction. Thus $M_{\mathfrak{p}} \neq 0$, so $\mathfrak{p} \in \operatorname{supp} M$.

($\supset$) Conversely, suppose $\mathfrak{p} \in \operatorname{supp} M$, that is, $M_{\mathfrak{p}} \neq 0$. Then there exists $m \in M$ such that $sm \neq 0$ for all $s \in A \smallsetminus \mathfrak{p}$, that is, $A \smallsetminus \mathfrak{p} \cap \operatorname{Ann}_A(M) = \varnothing$, hence $\operatorname{Ann}_A(M) \subset \mathfrak{p}$. □

Solution to Exercise 10.18. (a) Let A be a PID and let $I_1 \subset I_2 \subset \ldots$ be an ascending chain of ideals. Then $I = \bigcup_{n \in \mathbb{Z}_{\geqslant 1}} I_n$ is an ideal (as a union of an increasing chain of ideals), and $I = (x)$ for some $x \in I_n$ since A is a PID. By definition of I, this means $I_n = (x)$ for some $n \in \mathbb{Z}_{\geqslant 1}$. Then $I_n = I_{n+1} = \cdots$, so every ascending chain of ideals stabilizes. Thus A is Noetherian.

(b) If A is a field, then every ideal is (0) or A, so A is Artinian (since the descendng chain condition is clear—the only possible descending chains are $(0) \supset (0) \supset \cdots$ and $A \supset (0) \supset (0) \supset \cdots$, which trivially stabilize). Conversely, assume A is an Artinian integral domain. Then for any nonzero $a \in A$,

$$(a) \supset (a^2) \supset (a^3) \supset \cdots$$

stabilizes, so $(a^n) = (a^{n+1})$ for some $n \in \mathbb{Z}_{\geqslant 1}$. But this means there exists $b \in A$ such that $a^n = ba^{n+1}$, so $a^n(1 - ba) = 0$. But then $a^n = 0$ or $1 - ba = 0$. Since $a^n \neq 0$ (as A is an integral domain), $1 = ba$, that is, a is a unit. Thus A is a field.

Alternatively, one could apply Lemma 5.32 (If M is a Noetherian A-module and an A-module homomorphism $f\colon M \to M$ is injective, then f is an isomorphism), which is the Artinian analog of Exercise 10.5. □

Solution to Exercise 10.19. (a) By the structure theorem for finitely generated modules over a PID (in this case $K[x]$), conjugacy classes of $M_3(K)$ correspond to $s \in \mathbb{Z}_{\geqslant 1}$ together with monic $q_1(x) \mid q_2(x) \mid \cdots \mid q_s(x)$ such that $\sum_{i=1}^{s} \deg(q_i(x))$. Using that $m_T(x) = q_s(x)$ and $p_T(x) = q_1(x)q_2(x)\cdots q_s(x)$, restraints force three cases:

- If m_T is a cubic then $s = 1$ and $q_1 = m_T$, thus determining the conjugacy class.
- If m_T is quadratic then $s = 2$, $q_1 = p_T/q_2$, and $q_2 = m_T$, thus determining the conjugacy class.
- If $s = 3$ then $m_T = q_1 = q_2 = q_3$, thus determining the conjugacy class.

(b) Consider the following matrices corresponding to conjugacy classes in the case $\dim_K(V) = 4$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

These matrices have the same m_T and p_T (x^2 and x^4, respectively), but are not conjugate since (in the notation of part (a)) the left matrix has $s = 3$ elementary factors (x, x, x^2), while the right matrix has $s = 2$ elementary factors (x^2, x^2). □

Alphabetical Index