Solutions to Algebra: Chapter 0 by Aluffi

Akash Narayanan

Contents

Chapter I

Preliminaries: Set theory and categories

I.1 Naive Set Theory

Exercise I.1.1. Locate a discussion of Russell's paradox, and understand it.

Solution. Consider the set of all sets which do not contain themselves. Does this set contain itself? If it is an element of itself, then clearly it contains itself. Thus it fails to satisfy its defining property and does not contain itself. If it does not contain itself, then it satisfies its defining property and does contain itself. The paradox demonstrates that not all properties can define a set. □

Exercise I.1.2. Prove that if $\sim$ is an equivalence relation on a set S, then the corresponding family $\mathscr{P}_\sim$ defined in §1.5 is indeed a partition of S: that is, its elements are nonempty, disjoint, and their union is S.

Solution. Let S be a set with the equivalence relation $\sim$. Consider $\mathscr{P}_\sim = \{[a]_\sim \mid a \in S\}$. Let $[a]_\sim \in \mathscr{P}_\sim$. Since $\sim$ is reflexive, $a \sim a$ so $[a]_\sim$ is nonempty.

Now suppose $a, b \in S$ and $a \nsim b$. Suppose $x \in [a]_\sim \cap [b]_\sim$. Then, since $\sim$ is transitive, $x \sim a$ and $x \sim b$ so $a \sim b$, a contradiction. Thus, each $[a]_\sim$ is disjoint.

Finally, consider $\bigcup_{[a]_\sim \in \mathscr{P}_\sim} [a]_\sim$. If $a \in S$, then $a \in [a]_\sim$. Thus, $\bigcup [a]_\sim = S$. □

Exercise I.1.3. Given a partion $\mathscr{P}$ on a set S, show how to define a relation $\sim$ on S such that $\mathscr{P}$ is the corresponding partition.

Solution. Let $a \sim b$ if and only if $\exists X \in \mathscr{P}$ such that $a \in X$ and $b \in X$ and let $\mathscr{P}_\sim$ be the corresponding partition.

Let $X \in \mathscr{P}$. Certainly X is nonempty, so let $a \in X$ and consider $[a]_\sim \in \mathscr{P}_\sim$. We must show that $X = [a]_\sim$. Suppose $a' \in X$ (it may be the case that $a' = a$). Since $a, a' \in X$, we have $a \sim a'$, so $a' \in [a]_\sim$. Now suppose $a' \in [a]_\sim$. Then $a' \sim a$ so $a' \in X$. Thus, $X = [a]_\sim \in \mathscr{P}_\sim$, so $\mathscr{P} \subseteq \mathscr{P}_\sim$.

Now let $[a]_\sim \in \mathscr{P}_\sim$. We know that $[a]_\sim$ is nonempty, so choose $a' \in [a]_\sim$. Then $a' \sim a$ and there exists $X \in \mathscr{P}$ such that $a, a' \in X$. Hence, $[a]_\sim \subseteq X$. Furthermore, if $a, a' \in X$ then $a \sim a'$. Therefore, $\mathscr{P}_\sim \subseteq \mathscr{P}$ and we have that $\mathscr{P} = \mathscr{P}_\sim$. $\square$

Exercise I.1.4. How many different equivalence relations may be defined on the set $\{1, 2, 3\}$?

Solution. The number of equivalence relations is in bijection with the number of partitions. We can count these by hand:

$$\begin{aligned}
\mathscr{P}_0 &= \{\{1, 2, 3\}\} \\
\mathscr{P}_1 &= \{\{1\}, \{2\}, \{3\}\} \\
\mathscr{P}_2 &= \{\{1, 2\}, \{3\}\} \\
\mathscr{P}_3 &= \{\{1\}, \{2, 3\}\} \\
\mathscr{P}_4 &= \{\{1, 3\}, \{2\}\}
\end{aligned}$$

There are 5 equivalence relations defined on $\{1, 2, 3\}$. $\square$

Exercise I.1.5. Give an example of a relation that is reflexive and symmetric but not transitive. What happens if you attempt to use this relation to define a partition on the set?

Solution. Consider the set of integers $\mathbb{Z}$ and define $a \sim b$ if and only if $|a - b| \le 1$. Certainly this is reflexive since $a \sim a$ if and only if $|a - a| = 0 \le 1$, which holds for all integers. It is also symmetric because if $a \sim b$ then $|a - b| \le 1$, but $|a - b| = |b - a|$ so $|b - a| \le 1$, implying that $b \sim a$. However, it is not transitive. For example, consider $a = 0, b = 1, c = 2$. Then $a \sim b$ and $b \sim c$, but $a \nsim c$.

Attempting to define a partition using a relation which is not transitive means that partitions are not necessarily disjoint. For example, $[2]_\sim = \{1, 2, 3\}$, but $[3]_\sim = \{2, 3, 4\}$. Hence $\mathscr{P}_\sim$ is not a partition of $\mathbb{Z}$. $\square$

Exercise I.1.6. Define a relation $\sim$ on the set $\mathbb{R}$ of real numbers by setting $a \sim b \iff b - a \in \mathbb{Z}$. Prove that this is an equivalence relation, and find a 'compelling' description for $R/\sim$. Do the same for the relation $\approx$ on the plane $\mathbb{R} \times \mathbb{R}$ defined by declaring $(a_1, a_2) \approx (b_1, b_2) \iff b_1 - a_1 \in \mathbb{Z}$ and $b_2 - a_2 \in \mathbb{Z}$.

Solution. Let $a, b, c \in \mathbb{R}$. Then $a - a = 0 \in \mathbb{R}$ so $a \sim a$ and $\sim$ is reflexive. If $a \sim b$ then $b - a = n \in \mathbb{Z}$. Then $a - b = -n \in \mathbb{Z}$ so $b \sim a$ and $\sim$ is symmetric. If $a \sim b$ and $b \sim c$ then $b - a = m \in \mathbb{Z}$ and $c - b = n \in \mathbb{Z}$. Then $c - a = (c - b) + (b - a) = n + m \in \mathbb{Z}$, so $a \sim c$ and $\sim$ is transitive. Thus, $\sim$ is an equivalence relation.

$\mathbb{R}/{\sim}$ is the set of equivalence classes under the given relation. It may be interpreted as the set of integers shifted by a real number $\epsilon \in [0, 1)$. That is, for every set $X \in \mathbb{R}/{\sim}$, there is a real number $\epsilon \in [0, 1)$ such that every $x \in X$ is of the form $n + \epsilon$ for some $n \in \mathbb{Z}$.

We use a similar procedure to show that $\approx$ is an equivalence relation. Let $(a_1, a_2) \in \mathbb{R} \times \mathbb{R}$. Then we have $a_1 - a_1 = a_2 - a_2 = 0 \in \mathbb{Z}$. Thus, $(a_1, a_2) \approx (a_1, a_2)$ and $\approx$ is reflexive. Let $(b_1, b_2), (c_1, c_2) \in \mathbb{R} \times \mathbb{R}$. If we have $(a_1, a_2) \approx (b_1, b_2)$, then $b_1 - a_1 = m_1 \in \mathbb{Z}$ and $b_2 - a_2 = m_2 \in \mathbb{Z}$. Hence $a_1 - b_1 = -m_1 \in \mathbb{Z}$ and $a_2 - b_2 = -m_2 \in \mathbb{Z}$ so $(b_1, b_2) \approx (a_1, a_2)$ and $\approx$ is symmetric. Finally, suppose $(a_1, a_2) \approx (b_1, b_2)$ and $(b_1, b_2) \approx (c_1, c_2)$. Then $b_1 - a_1 = m_1 \in \mathbb{Z}$, $b_2 - a_2 = m_2 \in \mathbb{Z}$, $c_1 - b_1 = n_1 \in \mathbb{Z}$, and $c_2 - b_2 = n_2 \in \mathbb{Z}$. Therefore, $c_1 - a_1 = (c_1 - b_1) + (b_1 - a_1) = n_1 + m_1 \in \mathbb{Z}$ and $c_2 - a_2 = (c_2 - b_2) + (b_2 - a_2) = n_2 + m_2 \in \mathbb{Z}$. Thus, $(a_1, a_2) \approx (c_1, c_2)$ and $\approx$ is transitive. Then $\approx$ is an equivalence relation over $\mathbb{R} \times \mathbb{R}$.

$\mathbb{R} \times \mathbb{R}/{\approx}$ is the set of equivalence classes under the given relation. Every element is the 2-dimensional integer lattice shifted by a pair of real numbers $(\epsilon_1, \epsilon_2) \in [0, 1) \times [0, 1)$. $\square$

I.2 Functions between sets

Exercise I.2.1. How many different bijections are there between a set S with n elements and itself?

Solution. A function $f : S \to S$ is a subset $\Gamma_f \subseteq S \times S$. Since f is bijective, then for all $y \in S$, there exists a unique $x \in S$ such that $(x, y) \in \Gamma_f$. Certainly $|\Gamma_f| = n$. Since each x is unique, every element $x \in S$ must be present in the first component of exactly one element in Γ_f. Similarly, each element $y \in S$ must be present in the second component of exactly one element in Γ_f. Then each bijection is merely a permutation of S, and there are $n!$ permutations. Thus, there are $n!$ bijections from S to itself. $\square$

Exercise I.2.2. Prove statement (2) in Proposition 2.1. You may assume that given a family of disjoint subsets of a set, there is a way to choose one element in each member of the family.

Proposition 2.1. *Assume $A \neq \emptyset$, and let $f : A \to B$ be a function. Then (1) f has a left-inverse if and only if f is injective; and (2) f has a right-inverse if and only if f is surjective.*

Solution. Assume $A \neq \emptyset$ and let $f : A \to B$ be a function.

($\Longrightarrow$) Suppose there exists a function g that is a right-inverse of f. Then $f \circ g = \mathrm{id}_B$. Let $b \in B$. Then $g(b) \in A$ and $f(g(b)) = b$. Thus for all $b \in B$, there exists $a = g(b)$ such that $f(a) = b$. Hence, f is surjective.

($\Longleftarrow$) Suppose that f is surjective. We want a function $g : B \to A$ such that $f(g(b)) = b$ for all $b \in B$. Since f is surjective, for all $b \in B$, there exists an $a \in A$ such that $f(a) = b$. Construct a set $\Gamma = \{(b, a) \mid f(a) = b\} \subseteq B \times A$. Note that Γ is not necessarily unique since there may be several a such that $f(a) = b$. However, its existence is guaranteed since f is surjective. Then this set may be used to define g where $g(b) = a$ if and only if $(a, b) \in \Gamma$. Now let $b \in B$. Then there exists an $a \in A$ such that $f(a) = b$. Therefore, $(a, b) \in \Gamma$ so $g(b) = a$. We get that $f(g(b)) = f(a) = b$ so g is a right-inverse of f. $\square$

Exercise I.2.3. Prove that the inverse of a bijection is a bijection and that the composition of two bijections is bijection.

Solution. Let $f : A \to B$ be a bijection. Consider $f^{-1} : B \to A$. We have that $f^{-1} \circ f = \mathrm{id}_A$ and $f \circ f^{-1} = \mathrm{id}_B$. Then f is the left- and right-inverse of f^{-1}, so f^{-1} is also a bijection.

Let $f : A \to B$ and $g : B \to C$ be bijections and consider $g \circ f$. Suppose $a, a' \in A$ such that $(g \circ f)(a) = (g \circ f)(a')$. Since g is bijective, and in particular it is injective, we have $(g \circ f)(a) = (g \circ f)(a') \Longrightarrow f(a) = f(a')$. Similarly, f is injective so $f(a) = f(a') \Longrightarrow a = a'$. Thus, $g \circ f$ is injective. Now let $c \in C$. Since g is surjective, there exists a $b \in B$ such that $g(b) = c$. Similarly, since f is surjective, there exists an $a \in A$ such that $f(a) = b$. Then $(g \circ f)(a) = g(b) = c$ so $g \circ f$ is surjective. Hence, $g \circ f$ is bijective. $\square$

Exercise I.2.4. Prove that 'isomorphism' is an equivalence relation (on any set of sets).

Solution. Let A be a set. Then id_A is a bijection so $A \cong A$. Let B be another set such that $A \cong B$. That is, there exists a bijection $f : A \to B$. Since f is bijective, it has an inverse $f^{-1} : B \to A$, so $B \cong A$. If C is another set such that $B \cong C$, then there exists a bijection $g : B \to C$. The composition of bijections is a bijection so $g \circ f : A \to C$ is bijective. Hence $A \cong C$ and $\cong$ is an equivalence relation. $\square$

Exercise I.2.5. Formulate a notion of *epimorphism*, in the style of the notion of *monomorphism* seen in §2.6, and prove a result analogous to Proposition 2.3, for epimorphisms and surjections.

Proposition 2.3. *A function is injective if and only if it is a monomorphism.*

Solution. A function $f : A \to B$ is an epimorphism if for all sets Z and all functions $\beta, \beta' : B \to Z$ we have $\beta \circ f = \beta' \circ f \implies \beta = \beta'$. Now we show that a function is surjective if and only if it is an epimorphism.

($\Longrightarrow$) Suppose that $f : A \to B$ is surjective. Then f has a right-inverse $g : B \to A$. Let β, β' be functions from B to another set Z such that $\beta \circ f = \beta' \circ f$. Compose on the right by g and use associativity of composition:

$$\beta \circ (f \circ g) = (\beta \circ f) \circ g = (\beta' \circ f) \circ g = \beta' \circ (f \circ g)$$

Since g is a right-inverse of f, we have

$$\beta \circ \mathrm{id}_B = \beta' \circ \mathrm{id}_B$$

and thus $\beta = \beta'$ and f is an epimorphism.

($\Longleftarrow$) Now suppose that $f : A \to B$ is an epimorphism. Let $Z = \{0, 1\}$ and consider the morphisms $\beta, \beta' : B \to Z$ where $\beta(b) = 0$ for all $b \in B$ and $\beta'(b) = 0$ if $b \in \mathrm{im}(f)$ or $\beta'(b) = 1$ otherwise. By construction, $\beta \circ f = \beta' \circ f$. This implies that $\beta = \beta'$, which is only the case if every element $b \in B$ is sent to the same element of Z. β sends every element of B to 0, and β' sends every element of $\mathrm{im}(f)$ to 0, so $\mathrm{im}(f) = B$ and f is surjective. $\square$

Exercise I.2.6. With notation as in Example 2.4, explain how any function $f : A \to B$ determines a section of π_A.

Solution. We know f corresponds to a subset $\Gamma_f = \{(a, b) \mid f(a) = b\} \subseteq A \times B$. The projection $\pi_A : A \times B \to A$ is defined such that $\pi_A(a, b) = a$. Let $g : A \to A \times B$ be a function such that $g(a) = (a, f(a)) \in \Gamma_f$. Since $(\pi_A \circ g)(a) = \pi_A(a, f(a)) = a$ for all $a \in A$, g is a section of π_A which is determined by f. $\square$

Exercise I.2.7. Let $f : A \to B$ be any function. Prove that the graph Γ_f of f is isomorphic to A.

Solution. Recall that $\Gamma_f = \{(a, b) \mid b = f(a)\} \subseteq A \times B$. Let $g : A \to \Gamma_f$ be defined as $g(a) = (a, f(a))$. For all $(a, b) \in \Gamma_f$, we have $g(a) = (a, f(a)) = (a, b)$ so g is surjective. If $g(a) = g(a')$, then $(a, f(a)) = (a', f(a'))$. That is, $a = a'$ so g is injective, hence it is a bijection. Therefore, $\Gamma_f \cong A$. $\square$

Exercise I.2.8. Describe as explicitly as you can all terms in the canonical decomposition of the function $\mathbb{R} \to \mathbb{C}$ defined by $r \mapsto e^{2\pi i r}$. (This exercise matches one assigned previously. Which one?)

Solution. Let $f : \mathbb{R} \to \mathbb{C}$ be the function defined above. The first part of the decomposition is defined by letting $\sim$ be an equivalence relation on $\mathbb{R}$ such that $a \sim b \iff f(a) = f(b)$. That is, $[a]_\sim$ is the set of elements in $\mathbb{R}$ that are mapped to the same element as a in $\mathbb{C}$. Then we have a projection $\mathbb{R} \twoheadrightarrow \mathbb{R}/\sim$ which sends each element $a \in \mathbb{R}$ to its equivalence class $[a]_\sim$. Note that $f(x) = f(x+1)$. That is, the function is periodic about the integers so real numbers which differ by an integer amount belong to the same equivalence class. Then $\mathbb{R}/\sim = \{\{r + k \mid k \in \mathbb{Z}\} \mid r \in [0, 1)$ which is identical to the quotient set in Exercise 1.1.6.

The function $\tilde{f} : \mathbb{R} \to \operatorname{im}(f)$ maps each equivalence class to the complex number that f maps the representative to. Certainly if $\tilde{f}([a]_\sim) = \tilde{f}([a']_\sim)$ then $f(a) = f(a')$ and $a \sim a'$ by definition. Thus $[a]_\sim = [a']_\sim$ so $\tilde{f}$ is injective. Similarly, let $b \in \operatorname{im}(f)$. Then there is an element $a \in \mathbb{R}$ such that $f(a) = b$. Then $\tilde{f}([a]_\sim) = f(a) = b$ so $\tilde{f}$ is surjective and hence a bijection. Finally, we have the inclusion $\operatorname{im}(f) \hookrightarrow \mathbb{C}$ which embeds the image of f into its codomain. $\square$

Exercise I.2.9. Show that if $A' \cong A''$ and $B' \cong B''$, and further $A' \cap B' = \emptyset$ and $A'' \cap B'' = \emptyset$, then $A' \cup B' \cong A'' \cup B''$. Conclude that the operation $A \coprod B$ is well-defined *up to isomorphism*.

Solution. There exist bijections $f : A' \to A''$ and $g : B' \to B''$. Then we can define $h : A' \cup B' \to A'' \cup B''$ where

$$h(x) = \begin{cases} f(x) \text{ if } x \in A' \\ g(x) \text{ if } x \in B' \end{cases}$$

Let $y \in A'' \cup B''$. Since $A'' \cap B'' = \emptyset$, we have either $y \in A''$ or $y \in B''$. WLOG, suppose that $y \in A''$. Note that since f is surjective, there exists $x \in A'$ such that $f(x) = y$. Then $h(x) = f(x) = y$ so h is surjective. Suppose $x \neq x'$ for $x, x' \in A' \cup B'$. If $x, x' \in A'$ then since f is injective and $h(x) = f(x)$ for all $x \in A'$, we have $h(x) \neq h(x')$. A similar reasoning shows that if $x, x' \in B'$, then $h(x) \neq h(x')$. WLOG, suppose that $x \in A'$ and $x' \in B'$. Then $h(x) = f(x) \neq g(x') = h(x')$ since $A'' \cap B'' = \emptyset$. Thus h is surjective and hence a bijection, showing that $A' \cup B' \cong A'' \cup B''$.

The constructions of A', A'', B', B'' are equivalent to creating "copies" of sets A and B to use in the disjoint union. Thus, the disjoint union $A \coprod B$ is well-defined up to isomorphism. $\square$

Exercise I.2.10. Show that if A and B are finite sets, then $|B^A| = |B|^{|A|}$.

Solution. Recall that $|B^A|$ is the number of functions from A to B. Each functions assigns a single element of A to a single element of B. There are $|B|$ choices for each of the $|A|$ elements. This is equivalent to $|B|^{|A|}$ total choices. Thus, $|B^A| = |B|^{|A|}$. $\square$

Exercise I.2.11. In view of Exercise 2.10, it is not unreasonable to use 2^A to denote the set of functions from an arbitrary set A to a set with 2 elements (say $\{0,1\}$). Prove that there is a bijection between 2^A and the *power set* of A.

Solution. Consider $f : \mathscr{P}(A) \to 2^A$ defined as

$$f(X) = \{(a,1) \text{ if } a \in X, \text{ and } (a,0) \text{ otherwise}\}$$

Let $g \in 2^A$. Then g is a function from A to $\{0,1\}$. Let $A_1 = \{a \in A \mid g(a) = 1$. Then $A_1 \in \mathscr{P}(A)$ and $f(A_1) = g$, so f is surjective. Now suppose that $X, Y \subseteq A$ such that $f(X) = f(Y)$. That is, for all $a \in A$, $a \in X \iff (a,1) \in f(X) \iff (a,1) \in f(Y) \iff a \in Y$. Thus, $X = Y$ so f is injective and a bijection. Therefore, $2^A \cong \mathscr{P}(A)$. $\square$

I.3 Categories

Exercise I.3.1. Let C be a category. Consider a structure C^{op} with

- $\text{Obj}(\mathsf{C}^{op}) := \text{Obj}(\mathsf{C})$;
- for A, B objects of C^{op} (hence objects of C), $\text{Hom}_{\mathsf{C}^{op}}(A,B) := \text{Hom}_{\mathsf{C}}(B,A)$.

Show how to make this into a category (that is, define composition of moprhisms in C^{op} and verify the properties listed in §3.1).

Intuitively, the 'opposite' category C^{op} is simply obtained by 'reversing all the arrows' in C.

Solution. For objects $A, B, C \in \text{Obj}(\mathsf{C}^{op})$, the set of morphisms from A to B, $\text{Hom}_{\mathsf{C}^{op}}(A,B)$, is defined as $\text{Hom}_{\mathsf{C}}(B,A)$. For morphisms $f \in \text{Hom}_{\mathsf{C}^{op}}(A,B)$ and $g \in \text{Hom}_{\mathsf{C}^{op}}(B,C)$, define composition as follows:

$$\circ_{\mathsf{C}^{op}} : \text{Hom}_{\mathsf{C}^{op}}(A,B) \times \text{Hom}_{\mathsf{C}^{op}}(B,C) \to \text{Hom}_{\mathsf{C}^{op}}(A,C)$$

such that

$$\circ_{\mathsf{C}^{op}}(g,f) = \circ_{\mathsf{C}}(f,g)$$

Then if $f \in \text{Hom}_{\mathsf{C}^{op}}(A,B), g \in \text{Hom}_{\mathsf{C}^{op}}(B,C), h \in \text{Hom}_{\mathsf{C}^{op}}(C,D)$, then

$$(h \circ_{\mathsf{C}^{op}} g) \circ_{\mathsf{C}^{op}} f = f \circ_{\mathsf{C}} (g \circ_{\mathsf{C}} h) = (f \circ_{\mathsf{C}} g) \circ_{\mathsf{C}} h = h \circ_{\mathsf{C}^{op}} (g \circ_{\mathsf{C}^{op}} f)$$

so composition is associative. Furthermore, define the identity morphism $1_{A_{\mathsf{C}^{op}}} = 1_{A_{\mathsf{C}}}$. Then for all $f \in \text{Hom}_{\mathsf{C}^{op}}(A,B)$ we have

$$f \circ_{\mathsf{C}^{op}} 1_{A_{\mathsf{C}^{op}}} = 1_{A_{\mathsf{C}}} \circ_{\mathsf{C}} f = f$$
$$1_{B_{\mathsf{C}^{op}}} \circ_{\mathsf{C}^{op}} f = f \circ_{\mathsf{C}} 1_{B_{\mathsf{C}}} = f$$

so identities preserve morphisms. Finally, let $A, B, C, D \in \text{Obj}(\mathsf{C}^{op})$ where $A \neq C$ and $B \neq D$. Consider the sets $\text{Hom}_{\mathsf{C}^{op}}(A,B)$ and $\text{Hom}_{\mathsf{C}^{op}}(C,D)$. These are equal to the sets $\text{Hom}_{\mathsf{C}}(B,A)$ and $\text{Hom}_{\mathsf{C}}(D,C)$ respectively, which are disjoint since C is a category. Thus, C^{op} forms a category. $\square$

Exercise I.3.2. If A is a finite set, how large is $\text{End}_{\mathsf{Set}}(A)$?

Solution. Recall that $\text{End}_{\mathsf{Set}}(A)$ is the set of functions from A to A. By Exercise 2.10, we have $|B^A| = |B|^{|A|}$. Thus, $|\text{End}_{\mathsf{Set}}(A)| = |A|^{|A|}$. □

Exercise I.3.3. Formulate precisely what it means to say that 1_a is an identity with respect to composition in Example 3.3, and prove this assertion.

Solution. Let S be a set and $\sim$ be a reflexive and transitive relation on S. Consider a category C where

- $\text{Obj}(\mathsf{C})$ are the elements in S
- If a, b are objects, then let $\text{Hom}(a, b) = (a, b) \in S \times S$ if $a \sim b$ and let $\text{Hom}(a, b) = \emptyset$ otherwise.

This forms a category and composition is defined as follows. Let a, b, c be objects and $f \in \text{Hom}(a, b)$, $g \in \text{Hom}(b, c)$. Then $g \circ f = (a, c) \in \text{Hom}(a, c)$ by the transitivity of $\sim$.

Now we verify that the identity preserves morphisms in this category. Let $a, b \in S$ and $f \in \text{Hom}(a, b)$. A morphism $1_a = (a, a) \in \text{End}(a)$ is an identity with respect to composition if

$$f \circ 1_a = f$$

Indeed, we have $f = (a, b)$ and $1_a = (a, a)$. Then by definition we have

$$f \circ 1_a = (a, b)(a, a) = (a, b) = f$$

Thus 1_a is an identity with respect to composition as required. □

Exercise I.3.4. Can we define a category in the style of Example 3.3 using the relation $<$ on the set $\mathbb{Z}$.

Solution. No, since the relation $<$ is not reflexive. That is, $a < a$ does not hold for any $a \in \mathbb{Z}$. There is no reasonable way to define an identity morphism. □

Exercise I.3.5. Explain in what sense Example 3.4 is an instance of the categories considered in Example 3.3.

Solution. Let S be a set and consider the category $\hat{S}$ where

- $\text{Obj}(\hat{S}) = \mathscr{P}(S)$
- For $A, B \in \text{Obj}(\hat{S})$, let $\text{Hom}_{\hat{S}}(A, B)$ be the pair (A, B) if $A \subseteq B$, and let $\text{Hom}_{\hat{S}}(A, B) = \emptyset$ otherwise.

Composition is obtained by using the transitivity of inclusion.

This is equivalent to the category in Example 3.3 by considering the relation $\sim$ defined on $\mathscr{P}(S)$ where $A \sim B$ if and only if $A \subseteq B$. Indeed, this relation is both reflexive and transitive so we may construct the category considered in Example 3.3, and the two are equivalent. $\square$

Exercise I.3.6. (Assuming some familiarity with linear algebra.) Define a category V by taking $\mathrm{Obj}(\mathsf{V}) = \mathbb{N}$ and letting $\mathrm{Hom}_{\mathsf{V}}(n, m)$ = the set of $m \times n$ matrices with real entries, for all $n, m \in \mathbb{N}$. (We will leave the reader the task of making sense of a matrix with 0 rows or columns.) Use products of matrices to define composition. Does this category 'feel' familiar?

Solution. First of all, the identity morphism for the object n is the set of $n \times n$ matrices. Let $l, m, n \in \mathbb{N}$ and

$$f \in \mathrm{Hom}(l, m), \quad g \in \mathrm{Hom}(m, n)$$

Then fg is an $l \times n$ matrix and is in $\mathrm{Hom}(l, n)$. Furthermore, matrix multiplication is associative.

This category is another instance of Example 3.3 where the set is $\mathbb{N}$ and the relation $\sim$ is defined as follows: $m \sim n$ if and only if $\mathrm{Hom}(m, n)$ is nonempty. Certainly this relation is both reflexive and transitive so it is an instance of Example 3.3. $\square$

Exercise I.3.7. Define carefully objects and morphisms in Example 3.7, and draw the diagram corresponding to composition.

Solution. Given a category C and an object $A \in \mathrm{Obj}(\mathsf{C})$, consider the category C^A where

- $\mathrm{Obj}(\mathsf{C}^A)$ = all morphisms from A to any object of C;
- Let f_1, f_2 be objects of C^A, or two arrows

$$\begin{tikzcd} A \arrow[d, "f_1"'] & A \arrow[d, "f_2"] \\ Z_1 & Z_2 \end{tikzcd}$$

in C. Morphisms $f_1 \to f_2$ are *commutative diagrams*

$$\begin{tikzcd} & A \arrow[dl, "f_1"'] \arrow[dr, "f_2"] & \\ Z_1 \arrow[rr, "\sigma"'] & & Z_2 \end{tikzcd}$$

in the category C.

That is, morphisms $\sigma \in \mathrm{Hom}_{\mathsf{C}^A}(f_1, f_2)$ are precisely the morphisms $\sigma : Z_1 \to Z_2$ in C such that $f_2 = \sigma \circ f_1$.

If $\sigma \in \mathrm{Hom}(f, g)$ and $\tau \in \mathrm{Hom}(g, h)$, then $\tau \circ \sigma \in \mathrm{Hom}(f, h)$ is the morphism in C making the following diagram commute:

$$\begin{tikzcd}
& A \arrow[dl, "f"'] \arrow[d, "g"] \arrow[dr, "h"] & \\
Z_1 \arrow[r, "\sigma"'] \arrow[rr, bend right, "\tau\circ\sigma"'] & Z_2 \arrow[r, "\tau"'] & Z_3
\end{tikzcd}$$

□

Exercise I.3.8. A *subcategory* C' of a category C consists of a collection of objects of C, with morphisms $\mathrm{Hom}_{\mathsf{C}'}(A, B) \subseteq \mathrm{Hom}_{\mathsf{C}}(A, B)$ for all objects A, B in $\mathrm{Obj}(\mathsf{C}')$, such that identities and compositions in C make C' into a category. A subcategory C' is *full* if $\mathrm{Hom}_{\mathsf{C}'}(A, B) = \mathrm{Hom}_{\mathsf{C}}(A, B)$ for all A, B in $\mathrm{Obj}(\mathsf{C}')$. Construct a category of *infinite sets* and explain how it may be viewed as a full subcategory of Set.

Solution. Let Set^∞ be a category whose objects are infinite sets and whose morphisms are set functions between them. That is, for infinite sets A, B we let $\mathrm{Hom}_{\mathsf{Set}^\infty}(A, B)$ be the set of set functions from A to B. Certainly this is equivalent to $\mathrm{Hom}_{\mathsf{Set}}(A, B)$ so the subcategory is full. □

Exercise I.3.9. An alternative to the notion of *multiset* introduced in §2.2 is obtained by considering sets endowed with equivalence relations; equivalent elements are taken to be multiple instances of elements 'of the same kind'. Define a notion of morphism between such enhanced sets, obtaining a category MSet containing (a 'copy' of) Set as a full subcategory. (There may be more than one reasonable way to do this! This is intentionally an open-ended exercise.) Which objects in MSet determine ordinary multisets as defined in §2.2 and how? Spell out what a morphism of multisets would be from this point of view. (There are several natural notions of morphisms of multisets. Try to define morphisms in MSet so that the notion you obtain for ordinary multisets captures your intuitive understanding of these objects.)

Solution. Consider the category MSet where

- $\mathrm{Obj}(\mathsf{MSet})$ = sets endowed with equivalence relations;

- If $A, B \in \text{Obj}(\mathsf{MSet})$ then $\text{Hom}_{\mathsf{MSet}}(A, B)$ is the collection of functions from A to B which preserve equivalence classes. That is, if $\sim$ is an equivalence relation on A and $\approx$ is an equivalence relation on B then for $a, b \in A$ and $f \in \text{Hom}_{\mathsf{MSet}}(A, B)$ we have $a \sim b \implies f(a) \approx f(b)$.

Composition is naturally defined as it is Set. For objects A, B, C, let $f \in \text{Hom}_{\mathsf{MSet}}(A, B)$ and $g \in \text{Hom}_{\mathsf{MSet}}(B, C)$. If $a, b \in A$ and $a \sim_A b$ then, since f is a morphism, $f(a) \sim_B f(b)$. Furthermore, g is a morphism so $g(f(a)) \sim_C g(f(b))$ so $g \circ f \in \text{Hom}_{\mathsf{MSet}}(A, C)$. The identity morphism has a natural definition where $1_S : S \to S$ is the identity function Set. It obviously preserves equivalence classes. Associativity is similarly inherited from Set.

In §2.2, multisets are defined as a set A along with a function $m : A \to \mathbb{N}^*$ which takes each element of A to the number denoting its multiplicity. We define the equivalence relation $\sim$ on A which partitions A into its distinct elements, or those elements which are not equal. In other words, $m(a) \neq m(b) \implies a \nsim b$. Morphisms between these objects as defined above can intuitively be expressed as the functions which allow elements to be renamed and naturally mapped to other multisets which preserve multiplicity. □

Exercise I.3.10. Since the objects of a category C are not (necessarily) sets, it is not clear how to make sense of a notion of 'subobject' in general. In some situations it *does* make sense to talk about subobjects, and the subobjects of any given object A in C are in one-to-one correspondence with the morphisms $A \to \Omega$ for a fixed special object Ω of C, called a *subobject classifier*. Show that Set has a subobject classifier.

Solution. Consider the set $\Omega = \{0, 1\}$. Let A be any set. The subsets $X \subseteq A$ induce morphisms $f : A \to \Omega$ where

$$f(x) = \begin{cases} 1 \text{ if } x \in X \\ 0 \text{ if } x \notin X \end{cases}$$

Certainly these morphisms are in bijection with subsets of A. Thus $\{0, 1\}$ is a subobject classifier of Set, though any set with 2 elements works. □

Exercise I.3.11. Draw the relevant diagrams and define composition and identities for the category $\mathsf{C}^{A,B}$ mentioned in Example 3.9. Do the same for the category $\mathsf{C}^{\alpha,\beta}$ mentioned in Example 3.10.

Solution. Consider the category $\mathsf{C}^{A,B}$ where

- $\mathrm{Obj}(\mathsf{C}^{A,B})$ = diagrams

$$\begin{tikzcd}
A \arrow[dr, "f"] & \\
& Z \\
B \arrow[ur, "g"'] &
\end{tikzcd}$$

  in C

- Morphisms between objects (Z_1, f_1, g_1) and (Z_2, f_2, g_2) are commutative diagrams

$$\begin{tikzcd}
A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_2"] & & \\
& Z_1 \arrow[r, "\sigma"] & Z_2 \\
B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_2"'] & &
\end{tikzcd}$$

  That is, we have a morphism $\sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$ such that $f_2 = \sigma \circ f_1$ and $g_2 = \sigma \circ g_1$.

Composition has a natural definition. Given a third object (Z_3, f_3, g_3) with a morphism $\tau : Z_2 \to Z_3$ we define $\tau \circ \sigma : Z_1 \to Z_3$ such that $f_3 = \tau \circ \sigma(f_1)$ and $g_3 = \tau \circ \sigma(g_1)$. Given an object (Z, f, g), the identity morphism $1_Z \in \mathrm{End}_{\mathsf{C}}(Z)$ serves as an identity in $\mathsf{C}^{A,B}$ as well. Specifically, we have $f = 1_Z \circ f$ and $g = 1_Z \circ g$.

Now consider the category $\mathsf{C}^{\alpha,\beta}$ where $\alpha : C \to A$ and $\beta : C \to B$. Then we have

- $\mathrm{Obj}(\mathsf{C}^{\alpha,\beta})$ = commutative diagrams

$$\begin{tikzcd}
& A \arrow[dr, "f"] & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z \\
& B \arrow[ur, "g"'] &
\end{tikzcd}$$

  where Z is an object in C

- Morphisms between objects (Z_1, f_1, g_1) and (Z_2, f_2, g_2) are commutative diagrams

$$\begin{tikzcd}
 & A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_2"] & & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z_1 \arrow[r, "\sigma"] & Z_2 \\
 & B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_2"'] & &
\end{tikzcd}$$

That is, we have a morphism $\sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$ such that the diagram commutes.

Composition again has a natural definition. Given a third object (Z_3, f_3, g_3) and a morphism $\tau : Z_2 \to Z_3$, we can define a morphism $\tau \circ \sigma : Z_1 \to Z_3$ such that the corresponding diagram commutes. Finally, given an object (Z, f, g) we inherit the identity morphism 1_Z from C. Certainly the corresponding diagram commutes. $\square$

I.4 Morphisms

Exercise I.4.1. Composition is defined for *two* morphisms. If more than two morphisms are given, e.g.,

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \xrightarrow{i} E$$

then one may compose them in several ways, for example:

$$(ih)(gf), \quad (i(hg))f, \quad i((hg)f), \quad \text{etc.}$$

so that at every step one is only composing two morphisms. Prove that the result of any such nested composition is independent of the placement of the parentheses. (Hint: Use induction on n to show that any such choice for $f_n f_{n-1} \cdots f_1$ equals

$$((\cdots((f_n f_{n-1}) f_{n-2}) \cdots) f_1).$$

Carefully working out the case $n = 5$ is helpful.)

Solution. For $n = 3$, we have $(fg)h = f(gh)$ by the associativity of composition in a category. Suppose $n \geq 4$ and that for $n-1$ morphisms we have shown that composition is independent of the placement of the parentheses. Let $f_1, \ldots, f_n$ be morphisms in a category:

$$Z_1 \xrightarrow{f_1} Z_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} Z_n \xrightarrow{f_n} Z_{n+1}$$

Suppose that a parenthesization of $f_n, f_{n-1}, \ldots, f_1$ is f and that $f = hg$ where h is some parenthesization of $f_n, f_{n-1}, \ldots, f_{i+1}$, and g is some parenthesization of $f_i, f_{i-1}, \ldots, f_1$, where $1 \leq i \leq n$. Applying the inductive to h and g, we see that

$$h = ((\cdots((f_n f_{n-1})f_{n-2})\cdots)f_{i+1})$$
$$g = (f_i(f_{i-1}(\cdots(f_2 f_1)\cdots)) = f_i g'$$

hence $f = hg = h(f_i g') = (hf_i)g'$. Effectively, we remove morphisms f_i from the left side of g' and attach them to the right side of h to obtain the form

$$f = ((\cdots((f_n f_{n-1})f_{n-2})\cdots)f_1)$$

□

Exercise I.4.2. In Example 3.3 we have seen how to construct a category from a set endowed with a relation, provided this latter is reflexive and transitive. For what types of relations is the corresponding category a groupoid (cf. Example 4.6)?

Solution. Recall that a groupoid is a category in which every morphism is an isomorphism and hence has a two-sided inverse. The corresponding category is a groupoid when the relation is also symmetric and hence an equivalence relation. Indeed, if $(x, y) \in \mathrm{Hom}(x, y)$ then $x \sim y$. If $\sim$ is reflexive then this implies that $y \sim x$ so $(y, x) \in \mathrm{Hom}(y, x)$. Then $(x, y)(y, x) = (x, x)$ and $(y, x)(x, y) = (y, y)$, both of which are the identity morphisms of their respective objects. Thus, (x, y) is an isomorphism and the category is a groupoid. □

Exercise I.4.3. Let A, B be objects of a category C, and let $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ be a morphism.

- Prove that if f has a right-inverse, then f is an epimorphism.
- Show that the converse does not hold, by giving an explicity example of a category and an epimorphism without a right-inverse.

Solution. Suppose f has a right-inverse. That is, there exists a morphism $g \in \mathrm{Hom}_{\mathsf{C}}(B, A)$ such that $f \circ g = 1_B$. Then if we consider two morphisms $\beta, \beta' \in \mathrm{Hom}_{\mathsf{C}}(B, Z)$ such that $\beta \circ f = \beta' \circ f$ we have

$$\begin{aligned}
&(\beta \circ f) \circ g = (\beta' \circ f) \circ g \\
\Longrightarrow &\beta \circ (f \circ g) = \beta' \circ (f \circ g) \\
\Longrightarrow &\beta \circ 1_B = \beta' \circ 1_B \\
\Longrightarrow &\beta = \beta'
\end{aligned}$$

Thus, f is an epimorphism.

However, consider the category C where

- $\mathrm{Obj}(\mathsf{C}) = \mathbb{Z}$
- For objects $a, b \in \mathbb{Z}$ we have $\mathrm{Hom}_{\mathsf{C}}(a,b) = \{(a,b)\}$ if $a \leq b$ and $\emptyset$ otherwise.

The reflexivity and transitivity of $\leq$ makes this a category. Given morphisms $f \in \mathrm{Hom}_{\mathsf{C}}(a,b)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(b,c)$ we define composition as $g \circ f = (b,c) \circ (a,b) = (a,c) \in \mathrm{Hom}_{\mathsf{C}}(a,c)$. Consider two objects $a, b \in \mathbb{Z}$ such that $a < b$ and let $f : a \to b = (a,b)$ be the morphism from a to b. Consider two morphisms $\beta, \beta' \in \mathrm{Hom}_{\mathsf{C}}(b,c)$ such that $\beta \circ f = \beta' \circ f$. Then we have $\beta = \beta'$ since each Hom set has at most one morphism. Thus f is an epimorphism. However, it does not have a right-inverse. Indeed, suppose $\mathrm{Hom}_{\mathsf{C}}(b,a)$ is nonempty. Then it can only contain (b,a) which would imply that $b \leq a$, a contradiction since we assumed $a < b$. Thus, we have a category where epimorphisms do not necessarily have right-inverses. $\square$

Exercise I.4.4. Prove that the composition of two monomorphims is a monomorphism. Deduce that one can define a subcategory $\mathsf{C}_{\mathrm{mono}}$ of a category C by taking the same objects as in C and defining $\mathrm{Hom}_{\mathsf{C}_{\mathrm{mono}}}(A,B)$ to be subset of $\mathrm{Hom}_{\mathsf{C}}(A,B)$ consisting of monomorphisms, for all objects A, B. (Cf. Exercise 3.8; of course, in general $\mathsf{C}_{\mathrm{mono}}$ is not full in C.) Do the same for epimorphisms. Can you define a subcategory $\mathsf{C}_{\mathrm{nonmono}}$ of C by restricting to morphisms that are *not* monomorphisms?

Solution. Suppose that $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(B,C)$ are two monomorphisms. Let $\alpha, \alpha' \in \mathrm{Hom}_{\mathsf{C}}(Z,A)$ be two morphisms such that $(g \circ f) \circ \alpha = (g \circ f) \circ \alpha'$. Then we have

$$\begin{aligned}
&(g \circ f) \circ \alpha = (g \circ f) \circ \alpha' && \\
\Longrightarrow\, & g \circ (f \circ \alpha) = g \circ (f \circ \alpha') && \text{by the associativity of composition} \\
\Longrightarrow\, & f \circ \alpha = f \circ \alpha' && \text{since } g \text{ is a monomorphism} \\
\Longrightarrow\, & \alpha = \alpha' && \text{since } f \text{ is a monomorphism}
\end{aligned}$$

Hence, $g \circ f$ is a monomorphism. Therefore, the subcategory $\mathsf{C}_{\mathrm{mono}}$ is closed with respect to composition.

We use a similar proof to show that the composition of two epimorphisms is an epimorphism. Suppose that $f \in \mathrm{Hom}_{\mathsf{C}}(A,B)$ and $g \in \mathrm{Hom}_{\mathsf{C}}(B,C)$ are epimorphisms. Let $\beta, \beta' \in \mathrm{Hom}_{\mathsf{C}}(C,Z)$ be two morphisms such that $\beta \circ (g \circ f) = \beta' \circ (g \circ f)$. Then we have

$$\begin{aligned}
&(\beta \circ g) \circ f = (\beta' \circ g) \circ f && \text{by the associativity of composition} \\
\Longrightarrow\, & \beta \circ g = \beta' \circ g && \text{since } f \text{ is an epimorphism} \\
\Longrightarrow\, & \beta = \beta' && \text{since } g \text{ is an epimorphism}
\end{aligned}$$

Thus, $g \circ f$ is an epimorphism so we can define a similar subcategory $\mathsf{C}_{\mathrm{epi}}$ which is closed with respect to compositon.

We can also define a category $\mathsf{C}_{\text{nonmono}}$ whose morphisms are restricted to those of C which are not monomorphisms. Indeed, suppose $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ is not a monomorphism. That is, there exist morphisms $\alpha, \alpha' \in \mathrm{Hom}_{\mathsf{C}}(Z, A)$ such that $f \circ \alpha = f \circ \alpha'$ but $\alpha \neq \alpha'$. Let $g \in \mathrm{Hom}_{\mathsf{C}}(B, C)$ be a non-monomorphism. Then we have $(g \circ f) \circ \alpha = (g \circ f) \circ \alpha'$ but $\alpha \neq \alpha'$. Thus, $(g \circ f)$ is not a monomorphism so the category $\mathsf{C}_{\text{nonmono}}$ is closed under composition. Interestingly, this only relies on the fact that f is not a monomorphism. □

Exercise I.4.5. Give a concrete description of monomorphims and epimorphisms in the category MSet you constructed in Exercise 3.9. (Your answer will depend on the notion of morphism you defined in that exercise!)

Solution. Recall that we defined multisets to be sets equipped with equivalence relations. A morphism between two multisets is a set function which preserves the equivalence relation. The notions of monomorphism and epimorphism are naturally inherited from Set.

- A morphism $f \in \mathrm{Hom}_{\mathsf{MSet}}(A, B)$ is a monomorphism if for all $a_1, a_2 \in A$ we have $f(a_1) \sim_B f(a_2) \implies a_1 \sim_A a_2$. We call these morphisms *injective*.
- A morphism $f \in \mathrm{Hom}_{\mathsf{MSet}}(A, B)$ is an epimorphism if for all $b \in B$ there exists an $a \in A$ such that $f(a) = b$. We call these morphisms *surjective*.

We will prove that these definitions satisfy the category theoretical definitions of monomorphisms and epimorphisms. We start by proving an analogue of Proposition 2.1 in MSet.

Lemma. *Assume $A \neq \emptyset$ and let $f : A \to B$ be a morphism of multisets. Then*

1. *f has a left-inverse if and only if it is injective.*
2. *f has a right-inverse if and only if it is surjective.*

Proof. First we prove (1). If f has a left-inverse, then there exists a morphism $g \in \mathrm{Hom}_{\mathsf{MSet}}(B, A)$ such that $g \circ f = 1_A$. Let $a_1 \nsim_A a_2$ be elements in A not eqivalent under the relation. Then

$$g \circ f(a_1) = 1_A(a_1) = a_1 \nsim_A a_2 = 1_A(a_2) = g \circ f(a_2)$$

That is, $a_1 \nsim_A a_2 \implies f(a_1) \nsim_B f(a_2)$ which is the contrapositive of the definition for an injective morphism. Thus, if f has a left-inverse it must be injective.

Now suppose $f : A \to B$ is injective. We will construct a left-inverse $g : B \to A$. Choose one fixed element $s \in A$. Now set

$$g(b) = \begin{cases} a \text{ if } b = f(a) \text{ for some } a \in A, \\ s \text{ if } b \notin \mathrm{im} f \end{cases}$$

This definition guarantees that every b that is in the image of f maps to a unique element since f is injective. We can verify that g is a left-inverse of f. If $a \in A$, then $g \circ f(a) = a = 1_A(a)$.

A highly similar proof follows for (2). If $f : A \to B$ has a right-inverse, then there exists a morphism $g : B \to A$ such that $f \circ g = 1_B$. Let $b \in B$. Then $g(b) \in A$ and $f \circ g(b) = b$ for all such b. Thus f is surjective.

For the reverse direction, suppose that $f : A \to B$ is surjective. We will construct a right-inverse $g : B \to A$. Let $S = \{(a, b) \mid f(a) = b\}$. Certainly S contains elements for each $b \in B$ since f is surjective. Then define $g : B \to A$, $g(b) = a$ where a is the least element such that $(a, b) \in S$. This definition guarantees that every element of b is mapped to only one element since there may be several a which are mapped to b. We can verify that g is a right-inverse of f. Let $b \in B$. Then $f \circ g(b) = b = 1_B(b)$. □

With this lemma, we show that our definition of injective and surjective morphisms is precisely equivalent to monomorphisms and epimorphisms in the category MSet.

First suppose that $f : A \to B$ is injective. Then it has a left-inverse $g : B \to A$. Let $\alpha, \alpha' \in \mathrm{Hom}_{\mathsf{MSet}}(Z, A)$ be morphisms such that $f \circ \alpha = f \circ \alpha'$. Then we find

$$\begin{aligned} &(g \circ f) \circ \alpha = (g \circ f) \circ \alpha' && \text{by associativity of composition} \\ \Longrightarrow &1_A \circ \alpha = 1_A \circ \alpha' && \text{since } g \text{ is a left-inverse of } f \\ \Longrightarrow &\alpha = \alpha' \end{aligned}$$

Thus, f is a monomorphism in the category theoretical sense.

Now suppose that $f : A \to B$ is a monomorphism. We will show it is injective. Consider the set $Z = \{p\}$ and let $\alpha, \alpha' \in \mathrm{Hom}_{\mathsf{MSet}}(Z, A)$ be morphisms such that $f \circ \alpha = f \circ \alpha'$. Since f is a monomorphism, this forces $\alpha = \alpha'$. In turn, this means $\alpha(p) \sim_A \alpha'(p)$. Letting $a_1 = \alpha(p)$ and $a_2 = \alpha'(p)$, we have

$$f(a_1) \sim_A f(a_2) \Longrightarrow a_1 \sim_A a_2$$

Thus, f is injective. A nearly identical proof follows for epimorphisms and surjective morphisms. □

I.5 Universal Properties

Exercise I.5.1. Prove that a final object in a category C is initial in the opposite category C^{op}.

Solution. Let A be a final object in C. That is, for every object Z of C, there exists exactly one morphism $f \in \mathrm{Hom}_{\mathsf{C}}(Z, A)$. Recall that the opposite category C^{op} is formed by 'reversing' all arrows. More formally, we set $\mathrm{Hom}_{\mathsf{C}^{op}}(Z, B) = \mathrm{Hom}_{\mathsf{C}}(B, Z)$. In particular, for every object Z of C^{op}, there exists exactly one morphism $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, Z)$. Thus, A is initial in C^{op}. □

Exercise I.5.2. Prove that $\emptyset$ is the *unique* initial object in Set.

Solution. Note that the empty set $\emptyset$ is initial in Set with the only morphism to other sets being the empty mapping. Now let I be any other initial object in Set. Then $I \cong \emptyset$. Recall that isomorphic sets are those which have the same order (so that a bijection exists between them). Thus, $|I| = |\emptyset| = 0$ and I is necessarily the empty set $\emptyset$ since it is the only set with no elements. □

Exercise I.5.3. Prove that final objects are unique up to isomorphism.

Solution. First note that if F is a final object in a category C, then there is a unique morphism $F \to F$, namely the identity 1_F. Now assume F_1 and F_2 are both final in C. Since F_2 is final, there is a unique morphism $f : F_1 \to F_2$. We will show that f is an isomorphism. Since F_1 is final, there is a unique morphism $g : F_2 \to F_1$. Consider the composition $g \circ f : F_1 \to F_1$. As noted earlier, this is necessarily the identity morphism 1_{F_1}. Similarly, $f \circ g : F_2 \to F_2$ is necessarily the identity morphism 1_{F_2}. Thus, f is an isomorphism and $F_1 \cong F_2$. □

Exercise I.5.4. What are initial and final objects in the category of 'pointed sets'? Are they unique?

Solution. Recall that the category of pointed sets Set^* is defined as follows:

- $\mathrm{Obj}(\mathsf{Set}^*)$ = morphisms $f : \{*\} \to S$ in Set where S is any set. Note that objects may be denoted as pairs (S, s) where S is the set the morphism maps to and s is the element that f sends $*$ to.
- Given two objects (S, s) and (T, t), a morphism $f : (S, s) \to (T, t)$ corresponds to a set-function $\sigma : S \to T$ such that $\sigma(s) = t$.

Then the pointed singleton sets $(\{s\}, s)$ are the initial and final objects of Set^*. Indeed, let (T, t) be any object in Set^*. Then there is only one morphism $\sigma : S \to T$ such that $\sigma(s) = t$. Similarly, there is only one morphism $\sigma' : T \to S$ such that $\sigma(t) = s$. Thus, pointed singleton sets are both initial and final. They are also clearly not unique as both $(\{a\}, a)$ and $(\{b\}, b)$ where $a \neq b$ are distinct pointed singleton sets. □

Exercise I.5.5. What are the final objects in the category considered in §5.3?

Solution. The category considered in §5.3 is defined as follows: Let $\sim$ be an equivalence relation defined on a set A. Consider the category C_A where

- $\mathrm{Obj}(\mathsf{C}_A)$ = morphisms $\varphi : A \to Z$ where Z is an arbitrary set such that $a \sim a' \Longrightarrow \varphi(a) = \varphi(a')$. Objects are frequently denoted (φ, Z).

- Morphisms $(\varphi_1, Z_1) \to (\varphi_2, Z_2)$ are commutative diagrams

$$\begin{tikzcd} Z_1 \arrow[rr, "\sigma"] & & Z_2 \\ & A \arrow[ul, "\varphi_1"] \arrow[ur, "\varphi_2"'] & \end{tikzcd}$$

Then the objects $(\varphi^*, \{*\})$ are final in this category, where φ^* is the morphism mapping every element of A to $*$. To verify, let (φ, Z) be an object. Then there exists a unique morphism $\sigma : Z \to \{*\}$, namely the one mapping every element of Z to $*$. Certainly this morphism makes the diagram commute, and since it exists for all objects, $\varphi^*, \{*\}$ is final. $\square$

Exercise I.5.6. Consider the category corresponding to endowing (as in Example 3.3) the set $\mathbb{Z}^+$ of positive integers with the *divisibility* relation. Thus there is exactly one morphism $d \to m$ in this category if and only if d divides m without remainder; there is no morphism between d and m otherwise. Show that this category has products and coproducts. What are their conventional names?

Solution. Given two positive integers m, n, their categorical product $m \times n$ is the positive integer such that, given any positive integer z, the diagram

$$\begin{tikzcd} & & m \\ z \arrow[urr, bend left, "f_m"] \arrow[r, "\sigma"'] \arrow[drr, bend right, "f_n"'] & m \times n \arrow[ur, "\pi_m"'] \arrow[dr, "\pi_n"] & \\ & & n \end{tikzcd}$$

commutes.

Note that the existence of projections π_m, π_n implies $m \times n$ divides m and $m \times n$ divides n. Thus, we have $m \times n$ divides $\gcd(m, n)$. Furthermore, consider $z = \gcd(m, n)$. Certainly there exist morphisms $f_m : z \to m$ and $f_n : z \to n$. Then by the definition of categorical products, there exists a unique morphism $\sigma : z \to m \times n$. That is, we have $\gcd(m, n)$ divides $m \times n$. Combined with the earlier observation, we find $m \times n = \gcd(m, n)$.

Now let us consider the categorical coproduct $m \coprod n$. This is a positive integer such that, given any positive integer z, the diagram

$$\begin{tikzcd} m \arrow[dr, "i_m"] \arrow[drr, bend left, "f_m"] & & \\ & m \coprod n \arrow[r, "\sigma"] & z \\ n \arrow[ur, "i_n"'] \arrow[urr, bend right, "f_n"'] & & \end{tikzcd}$$

commutes.

The existence of the inclusion morphisms imply that both m and n divide $m \coprod n$, so $\operatorname{lcm}(m, n)$ divides $m \coprod n$. Furthermore, take z to be $\operatorname{lcm}(m, n)$. Then there certainly exist morphisms $f_m : m \to z$ and $f_n : n \to z$. By the definition of the categorical coproduct, there exists a unique morphism $\sigma : m \coprod n \to z$, so $m \coprod n$ divides $\operatorname{lcm}(m, n)$. Thus, we have $m \coprod n = \operatorname{lcm}(m, n)$. □

Exercise I.5.7. Redo Exercise 2.9, this time using Proposition 5.4.

Solution. Exercise 2.9 asks that we show if $A' \cong A''$ and $B' \cong B''$, and further $A' \cap B' = A'' \cap B'' = \emptyset$, then $A' \cup B' \cong A'' \cup B''$. We can conclude that $A \coprod B$ is well-defined up to isomorphism.

First consider $i_{A'} : A' \to A' \cup B', i_{A'}(a) = a$ for all $a \in A'$. Define a similar function $i_{B'}$. If Z is a set with morphisms $f_{A'} : A' \to Z$ and $f_{B'} : B' \to Z$, we have a unique morphism $\sigma : A' \coprod B' = A' \cup B' \to Z$ where

$$\sigma(x) = \begin{cases} f_{A'}(x) \text{ if } x \in A' \\ f_{B'}(x) \text{ if } x \in B' \end{cases}$$

This shows that the disjoint union is a coproduct.

We define entirely analagous morphisms for A'' and B''. Then we have a second coproduct $A'' \coprod B'' = A'' \cup B''$.

Proposition 5.4 states that in any category C, two initial objects I_1 and I_2 are isomorphic. Note that the coproducts $A' \coprod B'$ and $A'' \coprod B''$ we have defined are initial in the category $\mathsf{Set}_{A,B}$. Thus, they are isomorphic. □

Exercise I.5.8. Show that in every category C the products $A \times B$ and $B \times A$ are isomorphic, if they exist. (Hint: Observe that they both satisfy the universal property for the product of A and B; then use Proposition 5.4.)

Solution. Let $A \times B$ and $B \times A$ be products in a category C. Certainly $A \times B$ satisfies the universal property for products. That is, given an object Z and morphisms $f_A : Z \to A$ and $f_B : Z \to B$, we can construct a unique morphism $\sigma : Z \to A \times B$.

Now consider the morphism $\tau : A \times B \to B \times A, \tau(a, b) = (b, a)$. Certainly this morphism is an isomorphism since it has an inverse $\tau^{-1}(b, a) = (a, b)$. Then for any object Z and morphisms f_A, f_B as defined above, we consider the morphism $\varphi : Z \to B \times A, \varphi = \tau \circ \sigma$. It is unique since it is determined by the product $A \times B$. Therefore, $B \times A$ also satisfies the universal property for the product of A and B. By Proposition 5.4, the two objects are isomorphic. Admittedly, we already observed that an isomorphism exists between the two objects. □

Exercise I.5.9. Let C be a category with products. Find a reasonable candidate for the universal property that the product $A \times B \times C$ of *three* objects of C ought to satisfy, and prove that both $(A \times B) \times C$ and $A \times (B \times C)$ satisfy this universal property. Deduce that $(A \times B) \times C$ and $A \times (B \times C)$ are necessarily isomorphic.

Solution. Given three objects A, B, C of a category C, we can consider the product $A \times B \times C$ with three natural projections π_A, π_B, π_C. The reasonable definition of the universal property is as follows: For every object Z and morphisms $f_A : Z \to A$, $f_B : Z \to B$, and $f_C : Z \to C$, there exists a unique morphism $\sigma : Z \to A \times B \times C$ such that the diagram

$$\begin{tikzcd}
 & & A & \\
Z \arrow[urr, bend left, "f_A"] \arrow[r, "\sigma"] \arrow[drr, "f_B"'] \arrow[ddrrr, bend right, "f_A"'] & A \times B \times C \arrow[ur, "\pi_A"'] \arrow[dr, "\pi_B"] \arrow[ddrr, bend left, "\pi_C"] & & \\
 & & B & \\
 & & & C
\end{tikzcd}$$

commutes.

First we will show that $(A \times B) \times C$ satisfies this universal property. For every object Z, we have a unique morphism $\tau : Z \to A \times B, \tau(z) = (f_A(z), f_B(z))$. Now we define $\sigma : Z \to (A \times B) \times C$,

$$\sigma(z) = (\tau(z), f_C(z)) = ((f_A(z), f_B(z)), f_C(z))$$

We define a natural projection $\pi'_A : (A \times B) \times C \to A, \pi'_A = \pi_A \circ \pi_{A \times B}$ along with an analogous projection π'_B and the typical π_C. These morphisms make the diagram commute because for all $z \in Z$ we have

$$\pi'_A \circ \sigma(z) = \pi_A \circ \pi_{A \times B}((f_A(z), f_B(z)), f_C(z)) = \pi_A(f_A(z), f_B(z)) = f_A(z)$$

and similarly for f_B and f_C. Thus, $(A \times B) \times C$ satisfies the universal property for the product $A \times B \times C$.

An entirely analogous construction shows that $A \times (B \times C)$ also satisfies this universal property. By Proposition 5.4, we must have $(A \times B) \times C \cong A \times (B \times C)$. $\square$

Exercise I.5.10. Push the envelope a little further still, and define products and coproducts for *families* (i.e., indexed sets) of objects of a category. Do these exist in Set? It is common to denote the product $\underbrace{A \times \cdots \times A}_{n \text{ times}}$ by A^n.

Solution. Given a family of objects $\{A_i\}_{i\in I}$ for some set I in a category C, the product $\Pi_{i\in I}A_i$ with natural projections $\{\pi_{A_i}\}_{i\in I}$ should satisfy the universal property that for all objects Z and morphisms $\{f_{A_i}\}_{i\in I}, f_{A_i} : Z \to A_i$, there exists a unique morphism $\sigma : Z \to \Pi_{i\in I}A_i$ such that $\pi_{A_i} \circ \sigma = f_{A_i}$ for all $i \in I$.

Similarly, the coproduct $\coprod_{i\in I} A_i$ with natural inclusions $\{i_{A_i}\}_{i\in I}$ should satisfy the following universal property: for all objects Z and morphisms $\{f_{A_i}\}_{i\in I}, f_{A_i} : A_i \to Z$, there exists a unique morphism $\sigma : \coprod_{i\in I} A_i \to Z$ such that $\sigma\circ i_{A_i} = f_{A_i}$ for all $i \in I$.

The product for finite families of sets exists. However, we require the Axiom of Choice to ensure that the infinite product of nonempty sets is nonempty. The coproduct should exist for any family of sets since the family is indexed so we can just take the coproduct to be $\bigcup\{i\} \times \{A_i\}$ but I'm not positive. $\square$

Exercise I.5.11. Let A, resp. B, be a set endowed with an equivalence relation $\sim_A$, resp. $\sim_B$. Define a relation $\sim$ on $A \times B$ by setting

$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 \sim_A a_2 \text{ and } b_1 \sim_B b_2.$$

(This is immediately seen to be an equivalence relation.)

- Use the universal property for quotients (§5.3) to establish that there are functions $(A \times B)/{\sim} \to A/{\sim_A}$, $(A \times B)/{\sim} \to B/{\sim_B}$.
- Prove that $(A \times B)/{\sim}$, with these two functions, satisfies the universal property for the product of $A/{\sim_A}$ and $B/{\sim_B}$.
- Conclude (without further work) that $(A \times B)/{\sim}\ \cong (A/{\sim_A}) \times (B/{\sim_B})$.

Solution. Let $\pi_A : A\times B \to A$ and $\pi_B : A\times B \to B$ be the canonical projections for A and B. Let $\pi^Z_\sim : Z \to Z/{\sim}$ be the canonical quotient mapping for all objects Z and equivalence relations $\sim$. Consider the morphism $\varphi_A : A \times B \to A/{\sim_A}$,

$$\varphi_A = \pi^Z_{\sim_A} \circ \pi_A$$

We then use the universal property of quotients to see that there exists a unique morphism $\overline{\varphi}_A : (A\times B)/{\sim} \to A/{\sim_A}$. By analogous means, there exists a unique morphism $\overline{\varphi}_B : (A \times B)/{\sim} \to B/{\sim_B}$.

Now we will show that these morphisms act as natural projections from the product of $A/{\sim_A}$ and $B/{\sim_B}$. Let Z be a set with morphisms $f_A : Z \to A/{\sim_A}$ and $f_B : Z \to B/{\sim_B}$. Then there exists a unique morphism $\sigma : Z \to (A\times B)/{\sim}$ such that the diagram

$$\begin{tikzcd}
 & & A/{\sim_A} \\
Z \arrow[urr, bend left, "f_A"] \arrow[r, "\sigma"] \arrow[drr, bend right, "f_B"'] & (A\times B)/{\sim} \arrow[ur, "\overline{\varphi}_A"'] \arrow[dr, "\overline{\varphi}_B"] & \\
 & & B/{\sim_B}
\end{tikzcd}$$

commutes. Define a function $\tau : Z \to A/{\sim_A} \times B/{\sim_B}, \tau(z) = (f_A(z), f_B(z))$. Note that by the universal property of the quotient there exists a unique function $\overline{1}_A : A/{\sim_A} \to A$, $\overline{1}_A([a]_{\sim_A}) = a$. We define a similar function $\overline{1}_B$. Then we construct a morphism $\overline{1}_{A\times B} : A/{\sim_A} \times B/{\sim_B} \to A \times B$,

$$\overline{1}_{A\times B}([a]_{\sim_A}, [b]_{\sim_B}) = (\overline{1}_A([a]_{\sim_A}), \overline{1}_B([b]_{\sim_B}))$$

We now finally define $\sigma = \pi_{\sim}^{A\times B} \circ \overline{1}_{A\times B} \circ \tau$. Then we have

$$\begin{aligned} \overline{\varphi}_A \circ \sigma(z) &= \overline{\varphi}_A \circ \pi_{\sim}^{A\times B}(\overline{1}_{A\times B}(f_A(z), f_B(z))) \\ &= \overline{\varphi}_A(f_A(z), f_B(z)) \\ &= f_A(z) \end{aligned}$$

Similarly, $\overline{\varphi}_B \circ \sigma(z) = f_B(z)$. Thus, $(A \times B)/\sim$ satisfies the universal property for the product of $A/{\sim_A}$ and $B/{\sim_B}$. Therefore, $(A \times B)/\sim \cong A/{\sim_A} \times B/{\sim_B}$. □

Exercise I.5.12. Define the notions of *fibered products* and *fibered coproducts*, as terminal objects of the categories $\mathsf{C}_{\alpha,\beta}$, $\mathsf{C}^{\alpha,\beta}$ considered in Example 3.10 (cf. also Exercise 3.11), by stating carefullly the corresponding universal properties. As it happens, Set has both fibered products and coproducts. Define these objects 'concretely', in terms of naive set theory.

Solution. Recall that given two morphisms $\alpha : A \to C$ and $\beta : B \to C$, the category $\mathsf{C}_{\alpha,\beta}$ is defined as follows:

- $\mathrm{Obj}(\mathsf{C}_{\alpha,\beta})$ = commutative diagrams

$$\begin{tikzcd} & A \arrow[dr, "\alpha"] & \\ Z \arrow[ur, "f"] \arrow[dr, "g"'] & & C \\ & B \arrow[ur, "\beta"'] & \end{tikzcd}$$

  where Z is an object in C

- Morphisms between objects (Z_1, f_1, g_1) and (Z_2, f_2, g_2) are commutative diagrams

$$\begin{tikzcd} & & A \arrow[dr, "\alpha"] & \\ Z_1 \arrow[urr, bend left, "f_1"] \arrow[r, "\sigma"] \arrow[drr, bend right, "g_1"'] & Z_2 \arrow[ur, "f_2"] \arrow[dr, "g_2"'] & & C \\ & & B \arrow[ur, "\beta"'] & \end{tikzcd}$$

  That is, we have a morphism $\sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$ such that the diagram commutes.

The fibered product $A \times_C B$ is a final object in this category. In other words, for every object Z with morphisms $f : Z \to A$ and $g : Z \to B$ where $\alpha \circ f = \beta \circ g$, there exists a unique morphism $\sigma : Z \to A \times_C B$ such that the diagram

$$\begin{tikzcd}
 & & A \arrow[dr, "\alpha"] & \\
Z \arrow[r, "\sigma"] \arrow[urr, bend left, "f"] \arrow[drr, bend right, "g"'] & A \times_C B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"'] & & C \\
 & & B \arrow[ur, "\beta"'] &
\end{tikzcd}$$

commutes.

We claim that the fibered product in Set is defined as

$$A \times_C B = \{(a, b) \mid \alpha(a) = \beta(b)\}$$

with the natural projections π_A and π_B. Let Z be an arbitrary object with appropriate morphisms f and g. Define $\sigma : Z \to A \times_C B$ as $\sigma(z) = (f_A(z), f_B(z))$. Then we have $\pi_A \circ \sigma = f$ and $\pi_B \circ \sigma = g$. Combined with the condition that $\alpha \circ f = \beta \circ g$, it becomes clear that these definitions make the diagram commute.

We define the fibered coproduct analogously. Recall that given morphisms $\alpha : C \to A$ and $\beta : C \to B$, the category $\mathsf{C}^{\alpha,\beta}$ is defined as:

- $\mathrm{Obj}(\mathsf{C}^{\alpha,\beta})$ = commutative diagrams

  $$\begin{tikzcd}
   & A \arrow[dr, "f"] & \\
  C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z \\
   & B \arrow[ur, "g"'] &
  \end{tikzcd}$$

  where Z is an object in C

- Morphisms between objects (Z_1, f_1, g_1) and (Z_2, f_2, g_2) are commutative diagrams

  $$\begin{tikzcd}
   & A \arrow[dr, "f_1"] \arrow[drr, bend left, "f_2"] & & \\
  C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z_1 \arrow[r, "\sigma"] & Z_2 \\
   & B \arrow[ur, "g_1"'] \arrow[urr, bend right, "g_2"'] & &
  \end{tikzcd}$$

  That is, we have a morphism $\sigma \in \mathrm{Hom}_{\mathsf{C}}(Z_1, Z_2)$ such that the diagram commutes.

The fibered coproduct $A \coprod_C B$ is initial in this category. Thus, for every object Z with morphisms $f : A \to Z$ and $g : B \to Z$ where $f \circ \alpha = g \circ \beta$, the diagram

$$\begin{tikzcd}
 & A \arrow[dr, "i_A"] \arrow[drr, bend left, "f"] & & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & A \coprod_C B \arrow[r, "\sigma"] & Z \\
 & B \arrow[ur, "i_B"'] \arrow[urr, bend right, "g"'] & &
\end{tikzcd}$$

commutes.

To construct the fibered coproduct $A \coprod_C B$ in Set, first consider the disjoint union $(\{0\} \times A) \cup (\{1\} \times B)$. We define an equivalence relation $\sim$ on this set, setting

$$\begin{aligned}
&(0, a) \sim (0, a') \iff a = a', \\
&(1, b) \sim (1, b') \iff b = b', \\
&(0, a) \sim (1, b) \iff \exists c \in C : \alpha(c) = a \text{ and } \beta(c) = b
\end{aligned}$$

Interestingly, note that equivalence classes have at most 2 elements.

We claim that $A \coprod_C B/{\sim}$ is a fibered coproduct in Set with the maps $i_A(a) = [(0, a)]_\sim$ and $i_B(b) = [(1, b)]_\sim$. Let Z be a set with functions $f : A \to Z$ and $g : B \to Z$ such that $f \circ \alpha = g \circ \beta$. By the universal property of the coproduct, there is a unique morphism $\sigma' : A \coprod B \to Z$. Now we use the universal property of the quotient to construct a unique function $\sigma : A \coprod B/{\sim} \to Z$. We can verify that

$$\sigma \circ i_A(a) = \sigma([(0, a)]_\sim) = \sigma'(0, a) = f(a)$$

Similarly, we have $\sigma \circ i_B(b) = g(b)$. Combined with the condition that $f \circ \alpha = g \circ \beta$, it becomes clear that the diagram commutes. $\square$

Chapter V

Irreducibility and factorization in integral domains

V.1 Chain conditions and existence of factorizations

Exercise V.1.1. Let R be a Noetherian ring, and let I be an ideal of R. Prove that R/I is a Noetherian ring.

Solution. There is a surjective homomorphism $\varphi : R \to R/I$. By Exercise III.4.2, R/I is also Noetherian. In particular, we have an exact sequence

$$0 \longrightarrow I \longrightarrow R \longrightarrow R/I \longrightarrow 0$$

and by Proposition III.6.7, R is Noetherian if and only if both I and R/I are Noetherian. □

Exercise V.1.2. Prove that if $R[x]$ is Noetherian, so is R. (This is a 'converse' to Hilbert's basis theorem.)

Solution. Consider the ideal $I = (x)$. By Exercise 1, $R[x]/(x) \cong R$ is also Noetherian. One may also consider an arbitrary ideal I in R and realize that $I[x]$ is an ideal in $R[x]$. Since $I[x]$ is finitely generated, the coefficients in I are also finitely generated; hence, I is finitely generated and R is Noetherian. □

Exercise V.1.3. Let k be a field, and let $f \in k[x], f \notin k$. For every subring R of $k[x]$ containing k and f, define a homomorphism $\varphi : k[t] \to R$ by extending the identity on k and mapping t to f. This makes every such R a $k[t]$-algebra. (Example III.5.6).

- Prove that $k[x]$ is finitely generated as a $k[t]$-module.
- Prove that every subring R as above is finitely generated as a $k[t]$-module.
- Prove that every subring of $k[x]$ containing k is a Noetherian ring.

Solution. If $\deg(f) = n$, then $k[x]$ is generated as a $k[t]$-module by the set $\{1, x, x^2, \ldots, x^{n-1}\}$. Clearly any element $g(x) \in k[x]$ with degree $< n$ is generated by the set of generators given. If $\deg(g) = n$, then it is generated by 1 since it can have coefficient f. Thus, we can consider the case where $\deg(g) > n$. Using the division theorem, we can write $g(x) = p(x) \cdot f(x) + r(x)$ where $\deg(r) < n$. Thus, r is generated by the set. Since $\deg(f) > 0$, it must be the case that $\deg(p) < deg(g)$. If $\deg(p) \leq n$, it is finitely generated. Otherwise, we may repeat use of the division algorithm until it is. Thus, every element of $k[x]$ can be written as a linear combination of elements in the generating set. Therefore, $k[x]$ is a finitely generated $k[t]$-module.

Recall that if k is a field then $k[t]$ is a PID; that is, every ideal can be generated by a single element. Since $k[x]$ is finitely generated as a $k[t]$-module, $k[x]$ is also Noetherian. Any subring R containing k and f is a submodule of $k[x]$. Then R is finitely generated.

Certainly any subring R is Noetherian as a $k[t]$-module. Therefore, it is also a finite type $k[t]$-algebra and hence isomorphic to a quotient of $k[t]$. Since $k[t]$ is a Noetherian ring, by Hilbert's Basis Theorem so is any quotient of $k[t]$. That is, R is a Noetherian ring. □

Exercise V.1.4. Let R be the ring of real-valued continuous functions on the interval $[0, 1]$. Prove that R is not Noetherian.

Solution. Consider the ideal $I_{[a,b]} = \{f \in R \mid f([a, b]) = 0\}$. This is indeed an ideal because for $f, g \in I_{[a,b]}$, we have $(f + g)([a, b]) = f([a, b]) + g([a, b]) = 0$, so $f + g \in I_{[a,b]}$. Furthermore, if $h \in R$, then $(h \cdot f)([a, b]) = h([a, b]) \cdot f([a, b]) = h \cdot 0 = 0$ so $h \cdot f \in I_{[a,b]}$, proving that $I_{[a,b]}$ is an ideal.

Now notice that if $[c, d] \subset [a, b]$, then $I_{[c,d]} \subset I_{[a,b]}$. Since there are uncountably many inclusive subsets, there is an associated chain of ideals that never stabilizes. Thus, R is not Noetherian. □

Exercise V.1.5. Determine for which sets S the power set ring $\mathscr{P}(S)$ is Noetherian. (Cf. Exercise III.3.16.)

Solution. Recall that the power set ring is defined with the following operations:

$$A + B = (A \cup B) \setminus (A \cap B), \quad A \cdot B = A \cap B.$$

By Exercise III.3.16, if $T \subset S$, then the subsets of T form an ideal of $\mathscr{P}(S)$ and for finite S, every ideal is of this form. These ideals are finitely generated. Simply take the one element subsets of T and add them to form the other subsets (this works because the set difference is empty). Thus, $\mathscr{P}(S)$ is Noetherian for finite S. I believe for any infinite set S, the ring is not Noetherian since we can construct an ideal whose elements are all finite subsets of S. Such an ideal doesn't have any clear finite basis. $\square$

Exercise V.1.6. Let I be an ideal of $R[x]$, and let $A \subseteq R$ be the set defined in the proof of Theorem 1.2. Prove that A is an ideal of R.

Solution. The set is defined as follows:

$$A = \{0\} \cup \{a \in R \mid a \text{ is a leading coefficient of an element of } I\}$$

Certainly the set is nonempty. To see it is a subgroup, let $a, b \in A$. That is, there are polynomials f, g whose leading terms are ax^m and bx^n respectively. WLOG assume that $m < n$. Then consider $h = x^{n-m} \cdot f \in I$. The leading term of this polynomial is ax^n. Then $g - h$ has leading term $(a - b)x^n$ so $a - b \in A$ and A is an additive subgroup.

Given $r \in R$, the polynomial $r \cdot f \in I$ and it has leading term rax^m. Thus, $ra \in A$ so A is an ideal of R. $\square$

Exercise V.1.7. Prove that if R is a Noetherian ring, then the ring of power series $R[[x]]$ (cf. §III.1.3) is also Noetherian. (Hint: The order of a power series $\sum_{i=0}^{\infty} a_i x^i$ is the smallest i for which $a_i \neq 0$; the *dominant coefficient* is then a_i. Let $A_i \subseteq R$ be the set of dominant coefficients of series of order i in I, together with 0. Prove that A_i is an ideal of R and $A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$. This sequence stabilizes since R is Noetherian, and each A_i is finitely generated for the same reason. Now adapt the proof of Lemma 1.3)

Solution. Let I be an ideal of $R[[x]]$. Define the ideal A_i of R as follows:

$$A_i = \{0\} \cup \{a_i \mid a_i \text{ is a dominant coefficient of an order 0 power series in } I\}$$

We can verify that A_i is an ideal since the power series corresponding to elements $a, b \in A_i$ can be subtracted to yield another power series in I whose dominant coefficient is $a - b$. Similarly, multiplying a power series by some element of R yields another power series in I whose leading term is ra, hence $ra \in A_i$.

Note that $A_i \subseteq A_{i+1}$. Indeed, if $a_i \in A_i$, then there is a power series $f(x) = \sum_{k=i}^{\infty} a_k x^k$. Then the power series $f(x) \cdot x = \sum_{k=i}^{\infty} a_k x^{k+1}$ has order $i + 1$ and dominant coefficient a_i, so $a_i \in A_{i+1}$. Furthermore, each A_i is finitely generated since R is Noetherian and the ascending chain $A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$ stabilizes for some n.

Now consider the sets S_i which are finite sets of power series of order i whose dominant coefficients generate A_i. Certainly there are only finitely many such sets since the ascending chain stabilizes as shown above. We claim that the union $S = \bigcup S_i$ generates I. Indeed, given a power series f, the terms of degree $\leq n$ are killed off by elements in S. Terms of degree $> n$ require an infinite series of the form $\sum_{k=n+1}^{\infty} r_k x^{k-n}$ to be killed off. However, this is not an issue as the series is in the ring $R[[x]]$. Thus, the ideal I is finitely generated by S. $\square$

Exercise V.1.8. Prove that every ideal in a Noetherian ring R contains a finite product of prime ideals. (Hint: Let $\mathscr{F}$ be the family of ideals that do not contain finite products of prime ideals. If $\mathscr{F}$ is nonempty, it has a maximal element M since R is Noetherian. Since $M \in \mathscr{F}$, M is not itself prime, so $\exists a, b \in R$ s.t. $a \notin M, b \notin M$, yet $ab \in M$. What's wrong with this?)

Solution. Consider such a family $\mathscr{F}$ and a maximal element M. The ideals $M + (a)$ and $M + (b)$ are both strictly larger than M. Since M does not contain a finite product of prime ideals, neither does $M + (a)$. Thus, $M + (a) \in \mathscr{F}$, contradicting the maximality of M. $\square$

Exercise V.1.9. Let R be a commutative ring, and let $I \subseteq R$ be a proper ideal. The reader will prove in Exercise 3.12 that the set of prime ideals containing I has minimal elements (the *minimal primes* of I). Prove that if R is Noetherian, then the set of minimal primes of I is finite. (Hint: Let $\mathscr{F}$ be the family of ideals that do *not* have finitely many minimal primes. If $\mathscr{F} \neq \emptyset$, note that $\mathscr{F}$ must have a maximal element I, and I is not prime itself. Find ideals J_1, J_2 strictly larger than I, such that $J_1 J_2 \subseteq I$, and deduce a contradiction.)

Solution. Consider such a family $\mathscr{F}$ and maximal element I. Certainly I is not prime itself so there exists elements $a, b \notin I$ such that $ab \in I$. Consider the ideals $J_1 = I + (a), J_2 = I + (b)$, both of which are strictly larger than I. Both of these are proper. Indeed, if $I + (b) = R$, then we would have $(a)I + (a)(b) = (a)$. However, $(a)I + (a)(b) \subseteq I$, contradicting the fact that $a \notin I$. Thus, we have $J_1 J_2 \subseteq I$. Any prime ideal containing I also contains either J_1 or J_2. That is, any prime minimal over I is also minimal over J_1 or J_2. But J_1 and J_2 only have finitely many primes by the maximality of I, a contradiction. $\square$

Exercise V.1.10. By Proposition 1.1, a ring R is Noetherian if and only if it satisfies the a.c.c. for ideals. A ring is *Artinian* if it satisfies the d.c.c (descending chain condition) for ideals. Prove that if R is Artinian and $I \subseteq R$ is an ideal, then R/I is Artinian. Prove that if R is an Artinian integral domain, then it is a field. (Hint: Let $r \in R, r \neq 0$. The ideals (r^n) form a descending sequence; hence $(r^n) = (r^{n+1})$ for some n. Therefore....) Prove that Artinian rings have Krull dimension 0 (that is, prime ideals are maximal in Artinian rings).

Solution. Ideals of R/I are ideals of R containing I. Therefore, a chain of ideals in R/I is of the form $I_1/I \supseteq I_2/I \supseteq I_3/I \supseteq \cdots$. This corresponds to a descending chain of ideals in R, namely $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ which stabilizes since R is Artinian. That is, there is some n such that $I_n = I_{n+1} = \cdots$. Then $I_n/I = I_{n+1}/I = \cdots$ so the descending chain in R/I also stabilizes. Thus, R/I is Artinian.

Let R be an Artinian integral domain and consider the descending chain $(r) \supseteq (r^2) \supseteq (r^3) \supseteq \cdots$ which stabilizes for some n. That is, there is some n for which $(r^n) = (r^{n+1})$. Then there exists $s \in R$ such that $r^n = r^{n+1}s$. Since R is an integral domain, cancellation applies and we can write $1 = rs$. Thus r is a unit and hence R is a field.

Recall that an ideal I is prime if and only if R/I is an integral domain. If R is Artinian and I is a prime ideal, then R/I is an Artinian integral domain and hence a field. An ideal I is maximal if and only if R/I is a field. Thus, I is maximal in R. Since all prime ideals are maximal, the longest chain of prime ideals has length 0. Thus, the Krull dimension of an Artinian ring is 0. □

Exercise V.1.11. Prove that the 'associate' relation is an equivalence relation.

Solution. Say $a \sim b$ if a is associate with b. Certainly $(a) = (a)$ so $a \sim a$ and the relation is reflexive. If $a \sim b$ then $(a) = (b)$. Then $(b) = (a)$ so $b \sim a$ and the relation is symmetric. Finally, if $a \sim b$ and $b \sim c$, then $(a) = (b) = (c)$ so $a \sim c$ and the relation is transitive. Thus the associate relation is an equivalence relation. □

Exercise V.1.12. Let R be an integral domain. Prove that $a \in R$ is irreducible if and only if (a) is maximal among proper principal ideals of R.

Solution. Suppose a is irreducible. Consider the principal ideals of R. Suppose there exists b such that $(a) \subseteq (b)$. That is, there exists $c \in R$ such that $a = bc$. Since a is irreducible, either b or c is a unit. WLOG, suppose b is a unit (the proof is analogous for the ideal (c). Then there is an element $b^{-1} \in R$ such that $bb^{-1} = 1$. In particular, $1 \in (b)$ so $(b) = R$. Thus, (a) is maximal among principal ideals.

Now suppose that (a) is maximal among principal ideals of R. That is, if $(a) \subseteq (b)$ then either $(a) = (b)$ or $(b) = R$. If $(a) = (b)$ then a and b are associates and $a = ub$ for some unit u by Lemma 1.5. If $(b) = R$ then $1 \in (b)$ and there exists some element $c \in R$ such that $1 = bc$. Thus b is a unit and $a = bd$ for some d (by the assumption that $(a) \subseteq (b)$. In either case, a is irreducible. □

Exercise V.1.13. Prove that prime $\iff$ irreducible in $\mathbb{Z}$.

Solution. Suppose p is prime and that $p = ab$. Certainly $p \mid ab$ so $p \mid a$ or $p \mid b$. WLOG, assume $p \mid a$. We can write $a = pc$ for some c. That is, $a = abc$ so $1 = bc$. Thus, b is a unit and p is irreducible.

Now suppose that p is irreducible and that $p \mid ab$ but $p \nmid a$. Let $g = \gcd(p, a)$. Then $g \mid p$ and by the irreducibility of p, g is a unit. The only units of $\mathbb{Z}$ are 1 and -1 but just assume that $g = 1$ for the sake of simplicity. By Bezout's Theorem, there exist x, y such that $ax + py = 1$. Then $abx + bpy = b$, and since p divides the left side we also have $p \mid b$. Therefore, p is prime. $\square$

Exercise V.1.14. For a, b in a commutative ring R, prove that the class of a in $R/(b)$ is prime if and only if the class of b in $R/(a)$ is prime.

Solution. Denote the class of a as $\bar{a}$. Suppose that $\bar{a}$ is prime in $R/(b)$. That is, the ideal $(\bar{a})$ is prime. Then the quotient $(R/(b))/(\bar{a})$ is an integral domain. However, recall that

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

Thus, $(R/(a))/(\bar{b})$ is also an integral domain so $\bar{b}$ is prime in $R/(a)$. $\square$

Exercise V.1.15. Identify $S = \mathbb{Z}[x_1, \ldots, x_n]$ in the natural way with a subring of the polynomial ring in countably infinitely many variables $R = \mathbb{Z}[x_1, x_2, x_3, \ldots]$. Prove that if $f \in S$ and $(f) \subseteq (g)$ in R, then $g \in S$ as well. Conclude that the ascending chain condition for principal ideals holds in R, and hence R is a domain with factorizations.

Solution. If $(f) \subseteq (g)$, then there is a polynomial $h \in R$ such that $f = gh$. Suppose g involves m variables. Then $m \leq n$. Indeed, if $m > n$, there would be some variable x_m in g which vanishes when multiplied by h. However, $\mathbb{Z}$ is an integral domain so this only occurs if $h = 0$, in which case $f = 0$. Thus, g is a polynomial in fewer degrees than f so it can be identified in S by setting all coefficients of $x_{m+1}, x_{m+2}, \ldots, x_n$ to 0. The ascending chain condition for principal ideals holds in S since it is Noetherian by Hilbert's basis theorem. Therefore, it also holds in R since, given any element $f \in R$, the ascending chain $(f) \subseteq (f_1) \subseteq (f_2) \subseteq \cdots$ stabilizes in S. Thus, R is a domain with factorizations. $\square$

Exercise V.1.16. Let

$$R = \frac{\mathbb{Z}[x_1, x_2, x_3, \ldots]}{(x_1 - x_2^2, x_2 - x_3^2, \ldots)}.$$

Does the ascending chain condition for principal ideals hold in R?

Solution. By construction, we have $x_n = x_{n+1}^2$ so $(x_n) \subseteq (x_{n+1})$. To show that the inclusion is strict, suppose that $x_{n+1} \in (x_n)$. Then there is some polynomial $p \in R$ such that $p \cdot x_{n+1} = x_n$ or $x_{n+1}(p \cdot x_{n+1} - 1) = 0$, so we simply show that R is an integral domain.

Let $a, b \in R$ be nonzero. Using the relations in the ideal, we can write $a = p(x_n)$ and $b = q(x_n)$ for nonzero polynomials p, q. Then $ab = p(x_n)q(x_n) \neq 0$ since $\mathbb{Z}[x_n] \cap (x_1 - x_2^2, \cdots) = 0$ inside $\mathbb{Z}[x_1, x_2, \cdots]$.

Therefore, R is an integral domain and the equation $x_{n+1}(p \cdot x_{n+1} - 1) = 0$ implies that $p \cdot x_{n+1} = 1$, or x_{n+1} is a unit. But units are preserved by homomorphisms and evaluating at $x_n = 0$ yields $0 = 1$ in $\mathbb{Z}$, a contradiction. Thus, we have $x_{n+1} \notin (x_n)$ so we can construct an ascending chain $(x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \cdots$ which never stabilizes since there are countably infinite variables. $\square$

Exercise V.1.17. Consider the subring of $\mathbb{C}$:

$$\mathbb{Z}[\sqrt{-5}] := \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}.$$

- Prove that this ring is isomorphic to $\mathbb{Z}[t]/(t^2 + 5)$.
- Prove that it is a Noetherian integral domain.
- Define a 'norm' N on $\mathbb{Z}[\sqrt{-5}]$ by setting $N(a + bi\sqrt{5}) = a^2 + 5b^2$. Prove that $N(zw) = N(z)N(w)$. (Cf. Exercise III.4.10.)
- Prove that the units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1. (Use the preceding point.)
- Prove that $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ are all irreducible nonassociate elements of $\mathbb{Z}[\sqrt{-5}]$.
- Prove that no element listed in the preceding point is prime. (Prove that the rings obtained by modding out the ideals generated by these elements are not integral domains.)
- Prove that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

Solution. Consider the evaluation homomorphism $\varphi : \mathbb{Z}[t] \to \mathbb{Z}[\sqrt{-5}]$ sending $f(t) \mapsto f(i\sqrt{5})$. Clearly the homomorphism is surjective since $a + bi\sqrt{5}$ is mapped to by $f(t) = a + bt \in \mathbb{Z}[t]$. Thus, we have

$$\frac{\mathbb{Z}[t]}{\ker(\varphi)} \cong \mathbb{Z}[\sqrt{-5}]$$

By definition, $t^2 + 5 \in \ker(\varphi)$ so certainly $(t^2 + 5) \subseteq \ker(\varphi)$. Now let $f \in \ker(\varphi)$. By polynomial division, $f(t) = (t^2 + 5)g(t) + r(t)$ for some $g(t), r(t) \in \mathbb{Z}[t]$ where $\deg(r) < 2$. If $f(\sqrt{-5}) = 0$, then $r(\sqrt{-5}) = 0$, but r has degree at most one and integer coefficients. Thus, $r(t) = 0$ and $f(t) \in (t^2 + 5)$. That is, $\ker(\varphi) = (t^2 + 5)$ and $\mathbb{Z}[t]/(t^2 + 5) \cong \mathbb{Z}[\sqrt{-5}]$.

Since $\mathbb{Z}$ is Noetherian, by Hilbert's basis theorem, $\mathbb{Z}[t]$ is also Noetherian. Exercise 1 shows that quotients of Noetherian rings are Noetherian so $\mathbb{Z}[t]/(t^2+5) \cong \mathbb{Z}[\sqrt{-5}]$ is Noetherian. Furthermore, $\mathbb{Z}[\sqrt{-5}]$ is a subring of $\mathbb{C}$, a field. Thus, it has no non-trivial zero divisors and is an integral domain.

Let $z = a + bi\sqrt{5}$ and $w = c + di\sqrt{5}$. Then

$$\begin{aligned}
N(zw) &= N((ac - 5bd) + (ad + bc)i\sqrt{5}) \\
&= (ac - 5bd)^2 + 5(ad + bc)^2 \\
&= a^2c^2 + 5a^2d^2 + 5b^2c^2 + 25b^2d^2 \\
&= (a^2 + 5b^2)(c^2 + 5d^2) \\
&= N(z)N(w)
\end{aligned}$$

Suppose that z is a unit. That is, there is an element w such that $zw = 1$. Note that N is a ring homomorphism from $\mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$. Thus, we have $1 = N(1) = N(zw) = N(z)N(w)$ so $N(z)$ is a unit in $\mathbb{Z}$. However, the only units of $\mathbb{Z}$ are ± 1. Then we have $N(z) = a^2 + 5b^2 = 1$ (we can ignore -1 since all terms are positive). Since $5 > 1$, it must be the case that $b = 0$. Then the only remaining choices are $a = \pm 1$. That is, the only units in $\mathbb{Z}[\sqrt{-5}]$ are ± 1.

It is easy to see that all of $2, 3, 1 + i\sqrt{5}, 1 - \sqrt{5}$ are irreducible. Indeed, suppose $z = w_1 w_2$. Then $N(z) = N(w_1)N(w_2)$. Notice that for each element listed, $N(z)$ is prime in $\mathbb{Z}$. Thus, if $N(z) \mid N(w_1)$, then $N(w_2) = \pm 1$ (since prime $\iff$ irreducible in $\mathbb{Z}$). Then $w_2 = \pm 1$ in $\mathbb{Z}[\sqrt{-5}]$ so z is irreducible. Since we have shown that $\mathbb{Z}[\sqrt{-5}]$ is an integral domain, associate elements are unit multiples of one another. However, we have shown that the only units are ± 1 and clearly none of the listed elements are unit multiplies of each other. Therefore, none of them are associate.

I'll show that 2 is not prime, the rest follow somewhat similarly. First note that $\mathbb{Z}[\sqrt{-5}]/(2) = \mathbb{Z}_2[\sqrt{-5}]$. Then we have that $(1 + i\sqrt{5})^2 = 1 + 2i\sqrt{5} - 5 = 0$. Thus, $\mathbb{Z}_2[\sqrt{-5}]$ is not an integral domain so 2 is not prime in $\mathbb{Z}[\sqrt{-5}]$.

Simply note that $2 \cdot 3 = 6 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. Since none of these factors are associates, the factorization of 6 is not unique. Hence, $\mathbb{Z}[\sqrt{-5}]$ is not a UFD. $\square$

V.2 UFDs, PIDs, Euclidean domains

Exercise V.2.1. Prove Lemma 2.1.

Lemma 2.1. *Let R be a UFD, and let a, b, c be nonzero elements of R. Then*

- $(a) \subseteq (b) \iff$ *the multiset of irreducible factors of b is contained in the multiset of irreducible factors of a;*
- *a and b are associates (that is, $(a) = (b)$) $\iff$ the two multisets coincide;*

- *the irreducible factors of a product bc are the collection of all irreducible factors of b and c.*

Solution. Let M_a denote the multiset containing the irreducible factors of a.

- $(a) \subseteq (b) \iff a = bc \iff a = (q_1^{\alpha_1} \cdots q_r^{\alpha_r})c \iff M_b \subseteq M_a$.
- $(a) = (b) \iff (a) \subseteq (b)$ and $(b) \subseteq (a) \iff M_a \subseteq M_b$ and $M_b \subseteq M_a$. That is, the multisets coincide.
- It is clear from point 1 that the irreducible factors of b and c are contained in the irreducible factors of bc. Now suppose q is an irreducible factor of bc. If q is a factor of b then we are done so suppose not. Then we may factor $bc = bqr$ where r is some collection of units and irreducible factors. Since R is a UFD and in particular an integral domain, we cancel b on both sides and obtain $c = qr$. That is, q is a factor of c. Thus, the irreducible factors of bc are the collection of irreducible factors of b and c.

□

Exercise V.2.2. Let R be a UFD, and let a, b, c be elements of R such that $a \mid bc$ and $\gcd(a, b) = 1$. Prove that a divides c.

Solution. Since $a \mid bc$, there exists $r \in R$ such that $ar = bc$. By uniqueness, both sides of this equation share the same multiset of irreducible factors. Since $\gcd(a, b) = 1$, a and b share no irreducible factors. Thus, the irreducible factors of a are contained in those of c and we have $a \mid c$. □

Exercise V.2.3. Let n be a positive integer. Prove that there is a one-to-one correspondence preserving multiplicities between the irreducible factors of n (as an integer) and the composition factors of $\mathbb{Z}/n\mathbb{Z}$ (as a group). (In fact, the Jordan-Hölder theorem may be used to prove that $\mathbb{Z}$ is a UFD.)

Solution. Let d be the largest proper divisor of n and let $G_1 = \mathbb{Z}/d\mathbb{Z}$. Then G/G_1 is simple of cyclic, hence it has prime order. Repeating this process (a finite number of times since n is finite), we obtain a composition series of G,

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1,$$

where G_i/G_{i+1} has prime order. Then

$$n = |G| = |G/G_1||G_1/G_2| \cdots |G_{m-1}/G_{m-2}| = p_1 p_2 \cdots p_{m-1}.$$

Thus, this process produces a composition series whose factors are in bijection with the prime (and irreducible, since we are in $\mathbb{Z}$) factors of n. □

Exercise V.2.4. Consider the elements x, y in $\mathbb{Z}[x, y]$. Prove that 1 is a gcd of x and y, and yet 1 is *not* a linear combination of x and y. (Cf. Exercise II.2.13.)

Solution. Certainly $(x, y) \subseteq (1) = R$. Now consider d such that $(x, y) \subseteq (d)$. Then $d \mid x$ and $d \mid y$. However, both x and y are irreducible and $(x) \subsetneq (d)$ so the two are not associate. Thus, d is a unit in $\mathbb{Z}[x, y]$ such as 1. However, 1 cannot be written as a linear combination of x and y by comparing degrees. $\square$

Exercise V.2.5. Let R be the subring of $\mathbb{Z}[t]$ consisting of polynomials with no term of degree 1: $a_0 + a_2 t^2 + \cdots + a_d t^d$.

- Prove that R is indeed a subring of $\mathbb{Z}[t]$, and conclude that R is an integral domain.
- List all common divisors of t^5 and t^6 in R.
- Prove that t^5 and t^6 have no gcd in R.

Solution. Certainly if $f, g \in R$, then $f - g \in R$ since adding polynomials cannot introduce terms of a new degree. We also have

$$fg = (a_0 + a_2 t^2 + \cdots)(b_0 + b_2 t^2 + \cdots) = a_0 b_0 + (a_0 b_2 + a_2 b_0)t^2 + \cdots \in R$$

Thus, R is a subring of $\mathbb{Z}[t]$. A subring of an integral domain is also an integral domain (or else non-zero elements x, y such that $xy = 0$ would also be in the ring). Thus, R is an integral domain.

The common divisors of t^5 and t^6 in R are 1, t^2, and t^3. However, note that $t^6 = t^5 \cdot t$ and $t \notin R$. Suppose $d = \gcd(t^5, t^6)$. Then $t^6 \in (d)$. That is, there is an element a such that $t^6 = t^5 \cdot t = ad$. We may cancel since R is an integral domain to find that $t = bd$ and thus $t \in (d)$, a contradiction. Therefore, t^5 and t^6 have no greatest common divisor. $\square$

Exercise V.2.6. Let R be a domain with the property that the intersection of any family of principal ideals in R is necessarily a principal ideal.

- Show that greatest common divisors exist in R.
- Show that UFDs satisfy this property.

Solution. Since the intersection is associative, we may consider only two elements $a, b \in R$. Consider their intersection $(a) \cap (b) = (m)$. Then we have $ab = dm$ for some $d \in R$. We claim that $d = \gcd(a, b)$. Indeed, we have $(m) \subseteq (a)$ so $m = a \cdot r$ for some r. Then $ab = dm = dar \Longrightarrow b = dr \Longrightarrow d \mid b$. Similarly, $d \mid a$ so it is a common divisor of both. Now let $c \mid a$ and $c \mid b$. That is, $a = cr_1$ and $b = cr_2$. Then $c \mid ab$, or $ab = cx$ for some x. Rewriting, we have $cr_1 b = cx \Longrightarrow (x) \subseteq (b)$. Similarly, $(x) \subseteq (a)$. Then $(x) \subseteq (a) \cap (b) = (m)$ so

$x = ms$ for some s. Finally, we have $dm = ab = cx = c(ms) \Longrightarrow d = cs \Longrightarrow c \mid d$. Thus, d is indeed a gcd for a and b.

Let R be a UFD and consider a family of principal ideals $\{(a_i)\}$. Let $I \bigcap_i (a_i)$ and pick any $r_0 \in I$. If $(r_0) = I$, we are done so suppose not. Then pick $s \in I - (r_0)$. We may then set $r_1 = \gcd(r_0, s)$. The ideal (r_1) is the smallest principal ideal containing (r_0, s), which is a subset of each (a_i) since both generators are chosen from the intersection of these ideals. Thus $(r_1) \subseteq I$ and we have the chain

$$(r_0) \subsetneq (r_0, s) \subseteq (r_1) \subseteq I.$$

This process can be repeated as long as $(r_n) \subsetneq I$. Thus, we form an ascending chain of principal ideals and since R is a UFD, it must stabilize. This occurs when $(r_n) = I$. $\square$

Exercise V.2.7. Let R be a Noetherian domain, and assume that for all nonzero a, b in R, the greatest common divisors of a and b are linear combinations of a and b. Prove that R is a PID.

Solution. Suppose that R is not a PID and let I be a non-principal ideal. Choose $0 \neq a_0 \in I$. Then $(a_0) \subsetneq I$ so we may choose $b_0 \in I - (a_0)$. We may consider $a_1 = \gcd(a_0, b_0)$. Then we find

$$(a_0) \subsetneq (a_0, b_0) = (a_1) \subsetneq I$$

Repeating this indefinitely yields an ascending chain of ideals which does not stabilize, a contradiction to the assumption that R is Noetherian. Thus, R must be a PID. $\square$

Exercise V.2.8. Let R be a UFD, and let $I \neq (0)$ be an ideal of R. Prove that every descending chain of principal ideals containing I must stabilize.

Solution. Consider a descending chain of principal ideals containing I

$$(a_1) \supsetneq (a_2) \supsetneq \cdots$$

There is a corresponding ascending chain of multisets of irreducible factors. Let $0 \neq b \in I$. Then $(b) \subseteq (a_i)$ for all (a_i) in the ascending chain. Letting M_b denote the multiset of irreducible factors of b, we have that each multiset in the corresponding ascending chain is contained in M_b. If the chain does not stabilize, then eventually the multiset of irreducible factors for say a_n will have greater size than M_b, a contradiction. Therefore the descending chain of principal ideals must stabilize. $\square$

Exercise V.2.9. The *height* of a prime ideal P in a ring R is (if finite) the maximum length h of a chain of prime ideals $P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_h = P$ in R. (Thus, the Krull dimension of R, if finite, is the maximum height of a prime ideal in R.) Prove that if R is a UFD, then every prime ideal of height 1 in R is principal.

Solution. First note that (0) is prime in R since R is an integral domain. Thus, the chain of ideals looks like

$$(0) \subsetneq P.$$

Since P is non-empty, there is some non-zero element $a \in P$. Consider the factorization of a into irreducibles. Since P is prime, one of these elements belongs to P, say p. Since R is a UFD, irreducible elements are prime so (p) is a prime ideal. But then we have

$$(0) \subsetneq (p) \subseteq P.$$

Since P has height one, it must be the case that $(p) = P$, so P is principal. $\square$

Exercise V.2.10. It is a consequence of a theorem known as *Krull's Hauptidealsatz* that every nonzero, nonunit element in a Noetherian domain is contained in a prime ideal of height 1. Assuming this, prove a converse to Exercise 2.9, and conclude that a Noetherian domain R is a UFD if and only if every prime ideal of height 1 in R is principal.

Solution. Suppose R is a Noetherian domain such that every prime ideal of height 1 is principal. Since R is Noetherian, the a.c.c. holds for all ideals, and principal ideals in particular. Therefore, we only need to show that irreducible elements are prime. Let q be an irreducible element of R. By Krull's Hauptidealsatz, q is contained in some prime ideal of height 1, say (p). Then we have $q = pa$ for some unit a. Thus, $(p) = (q)$ and (q) is prime, implying that q is a prime element. Since every irreducible element is prime, R is a UFD. $\square$

Exercise V.2.11. Let R be a PID, and let I be a nonzero ideal of R. Show that R/I is an artinian ring (cf. Exercise 1.10), by proving explicitly that the d.c.c. holds in R/I.

Solution. Since R is a PID, let $I = (a)$. Consider a descending chain of ideals in R/I

$$\frac{I_0}{I} \supsetneq \frac{I_1}{I} \supsetneq \frac{I_2}{I} \supsetneq \cdots$$

This corresponds to a descending chain of ideals containing I in R. Since R is a PID, it is also a UFD and by Exercise 2.8, a descending chain of principal ideals containing a non-zero ideal must stabilize. Thus, this descending chain in R stabilizes and so does the one in R/I. $\square$

Exercise V.2.12. Prove that if $R[x]$ is a PID, then R is a field.

Solution. Consider the ideal (x). By Exercise 2.11, the quotient $R[x]/(x)$ is artinian. Furthermore, R is an integral domain (since $R[x]$ is) and by Exercise 1.10, an artinian integral domain is a field. $\square$

Exercise V.2.13. For a, b, c positive integers with $c > 1$, prove that $c^a - 1$ divides $c^b - 1$ if and only if $a \mid b$. Prove that $x^a - 1$ divides $x^b - 1$ in $\mathbb{Z}[x]$ if and only if $a \mid b$. (Hint: For the interesting implications, write $b = ad + r$ with $0 \leq r < a$, and take 'size' into account.)

Solution. Since $\mathbb{Z}$ is a Euclidean domain, we may write $b = ad+r$ with $0 \leq r < a$. Then we have

$$x^b - 1 = x^b - x^r + x^r - 1 = x^r \left(x^{ad} - 1\right) + x^r - 1$$

Furthermore, note that

$$x^{ad} - 1 = (x^a - 1)\left(x^{a(d-1)} + x^{a(d-2)} + \cdots + 1\right)$$

Then $x^a - 1$ divides the right side of the first equation if and only if $r = 0$, if and only if a divides b. The first statement is a direct implication by setting $x = c$. $\square$

Exercise V.2.14. Prove that if k is a field, then $k[[x]]$ is a Euclidean domain.

Solution. Define a valuation on $k[[x]] \setminus \{0\}$, setting $v(f)$ to be the degree of the smallest term of f with non-zero coefficient. Indeed, given power series f, g, we write

$$f = qg + r.$$

This is possible since k is a field. If $v(g) > v(f)$ then let $q = 0$ and set $r = f$ so that $v(r) < v(g)$. If $v(g) = v(f)$, then define q such that the first non-zero term of qg equals that of f. Then define r such that the remaining terms are equivalent and we have $v(r) < v(g)$. Similarly, if $v(g) < v(f)$, define q such that the first $v(f) - v(g)$ terms of qg are equal to those of f (possible since k is a field). Then $v(r) < v(g)$. Thus, this is indeed a Euclidean valuation. $\square$

Exercise V.2.15. Prove that if R is a Euclidean domain, then R admits a Euclidean valuation $\bar{v}$ such that $\bar{v}(ab) \geq \bar{v}(b)$ for all nonzero $a, b \in R$. (Hint: Since R is a Euclidean domain, it admits a valuation v as in Definition 2.7. For $a \neq 0$, let $\bar{v}(a)$ be the minimum of all $v(ab)$ as $b \in R, b \neq 0$. To see that R is a Euclidean domain with respect to $\bar{v}$ as well, let a, b be nonzero in R, with $b \nmid a$; choose q, r so that $a = bq + r$, with $v(r)$ minimal; assume that $\bar{v}(r) \geq \bar{v}(b)$, and get a contradiction.)

Solution. Define $\bar{v}$ as above; that is, set $\bar{v}(a) = \min\{v(ab) \mid b \in R, b \neq 0\}$. Clearly, $\bar{v}$ satisfies the property that $\bar{v}(ab) \geq \bar{v}(b)$. Let $a, b \in R$ be non-zero and $b \nmid a$. Write $a = bq + r$ with minimal $v(r)$. Suppose that $\bar{v}(r) \geq \bar{v}(b)$. That is, there exists $c \in R$ such that for all $x \in R$, $v(rx) \geq v(bc)$. In particular, for $x = c$, we have $v(rc) \geq v(bc)$. However, multiplying the initial equation by c yields $ac = bcq + rc$ where $v(rc) < v(bc)$, a contradiction. Thus, $\bar{v}$ is a Euclidean valuation. $\square$

Exercise V.2.16. Let R be a Euclidean domain with Euclidean valuation v; assume that $v(ab) \geq v(b)$ for all nonzero $a, b \in R$ (cf. Exercise 2.15). Prove that associate elements have the same valuation and that units have minimum valuation.

Solution. Let a and b be associates. That is, we can write $a = ub$ for some unit u. Then we have $v(a) = v(ub) \geq v(b)$. Furthermore, we have $b = u^{-1}a$ so $v(b) = v(u^{-1}a) \geq v(a)$. Thus, $v(a) = v(b)$.

Now consider a unit u. For all $r \in R$, we have $r = ru^{-1}u$. This implies that $v(u) \leq v(r)$ so units have minimum valuation. $\square$

Exercise V.2.17. Let R be a Euclidean domain that is not a field. Prove that there exists a nonzero, nonunit element c in R such that $\forall a \in R, \exists q, r \in R$ with $a = qc + r$ and either $r = 0$ or r a unit.

Solution. The existence of a nonzero, nonunit element c is guaranteed since R is not a field. Choose such a c with minimal valuation. Let $a \in R$ and choose q, r such that $a = qc + r$. If $r = 0$ then we are done so suppose not. We have $v(r) < v(c)$. If r is not a unit, then a contradiction arises as we chose c to have minimal valuation. Thus r must be a unit. $\square$

Exercise V.2.18. For an integer d, denote by $\mathbb{Q}(\sqrt{d})$ the smallest subfield of $\mathbb{C}$ containing $\mathbb{Q}$ and $\sqrt{d}$, with norm N defined as in Exercise III.4.10. See Exercise 1.17 for the case $d = -5$; in this problem, you will take $d = -19$.

Let $\delta = (1 + i\sqrt{19})/2$, and consider the following subring of $\mathbb{Q}(\sqrt{-19})$:

$$\mathbb{Z}[\delta] := \left\{ a + b\frac{1 + i\sqrt{19}}{2} \mid a, b \in \mathbb{Z} \right\}.$$

- Prove that the smallest values of $N(z)$ for $z = a + b\delta \in \mathbb{Z}[\delta]$ are 0, 1, 4, 5. Prove that $N(a + b\delta) \geq 5$ if $b \neq 0$.
- Prove that the units in $\mathbb{Z}[\delta]$ are ± 1.
- If $c \in \mathbb{Z}[\delta]$ satisfies the condition specified in Exercise 2.17, prove that c must divide 2 or 3 in $\mathbb{Z}[\delta]$, and conclude that $c = \pm 2$ or $c = \pm 3$.

- Now show that $\nexists q \in \mathbb{Z}[\delta]$ such that $\delta = qc + r$ with $c = \pm 2, \pm 3$ and $r = 0, \pm 1$.

Conclude that $\mathbb{Z}[(1+\sqrt{-19})/2]$ is not a Euclidean domain.

Solution. Certainly $N(z)$ takes on those values for values $(0,0)$, $(\pm 1, 0)$, $(\pm 2, 0)$, and $(0, \pm 1)$. To prove these are minimal, let $|a| > 2$. Then

$$N(a + b\delta) \geq N(a) = a^2 > 4 = N(\pm 2).$$

Furthermore, if $b \neq 0$ then

$$N(a + b\delta) \geq N(b\delta) = \frac{b^2}{4} + 19 \cdot \frac{b^2}{4} = 5b^2 \geq 5$$

Clearly two units in $\mathbb{Z}[\delta]$ are ± 1. Now let u be a unit. Then $N(u) = 1$. By Point 1, we have $u = \pm 1$.

If $c \in \mathbb{Z}[\delta]$ satisfies the condition from the previous problem then we have $2 = q_1 c + r_1$ and $3 = q_2 c + r_2$. If $r_1 = 0$ then $c \mid 2$. If $r_1 \neq 0$ then $r_1 = \pm 1$. If $r_1 = 1$ then $2 = q_1 c + 1 \implies q_1 c = 1$, contradicting that c is not a unit. If $r_1 = -1$, then we have

$$q_2 c + r_2 = 3 = 2 + 1 = q_1 c - 1 + 1 = q_1 c$$

so $c \mid 3$. Given the condition and point 1, it must be the case that $c = \pm 2$ or $c = \pm 3$.

Now suppose there exists $q = a + b\delta \in \mathbb{Z}[\delta]$ such that $\delta = qc + r$ with $c = \pm 2, \pm 3$ and $r = 0, \pm 1$. If $r = 0$, then we have $N(q)N(c) = N(qc) = N(\delta) = 5$. Since 5 is prime and $N(c) = 4$ or 9 respectively, q cannot exist. Similarly, if $r = 1$, then we have $N(q)N(c) = N(qc) = N(\delta - 1) = 5$ and the same contradiction arises. If $r = -1$, then $N(qc) = 7$, another contradiction. Thus, there can be no such q and $\mathbb{Z}[(1+\sqrt{-19})/2]$ is not a Euclidean domain. $\square$

Exercise V.2.19. A *discrete valuation* on a field k is a surjective homomorphism of abelian groups $v : (k^*, \cdot) \to (\mathbb{Z}, +)$ such that $v(a+b) \geq \min(v(a), v(b))$ for all $a, b \in k^*$ such that $a + b \in k^*$.

- Prove that the set $R := \{a \in k^* \mid v(a) \geq 0\} \cup \{0\}$ is a subring of k.
- Prove that R is a Euclidean domain.

Rings arising in this fashion are called *discrete valuation rings*, abbreviated DVR. They arise naturally in number theory and algebraic geometry. Note that the Krull dimension of a DVR is 1 (Example III.4.14); in algebraic geometry, DVRs correspond to particularly nice points on a 'curve'.

- Prove that the ring of rational numbers a/b with b *not* divisible by a fixed prime integer p is a DVR.

Solution. To show that R is a subring, first note that it is a subgroup under addition. Indeed, for nonzero $a, b \in R$ we have

$$v(a - b) \geq \min(v(a), v(-b)).$$

Note that $v(-b) = v(-1 \cdot b) = v(-1) + v(b)$ where -1 is the additive inverse of 1. Furthermore,

$$v(-1) + v(-1) = v(-1 \cdot -1) = v(1) = 0$$

implies that $v(-1) = 0$. Thus, we have $v(-b) = v(b)$ so $v(a-b) \geq \min(v(a), v(-b)) \geq 0$, meaning $a - b \in R$.

To show that R is closed under multiplication, see that $v(ab) = v(a) + v(b)$. Since both $v(a)$ and $v(b)$ are non-negative, so is their sum. Therefore, $ab \in R$ and R is a ring.

To prove that R is a Euclidean domain, we must show that v is a Euclidean valuation which we do by cases. Let $a, b \in R$ be nonzero. If $v(a) \geq v(b)$, then we have $v(a/b) = v(a) - v(b) \geq 0$ so $a/b \in R$. Therefore we can write $a = (a/b)b + 0$. If $v(a) < v(b)$, then we have $a = 0b + a$. Thus, in any case we can choose $q, r \in R$ such that $a = qb + r$ with either $r = 0$ or $v(r) < v(b)$.

Consider the ring R of rational numbers a/b with b not divisible by a fixed prime integer p. We should define a discrete valuation, that is a group homomorphism to $\mathbb{Z}$, on the field $\mathbb{Q}$ so that the resulting ring arises in the manner defined above. Given a rational number a/b such that a fixed prime $p \nmid b$, we can use the unique factorization of $\mathbb{Z}$ to write

$$\frac{a}{b} = \frac{p^k z}{b}$$

for integers k, z such that $p \nmid z$. Then define $v(a/b) = k$. To verify that v is a discrete valuation, we first show that it is a homomorphism of groups. Indeed, if $x, y \in \mathbb{Q}^*$, then

$$v(xy) = v\left(\frac{a_1 a_2}{b_1 b_2}\right) = v\left(\frac{p^{k_1} z_1 p^{k_2} z_2}{b_1 b_2}\right) = v\left(\frac{p^{k_1 + k_2} z_1 z_2}{b_1 b_2}\right) = k_1 + k_2 = v(x) + v(y)$$

Thus, v is a group homomorphism. Furthermore, we find that

$$v(x + y) = v\left(\frac{a_1 b_2 + a_2 b_1}{b_1 b_2}\right) = v\left(\frac{p^{k_1} z_1 b_2 + p^{k_2} z_2 b_1}{b_1 b_2}\right)$$

WLOG, we may assume $k_1 \leq k_2$. Then

$$v\left(\frac{p^{k_1} z_1 b_2 + p^{k_2} z_2 b_1}{b_1 b_2}\right) = v\left(p^{k_1} \frac{z_1 b_2 + p^{k_2 - k_1} z_2 b_1}{b_1 b_2}\right) = k_1 \geq \min(v(x), v(y))$$

Therefore, v is a discrete valuation and the resulting ring is in fact the one defined above. I did not formulate this valuation myself and I don't see how it's at all a natural definition but it works out. $\square$

Exercise V.2.20. As seen in Exercise 2.19, DVRs are Euclidean domains. In particular, they must be PIDs. Check this directly, as follows. Let R be a DVR, and let $t \in R$ be an element such that $v(t) = 1$. Prove that if $I \subseteq R$ is any nonzero ideal, then $I = (t^k)$ for some $k \geq 1$. (The element t is called a 'local parameter' of R.)

Solution. Let $a \in I$ be a nonzero element with minimal valuation $v(a) = n$. Then for all nonzero $b \in I$, we have

$$v(b/a) = v(b) - v(a) \geq 0 \Longrightarrow b/a \in R \Longrightarrow b \in (a).$$

Although this is sufficient, we can go on to show that if $v(a) = v(b)$ then $(a) = (b)$. Indeed, we find

$$v(a/b) = v(b/a) = 0 \Longrightarrow b \mid a \text{ and } a \mid b \Longrightarrow (a) = (b)$$

For a local parameter t, we have $v(t^k) = k$ so for an element $a \in I$ with minimal valuation n, we have $I = (t^n)$. □

Exercise V.2.21. Prove that an integral domain is a PID if and only if it admits a Dedekind-Hasse valuation. (Hint: For the $\Longleftarrow$ implication, adapt the argument in Proposition 2.8; for $\Longrightarrow$, let $v(a)$ be the size of the multiset of irreducible factors of a.)

Solution. First suppose that R is an integral domain admitting a Dedekind-Hasse valuation. Let I be an ideal of R. If I is zero then it is clearly principal so suppose not. Then choose $0 \neq b \in I$ to have minimal valuation. For all $a \in I$, we either have $(a, b) \in (b)$ or there exists $q, r, s \in R$ such that $as = bq + r$ with $v(r) < v(b)$. In the first case, $a \in (b)$. In the latter case, $r = as - bq \in I$. By choice of b, we cannot have $v(r) < v(b)$. Thus, $r = 0$ and $a \in (b)$. Therefore, $I = (b)$ so R is a PID.

Now suppose that R is a PID. We must show that it admits a Dedekind-Hasse valuation. Define $v : R \to \mathbb{Z}^{\geq 0}$ to send $v(a)$ to the size of the multiset of irreducible factors of a (recall that a PID is a UFD). To verify that this is a Dedekind-Hasse valuation, let $a, b \in R$. We have $(a, b) = (d)$ for some $d \in R$. In particular, $d \mid b$ so $v(d) \leq v(b)$. If $v(d) = v(b)$, then $(b) = (d)$ by considering the size of multisets of irreducible factors so we have $(a, b) = (b)$ and $b \mid a$. If $v(d) < v(b)$, we can write

$$-d = as + bq \Longrightarrow as = bq + d$$

for $q, s \in R$. Thus, v is indeed a Dedekind-Hasse valuation. □

Exercise V.2.22. Suppose $R \subseteq S$ is an inclusion of integral domains, and assume that R is a PID. Let $a, b \in R$ and let $d \in R$ be a gcd for a and b in R. Prove that d is also a gcd for a and b in S.

Solution. Since R is a PID, we have $(a, b) = (d)$. That is, there exist $x, y \in R$ such that $ax + by = d$. Now let $c \in S$ such that $c \mid a$ and $c \mid b$. Then $c \mid ax + by = d$. Thus, d is a gcd for a and b in S as well. $\square$

Exercise V.2.23. Compute $d = \gcd(5504227617645696, 2922476045110123)$. Further, find a, b such that $d = 5504227617645696a + 2922476045110123b$.

Solution. A brief application of the extended Euclidean algorithm shows that $d = 234982394879$. Furthermore, we have $a = 1055$ and $b = -1987$. $\square$

Exercise V.2.24. Prove that there are infinitely many prime integers. (Hint: Assume by contradiction that $p_1, \dots, p_N$ is a complete list of all positive prime integers. What can you say about $p_1 \cdot \dots \cdot p_N + 1$? This argument was already known to Euclid, more than 2,000 years ago.)

Solution. Let $P = p_1 \cdot \dots \cdot p_N + 1$. By assumption, P is not prime so it is divisible by some prime in our list, say p_i. But then we have $p \mid P - p_1 \cdot \dots \cdot p_N = 1$, a contradiction. Therefore the list of primes is not complete. $\square$

Exercise V.2.25. Variation on the theme of Euclid from Exercise 2.24: Let $f(x) \in \mathbb{Z}[x]$ be a nonconstant polynomial such that $f(0) = 1$. Prove that infinitely many primes divide the numbers $f(n)$, as n ranges in $\mathbb{Z}$. (If $p_1, \dots, p_n$ were a complete list of primes dividing the numbers $f(n)$, what could you say about $f(p_1 \cdots p_N x)$?)

Once you are happy with this, show that the hypothesis $f(0) = 1$ is unnecessary. (If $f(0) = a \neq 0$, consider $f(p_1 \cdots p_N a x)$. Finally note that there is nothing special about 0.)

Solution. First note that the requirement $f(0) = 1$ implies that the constant term of the polynomial is 1. Suppose there were a complete list of primes dividing the values of $f(n)$. Let $P = p_1 \cdots p_N$ and consider $f(Px)$. We find

$$f(Px) = 1 + a_1(Px) + a_2(Px)^2 + \cdots + a_n(Px)^n$$

In particular, for $x = 1$, we have p_i divides the left side. But p_i also divides P and so it divides the difference

$$p_i \mid f(Px) - (a_1 Px + a_2(Px)^2 + \cdots + a_n(Px)^n) = 1,$$

a contradiction.

An entirely analogous proof works for $f(0) = a \neq 0$ and considering the product $f(Pax)$. The case $f(0) = 0$ is trivial since all primes p divide $f(p)$. $\square$

V.3 Intermezzo: Zorn's lemma

Exercise V.3.1. Prove that every well-ordering is total.

Solution. Recall that a well-ordering on Z is an order relation such that every nonempty subset of Z has a least element. For any two elements $a, b \in Z$, consider the subset $\{a, b\} \subseteq Z$. Since this subset has a least element, it must be the case that either $a \preceq b$ or $b \preceq a$. As this holds for any pair of elements in Z, it follows that $\preceq$ is total on Z. $\square$

Exercise V.3.2. Prove that a totally ordered set $(Z, \preceq)$ is a woset if and only if every descending chain

$$z_1 \succeq z_2 \succeq z_3 \succeq \cdots$$

in Z stabilizes.

Solution. Suppose every such descending chain stabilizes. Let $S \subseteq Z$ be a nonempty subset. Since Z is totally ordered, the elements of S form a descending chain as described above. Then there is some element a such that for all $b \in Z$, $a \preceq b$. That is, a is a least element in S. Then Z is well-ordered.

Now suppose Z is a woset. Assume there is a descending chain which does not stabilize. Then the set formed by these elements does not have a minimum element, a contradiction. Therefore, every descending chain in Z stabilizes. $\square$

Exercise V.3.3. Prove that the axiom of choice is equivalent to the statement that a set-function is surjective if and only if it has a right-inverse (cf. Exercise I.2.2).

Solution. The proof of the statement about surjective set-functions assumes the axiom of choice, showing that it is sufficient. To see that it is necessary, assume that every surjective set-function has a right-inverse. Let A be a set of disjoint nonempty sets and $B = \bigcup A$. Then for each $b \in B$, there exists exactly one set $X \in A$ such that $b \in X$. Thus, we have a surjective function $f : B \to A$. Then it has a right-inverse g. Define $C := \{g(X) \mid X \in A\}$. Then C is a choice set. $\square$

Exercise V.3.4. Construct explicitly a well-ordering on $\mathbb{Z}$. Explain why you know that $\mathbb{Q}$ can be well-ordered, even without performing an explicit construction.

Solution. The well-ordering on $\mathbb{N}$, namely $\leq$, does not work because of the negative numbers so we work around this by imposing conditions. Let $a, b \in \mathbb{Z}$ and set $a \preceq b$ if and only if one of the following holds:

- $|a| < |b|$.
- $|a| = |b|$ and $a \leq b$.

This well ordering yields the following visualization: $0, -1, 1, -2, 2, \ldots$ Assuming the Well-ordering Theorem, every set admits a well-ordering, including $\mathbb{Q}$. Without directly invoking the theorem, we also know that $\mathbb{Q}$ is a countable set and thus is in bijection with $\mathbb{N}$, which has a well-ordering. $\square$

Exercise V.3.5. Prove that the (ordinary) principle of induction is equivalent to the statement that $\leq$ is a well-ordering on $\mathbb{Z}^{>0}$. (To prove by induction that $(\mathbb{Z}^{>0}, \leq)$ is well-ordered, assume it is known that 1 is the least element of $\mathbb{Z}^{>0}$ and that $\forall n \in \mathbb{Z}^{>0}$ there are no integers between n and $n+1$.)

Solution. In Claim 3.2, it was shown that the principle of induction holds for any well-ordered set. That is, $\leq$ being a well-ordering on $\mathbb{Z}^{>0}$ implies that the principle of induction holds. To show the converse, we can assume that 1 is the least element of $\mathbb{Z}^{>0}$ and that there are no integers between n and $n+1$ for all $n \in \mathbb{Z}$. Suppose that there exist a non-empty subset S of $\mathbb{Z}^{>0}$ such that S has no minimum element. Then $1 \notin S$ or else it would be a minimal element. Similarly, $2 \notin S$ because there are no integers between 1 and 2, which would make 1 a minimal element. If none of $1, 2, \ldots, n$ are in S, then $n+1 \notin S$ or it would be minimal. Thus, the principle of induction implies that S is empty, a contradiction. Therefore, S must have a minimal element so $\leq$ is a well-ordering on $\mathbb{Z}^{>0}$. $\square$

Exercise V.3.6. In this exercise assume the truth of Zorn's lemma and the conventional set-theoretic constructions; you will be proving the well-ordering theorem.

Let Z be a nonempty set, and let $\mathscr{Z}$ be the set of pairs $(S, \leq)$ consisting of a subset S of Z and of a *well-ordering* $\leq$ on S. Note that $\mathscr{Z}$ is not empty (singletons can be well-ordered). Define a relation $\preceq$ on $\mathscr{Z}$ by prescribing

$$(S, \leq) \preceq (T, \leq')$$

if and only if $S \subseteq T, \leq$ is the restriction of $\leq'$ to S, and every element of S precedes every element of $T \setminus S$ w.r.t. $\leq'$.

- Prove that $\preceq$ is an order relation in $\mathscr{Z}$.
- Prove that every chain in $\mathscr{Z}$ has an upper bound in $\mathscr{Z}$.
- Use Zorn's lemma to obtain a maximal element $(M, \leq)$ in $\mathscr{Z}$. Prove that $M = Z$.

Thus every set admits a well-ordering, as stated in Theorem 3.3.

Solution. Recall that an order relation is reflexive, transitive, and antisymmetric. Given a pair $(S, \leq)$, certainly we have $S \subseteq S$ and every element of S precedes every element of $S \setminus S = \emptyset$ with respect to $\leq$. Therefore, $\preceq$ is reflexive. Let $(T, \leq'), (R, \leq'') \in \mathscr{Z}$ such that $(S, \leq) \preceq (T, \leq')$ and $(T, \leq') \preceq (R, \leq'')$. Then $S \subseteq R$ (by transitivity of subsets) and $\leq$ is the restriction of $\leq'$ to S, which is the restriction of $\leq''$ to S. Furthermore, $S \subseteq T$ and every element of T precedes every element of $R \setminus T$ w.r.t. $\leq''$. In particular, every element of S precedes the elements of $R \setminus T$ w.r.t. $\leq''$. Thus, we have $(S, \leq) \preceq (R, \leq'')$, proving transitivity. Finally, suppose we have $(S, \leq) \preceq (T, \leq')$ and $(T, \leq') \preceq (S, \leq)$. Then $S \subseteq T$ and $T \subseteq S$ so $S = T$. To show the two order relations are equivalent, let $a, b \in S$ such that $a \leq b$. Since $\leq$ is the restriction of $\leq'$, we have $a \leq' b$. Similarly, we find $a \leq' b \Longrightarrow a \leq b$. Thus, the two order relations are equivalent and we find $(S, \leq) = (T, \leq')$, proving antisymmetry and showing that $\preceq$ is in fact an order relation on $\mathscr{Z}$.

Now consider a chain $\mathscr{C}$ of subsets. We must show it has an upper bound in $\mathscr{Z}$. Consider the set

$$U := \bigcup_{S \in \mathscr{C}} S.$$

Certainly each $S \subseteq U$. Furthermore, there is a natural order relation on U since for all $a, b \in U$, there exists some $S \in \mathscr{C}$ containing both a and b. Then the order relation on S has $a \leq b$ which also holds in U. Thus, U is well-ordered and is an upper bound for $\mathscr{C}$.

Since every chain has an upper bound, Zorn's lemma states that there is a maximal element $(M, \leq)$ in $\mathscr{Z}$. Clearly $M \subseteq Z$. To show that $M = Z$, suppose otherwise. That is, suppose there is some element $x_0 \in Z \setminus M$. Then consider the set $M \cup \{x_0\}$ with the order relation $\leq'$ such that for all $x \in M$, $x \leq' x_0$. Then $(M, \leq) \preceq (M \cup \{x_0\}, \leq')$, contradicting the maximality of M. Thus, $M = Z$ so Z has a well-ordering. $\square$

Exercise V.3.7. In this exercise assume the truth of the axiom of choice and the conventional set-theoretic constructions; you will be proving the well-ordering theorem.

Let Z be a nonempty set. Use the axiom of choice to choose an element $\gamma(S) \notin S$ for each proper subset $S \subsetneq Z$. Call a pair $(S, \leq)$ a γ-*woset* if $S \subseteq Z$, $\leq$ is a well-ordering on S, and for every $a \in S$, $a = \gamma(\{b \in S, b < a\})$.

- Show how to begin constructing a γ-woset, and show that all γ-wosets must begin in the same way.

Define an ordering on γ-wosets by prescribing that $(U, \leq'') \preceq (T, \leq')$ if and only if $U \subseteq T$ and $\leq''$ is the restriction of $\leq'$.

- Prove that if $(U, \leq'') \prec (T, \leq')$, then $\gamma(U) \in T$.
- For two γ-wosets $(S, \leq)$ and $(T, \leq')$, prove that there is a maximal γ-woset $(U, \leq'')$ preceding both w.r.t. $\preceq$. (Note: There is no need to use Zorn's lemma!)

- Prove that the maximal γ-woset found in the previous point in fact equals $(S, \leq)$ or $(T, \leq')$. Thus, $\preceq$ is a total ordering.
- Prove that there is a maximal γ-woset $(M, \leq)$ w.r.t. $\preceq$. (Again, Zorn's lemma need not and should not be invoked.)
- Prove that $M = Z$.

Thus every set admits a well-ordering, as stated in Theorem 3.3.

Solution. Given $\gamma(S)$, one can begin constructing a γ-woset $(S, \leq)$ by including $\gamma(\emptyset)$. In some sense, $a = \gamma(\emptyset)$ is minimal in S since no elements precede it. Furthermore, since every γ-woset is well-ordered, they all have a minimal element. That is, they all contain $\gamma(\emptyset)$. One can continue the construction of the γ-woset by letting the next element be γ of the elements currently in the set. The well-ordering on the set follows naturally.

Now suppose we have $(U, \leq'') \prec (T, \leq')$. By the definition of $\prec$, we have $U \subset T$. Since T is well-ordered, there is some minimum element a such that for all $b \in U$, $b <' a$. Then $a = \gamma(\{b \in S, b <' a\}) = \gamma(U)$.

Given two γ-wosets $(S, \leq)$ and $(T, \leq')$, consider the set $R = S \cap T$ with the obvious well ordering. Indeed, since $R \subseteq S$ and $R \subseteq T$, R precedes both w.r.t. $\preceq$. Furthermore, if there were any more elements then it would not satisfy the defining property of being a subset of both S and T so it is maximal.

If $R = S$, then there is nothing to prove so suppose otherwise. Then $R \prec S$ so $\gamma(R) = a \in S$ for some s. If $R \prec T$ then $\gamma(R) = b \in T$ for some b. But then $a = b \in S \cap T = R$, a contradiction (since $\gamma(R) \notin R$). Thus, $R = S$ or $R = T$ and $\preceq$ is a total ordering.

Since $\preceq$ is a total ordering, we can construct a chain of γ-wosets. Let M be the union of these γ-wosets with the ordering inherited from the wosets. Certainly each γ-woset $S \subseteq M$ so M is maximal.

Finally, we know $M \subseteq Z$. Suppose $Z \subsetneq M$. Then there exists some element $x \in Z \setminus M$. Consider $M \cup \{x\}$. Since $\gamma(\{x\})$ is defined, this set is a γ-woset properly containing M, contradicting the maximality of M. Thus, $M = Z$ so there is a well-ordering on Z. $\square$

Exercise V.3.8. Prove that every nontrivial finitely generated group has a maximal proper subgroup. Prove that $(\mathbb{Q}, +)$ has no maximal proper subgroup.

Solution. Let $\mathscr{S}$ be the set of all proper subgroups of a finitely generated group G. Then $\mathscr{S}$ is partially ordered by inclusion so let $\mathscr{C}$ be a chain in this poset. Let H be the union of all subgroups in this chain. Since the chain is nonempty, there is one subgroup K_0 containing the identity, so H contains the identity. Furthermore, suppose $x, y \in H$. Then there are subgroups K_1, K_2 with $x \in K_1$, $y \in K_2$. Suppose WLOG that $K_1 \subseteq K_2$. Then both $x, y \in K_2$ and since K_2 is a subgroup, $xy^{-1} \in K_2 \subseteq H$. Thus H is a subgroup.

To show H is a proper subgroup, suppose otherwise. In particular, H contains the generators $g_1, g_2, \ldots, g_n$ of G. Then there is some subgroup K_n containing all such generators, implying that $K_n = G$, a contradiction. Thus, H must be proper.

Since every chain in $\mathscr{S}$ has an upper bound in $\mathscr{S}$, Zorn's lemma applies and $\mathscr{S}$ has a maximal element. That is, G has a maximal proper subgroup.

Suppose that $(\mathbb{Q}, +)$ has a maximal proper subgroup H. Then the quotient $\mathbb{Q}/H$ is simple and abelian, so it must be cyclic with prime order. Say $\mathbb{Q}/H \cong \mathbb{Z}/p\mathbb{Z}$. Choose $x \in \mathbb{Q} \setminus H$. Then $H = p(\frac{x}{p} + H) = x + N$, implying that $x \in N$, a contradiction. Thus, $\mathbb{Q}$ has no maximal proper subgroup. $\square$

Exercise V.3.9. Consider the rng (= ring without 1; cf. §III.1.1) consisting of the abelian group $(\mathbb{Q}, +)$ endowed with the trivial multiplication $qr = 0$ for all $q, r \in \mathbb{Q}$. Prove that this rng has no maximal ideals.

Solution. Suppose the ring R has a maximal ideal M. Then M is also a maximal subgroup of $\mathbb{Q}$ (a larger subgroup would also act as an ideal). As shown above, $\mathbb{Q}$ does not contain maximal subgroups so neither can M be a maximal ideal. $\square$

Exercise V.3.10. As shown in Exercise III.4.17, every maximal ideal in the ring of continuous real-valued functions on a *compact* topological space K consists of the functions vanishing of a point of K.

Prove that there are maximal ideals in the ring of continuous real-value functions on the *real line* that do not correspond to points of the real line in the same fashion. (Hint: Produce a proper ideal that is not contained in any maximal ideal corresponding to a point, and apply Proposition 3.5.)

Solution. I still don't know topology but I imagine the solution uses something about the fact that the real line is not compact (whatever that means). $\square$

Exercise V.3.11. Prove that a UFD R is a PID if and only if every nonzero prime ideal in R is maximal. (Hint: One direction is Proposition III.4.13. For the other, assume that every nonzero prime ideal in a UFD R is maximal, and prove that every maximal ideal in R is principal; then use Proposition 3.5 to relate arbitrary ideals to maximal ideals, and prove that every ideal of R is principal.)

Solution. First suppose that R is a PID and let $I = (a)$ be a nonzero prime ideal. Assume $I \subseteq J$ for an ideal $J = (b)$ of R. Since $a \in (b)$, we have $a = bc$ for some $c \in R$. But since a is prime, we have $b \in (a)$ or $c \in (a)$. In the first case, there is nothing more to prove. In the second, we have $c = da$. Then

$$a = bda \Longrightarrow bd = 1 \Longrightarrow (b) = (1) = R.$$

Thus, I is maximal.

Now let R be a UFD such that every prime ideal is maximal. Let I be a maximal ideal. Then I is also a prime ideal of height 1. By Exercise 2.9, I is principal. Thus, every maximal ideal is principal. Now let I_0 be an arbitrary ideal. It is contained in some maximal ideal $\mathfrak{m}_0 = (a_0)$. In particular, every element admits a factor of a, which is irreducible (by Exercise 1.12). Then we may write $I = a_0 J_0$ for an ideal J_0. If $J_0 = R$ then $I = (a_0)$ and we are done. Otherwise, J_0 is properly contained in a maximal ideal $\mathfrak{m}_1 = (a_1)$ so we may write $J_0 = a_1 J_1$. We may repeat this and it will terminate since the elements of I only have finitely many irreducible factors. When it terminates, we find that $J_t = R$ so $I = (a_0 a_1 \cdots a_t)$. □

Exercise V.3.12. Let R be a commutative ring, and let $I \subseteq R$ be a proper ideal. Prove that the set of prime ideals containing I has minimal elements. (These are the *minimal primes* of I.)

Solution. Consider the set $\mathscr{I}$ of prime ideals of R which contain I. The set is ordered by inclusion so consider a chain $\mathscr{C}$ and let $\mathfrak{B}$ be the intersection of the prime ideals in $\mathscr{C}$. Certainly $I \subseteq \mathfrak{B}$. Now we must check that $\mathfrak{B}$ is in fact prime. Suppose $ab \in \mathfrak{B}$ but neither a nor b is. Then there exist two prime ideals $\mathfrak{p}, \mathfrak{p}'$ such that $a \notin \mathfrak{p}, b \notin \mathfrak{p}'$ and WLOG $\mathfrak{p} \subseteq \mathfrak{p}'$. Then $a, b \notin \mathfrak{p}$ but $ab \in \mathfrak{p}$, contradicting that $\mathfrak{p}$ is prime. Thus, $\mathfrak{B}$ is prime. Since every chain in $\mathscr{I}$ has a lower bound, $\mathscr{I}$ has a minimal element. □

Exercise V.3.13. Let R be a commutative ring, and let N be its nilradical (Exercise III.3.12). Let $r \notin N$.

- Consider the family $\mathscr{F}$ of ideals of R that do not contain any power r^k of r for $k > 0$. Prove that $\mathscr{F}$ has maximal elements.
- Let I be a maximal element of $\mathscr{F}$. Prove that I is prime.
- Conclude $r \notin N \implies r$ is not in the intersection of all prime ideals of R.

Together with Exercise III.4.18, this shows that the nilradical of a commutative ring R equals the intersection of all prime ideals of R.

Solution. Recall that the nilradical of a ring is the set of nilpotent elements (elements a such that $a^n = 0$ for some n). The nilradical is an ideal of R.

The family $\mathscr{F}$ of ideals not containing any power of r^k is ordered by inclusion. Each chain in this family has a maximal element, namely the union of all of the ideals in the chain. Therefore, by Zorn's lemma $\mathscr{F}$ has maximal elements.

Let I be a maximal element of $\mathscr{F}$ and suppose $ab \in I$ but $a, b \notin I$. Then the ideals $I + (a)$ and $I + (b)$ both properly contain I. By the maximality of I, we have $r^m \in I + (a)$ and $r^n \in I + (b)$. But then we find

$$r^{m+n} = (s_1 + ax)(s_2 + by) = s_1 s_2 + s_1 \cdot by + ax \cdot s_2 + ax \cdot by \in I$$

for $s_1, s_2 \in I$, a contradiction. Thus one of $a, b \in I$ so I is prime.

Suppose r is not in the nilradical of R. Then there is some prime ideal not containing any power of r, so r is not in the intersection of all prime ideals. In particular, $\bigcap \mathfrak{p} \subseteq N$. $\square$

Exercise V.3.14. The *Jacobson radical* of a commutative ring R is the intersection of the maximal ideals in R. (Thus, the Jacobson radical contains the nilradical.) Prove that r is in the Jacobson radical if and only if $1 + rs$ is invertible for every $s \in R$.

Solution. If r is in the Jacobson radical, then it is in every maximal ideal. Suppose there exists some $s \in R$ such that $1 + rs$ is not invertible. Then $(1 + rs)$ is a proper ideal and hence is contained in a maximal ideal $\mathfrak{m}$. But $r \in \mathfrak{m}$ so $1 = rs - r \cdot s \in \mathfrak{m}$, a contradiction. Thus $1 + rs$ is invertible for all $s \in R$.

Now suppose that $1 + rs$ is invertible for all $s \in R$ and let $\mathfrak{m}$ be a maximal ideal. If $r \notin \mathfrak{m}$ then $\mathfrak{m} + (r) = R$ so there exists $y \in \mathfrak{m}$ and $s \in (r)$ such that $rs + y = 1$. But then $y = 1 - rs$ is invertible so $1 = yy^{-1} \in \mathfrak{m}$, a contradiction. Thus, $r \in \mathfrak{m}$. $\square$

Exercise V.3.15. Recall that a (commutative) ring R is Noetherian if every ideal of R is finitely generated. Assume the seemingly weaker condition that every *prime* ideal of R is finitely generated. Let $\mathscr{F}$ be the family of ideals that are not finitely generated in R. You will prove $\mathscr{F} = \emptyset$.

- If $\mathscr{F} \neq 0$, prove that it has a maximal element I.
- Prove that R/I is Noetherian.
- Prove that there are ideals J_1, J_2 properly containing I, such that $J_1 J_2 \subseteq I$.
- Give a structure of R/I module to $I/J_1 J_2$ and $J_1/J_1 J_2$.
- Prove that $I/J_1 J_2$ is a finitely generated R/I-module.
- Prove that I is finitely generated, thereby reaching a contradiction.

Thus, a ring is Noetherian if and only if its *prime* ideals are finitely generated.

Solution. If $\mathscr{F}$ is nonempty, it is partially ordered by inclusion. For each chain $\mathscr{C}$ in $\mathscr{F}$, the ideal defined as the union of ideals in the chain is an upper bound for $\mathscr{C}$. Indeed, if it were finitely generated then the generating set would be contained in one of the ideals, contradicting the assumption that ideals in $\mathscr{F}$ are not finitely generated. By Zorn's lemma, $\mathscr{F}$ has maximal elements. Let I be one such maximal element.

Suppose R/I is not Noetherian. That is, there is some ideal of the form J/I which is not finitely generated. Then J is an ideal of R containing I and it is not finitely generated. But by the maximality of I, we have $J = R$ which is finitely generated by 1, a contradiction. Thus R/I is Noetherian.

Since I is not finitely generated, it is not prime. Thus, there exist elements $a, b \notin I$ with $ab \in I$. Then $J_1 = I + (a)$ and $J_2 = I + (b)$ both properly contain I (and thus are finitely generated) and elements of $J_1 J_2$ are of the form

$$(r_1 + ax)(r_2 + by) = r_1 \cdot r_2 + r_1 \cdot by + r_2 \cdot ax + ab \cdot xy \in I,$$

so $J_1 J_2 \subseteq I$.

We can give the quotient $I/J_1 J_2$ the structure of an R/I module by defining

$$(r + I)x = rx$$

for $r \in R$ and $x \in I/J_1 J_2$. Indeed, since $x = a + J_1 J_2$ for $a \in I$, we find

$$r(a + J_1 J_2) = ra + rJ_1 J_2 \in \frac{I}{J_1 J_2}$$

The other module axioms can be checked easily. We can define the same structure on $J_1/J_1 J_2$.

Recall that J_1 is finitely generated. Then $J_1/J_1 J_2$ is also finitely generated over R and hence over R/I. Since R/I is Noetherian and $I/J_1 J_2$ is a submodule of $J_1/J_1 J_2$, we find that $I/J_1 J_2$ is finitely generated.

Finally, observe that $J_1 J_2 \subseteq I$ is finitely generated and $I/J_1 J_2$ is finitely generated. Thus, I is finitely generated and we arrive at a contradiction. Therefore, a ring is Noetherian if and only if its prime ideals are finitely generated. □

V.4 Unique factorization in polynomial rings

Exercise V.4.1. Prove Lemma 4.1.

Lemma 4.1. *Let R be a ring, and let I be an ideal of R. Then*

$$\frac{R[x]}{IR[x]} \cong \frac{R}{I}[x].$$

Solution. The map from $R \to R/I$ induces a map from $R[x]$ to $R/I[x]$ which sends the coefficients of each polynomial to their coset. Clearly this map is surjective. Its kernel is the set of polynomials whose coefficients are in I. That is, the kernel is $IR[x]$. The isomorphism follows. □

Exercise V.4.2. Let R be a ring, and let I be an ideal of R. Prove or disprove that if I is maximal in R, then $IR[x]$ is maximal in $R[x]$.

Solution. If I is maximal in R, then R/I is a field. By Lemma 4.1, the ring $R[x]/IR[x]$ is a polynomial ring over a field, or a PID. In particular, the polynomial $f(x) = x$ has no inverse so the ring is not a field and $IR[x]$ is not maximal in $R[x]$. It is, however, prime in $R[x]$ which is interesting in its own right. $\square$

Exercise V.4.3. Let R be a PID, and let $f \in R[x]$. Prove that f is primitive if and only if it is very primitive. Prove that this is not necessarily the case in an arbitrary UFD.

Solution. If f is primitive, then for all principal prime ideals $\mathfrak{p}$, $f \notin \mathfrak{p}R[x]$. Since R is a PID, every prime ideal is principal. Thus, f is very primitive. The other direction follows from the definition.

For a counterexample in the more general case, consider the UFD $\mathbb{Z}[x]$ (note that we are only told this in §5.2 but we haven't proven it yet). Let $f = x + y \in \mathbb{Z}[x][y]$. Then f is primitive because $\gcd(x, y) = 1$ but $1 \notin (x, y)$ so $(x, y) \neq (1)$. In general, $d = \gcd(a_0, \dots, a_d)$ does not imply that $(d) = (a_0, \dots, a_d)$. $\square$

Exercise V.4.4. Let R be a commutative ring, and let $f, g \in R[x]$. Prove that

$$fg \text{ is very primitive} \iff \text{both } f \text{ and } g \text{ are very primitive.}$$

Solution. Suppose fg is very primitive. Then for all prime ideals $\mathfrak{p}$ in R, $fg \notin \mathfrak{p}R[x]$. That is, $f \notin \mathfrak{p}R[x]$ and $g \notin \mathfrak{p}R[x]$, or f is very primitive and g is very primitive. An equivalent reasoning proves the reverse direction. $\square$

Exercise V.4.5. Prove Lemma 4.7.

Lemma 4.7. *Let R be a UFD, and let $f \in R[x]$. Then*

- $(f) = (\mathrm{cont}_f)(\underline{f})$, *where $\underline{f}$ is primitive;*
- *if $(f) = (c)(g)$, with $c \in R$ and g primitive, then $(c) = (\mathrm{cont}_f)$.*

Solution. Recall that cont_f is the gcd of the coefficients of f. Let $\underline{f}$ be the polynomial obtained by dividing each coefficient of f by cont_f. Then $(\mathrm{cont}_{\underline{f}}) = (1)$ since the remaining coefficients have no common factors. Thus, $\underline{f}$ is primitive and $(f) = (\mathrm{cont}_f)(\underline{f})$.

For the second point, note that we have $f = ucg$ for some unit $u \in R$. Then $\mathrm{cont}_f = \mathrm{cont}_{ucg} = uc$ since g is primitive. But then $(c) = (uc) = (\mathrm{cont}_f)$. $\square$

Exercise V.4.6. Let R be a PID, and let K be its field of fractions.

- Prove that every element $c \in K$ can be written as a finite sum
$$c = \sum_i \frac{a_i}{p_i^{r_i}}$$
where the p_i are nonassociate irreducible elements in R, $r_i \geq 0$, and a_i, p_i are relatively prime.

- If $\sum_i \frac{a_i}{p_i^{r_i}} = \sum_j \frac{b_j}{q_j^{s_j}}$ are two such expressions, prove that (up to reshuffling) $p_i = q_i$, $r_i = s_i$, and $a_i \equiv b_i \mod p_i^{r_i}$.

- Relate this to the process of integration by 'partial fractions' you learned about when you took calculus.

Solution. Since R is a PID, it is in particular a UFD. Consider an element $c = \frac{x}{y}$. Then y has a unique factorization into non-associate irreducible elements (the p_i). Then we can write
$$\frac{x}{y} = \sum_i \frac{a_i}{p_i^{r_i}}$$
where the sum is guaranteed to have the same denominator by the way in which addition is defined in the field of fractions. To determine the a_i, note that expanding the sum on the right side yields a numerator whose terms are relatively prime. Thus, their gcd is a unit and since R is a PID, Bezout's identity holds. That is, there is a set of elements $a_1, \dots, a_n$ which satisfy the equation $u = a_1 x_1 + \cdots + a_n x_n$ where x_i is y divided by the i-th irreducible factor and u is some unit. Multiplying both sides by $u^{-1}x$ yields a set of a_i which satisfy the equation above. Furthermore, they must be relatively prime to their corresponding p_i or the product with x_i would simply yield y.

With regards to the second point, I don't know that the expressions are always equivalent if the unique factorization of y is multiplied by a unit. However, the process described is precisely what occurs in partial fraction decomposition. Since R is a field, $R[x]$ is a PID. The elements of its field of fractions K can be written as above. $\square$

Exercise V.4.7. A subset S of a commutative ring R is a *multiplicative subset* (or *multiplicatively closed*) if (i) $1 \in S$ and (ii) $s, t \in S \implies st \in S$. Define a relation on the set of pairs (a, s) with $a \in R, s \in S$ as follows:
$$(a, s) \sim (a', s') \iff (\exists t \in S), t(s'a - sa') = 0.$$
Note that if R is an integral domain and $S = R \setminus 0$, then S is a multiplicative subset, and the relation agrees with the relation introduced in §4.2.

- Prove that the relation $\sim$ is an *equivalence* relation.

- Denote by $\frac{a}{s}$ the equivalence class of (a, s), and define the same operations $+, \cdot$ on such 'fractions' as the ones introduced in the special case of §4.2. Prove that these operations are well-defined.

- The set $S^{-1}R$ of fractions, endowed with the operations $+, \cdot$, is the *localization of R at the multiplicative subset S*. Prove that $S^{-1}R$ is a commutative ring and that the function $a \mapsto \frac{a}{1}$ defines a ring homomorphism $\ell : R \to S^{-1}R$.
- Prove that $\ell(s)$ is invertible for every $s \in S$.
- Prove that $R \to S^{-1}R$ is initial among ring homomorphisms $f : R \to R'$ such that $f(s)$ is invertible in R' for every $s \in S$.
- Prove that $S^{-1}R$ is an integral domain if R is an integral domain.
- Prove that $S^{-1}R$ is the zero-ring if and only if $0 \in S$.

Solution. The relation is clearly reflexive. Let $t = 1$ and we find $t(sa - sa) = 0$ so $(a, s) \sim (a, s)$. Now suppose $(a, s) \sim (a', s')$. That is, there is a $t \in S$ such that $t(s'a - sa') = 0$. But then $-t(sa' - s'a) = 0$ so $t(sa' - s'a) = 0$. Thus, $(a', s') \sim (a, s)$. Finally, suppose $(a, s) \sim (a', s')$ and $(a', s') \sim (a'', s'')$. We have $t_1(s'a - sa') = 0$ and $t_2(s''a' - s'a'') = 0$. Then

$$s't_1t_2(s''a - sa'') = t_2s'' \cdot t_1(s'a - sa') + t_1s \cdot t_2(s''a' - s'a'') = 0$$

so the relation is transitive and hence an equivalence relation.

To verify that the operations are well-defined, suppose $(a_1, s_1) \sim (a_2, s_2)$. Then

$$t\left((s'a_1 + s_1a')(s_2s') - (s'a_2 - s_2a')(s_1s')\right) = (s')^2 \cdot t(a_1s_2 - a_2s_1) = 0$$

so addition is well-defined. Similarly,

$$t\left((s_2s')(a_1a') - (s_1s')(a_2a')\right) = a's' \cdot t(s_2a_1 - s_1a_2) = 0$$

so multiplication is well-defined.

To show that $S^{-1}R$ is a commutative ring, let $+, \cdot$ be the operations on the set of fractions. Clearly the set under $+$ forms a group with additive identity $\frac{0}{1}$ and inverses $-\frac{a}{s}$. Furthermore, we have

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + sa'}{ss'} = \frac{sa' + s'a}{s's} = \frac{a'}{s'} + \frac{a}{s}$$

so this group is abelian. Similarly, multiplication is commutative (assuming R is commutative). Lastly, we can see that distributivity holds since

$$\frac{a}{r}\left(\frac{b}{s} + \frac{c}{t}\right) = \frac{a}{r}\frac{(bt + cs)}{st} = \frac{abt}{rst} + \frac{acs}{rst} = \frac{a}{r} \cdot \frac{b}{s} + \frac{a}{r} \cdot \frac{c}{t}.$$

It is easy to verify that ℓ is a ring homomorphism since $\ell(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \ell(a) + \ell(b)$ and $\ell(a \cdot b) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = \ell(a) \cdot \ell(b)$. The identity is also preserved.

If $s \in S$, then $\ell(s) = \frac{s}{1}$. But we have $\frac{s}{1} \cdot \frac{1}{s} = 1$ and $\frac{1}{s} \in S^{-1}R$ since $s \in S$. Thus, $\ell(s)$ is invertible.

To prove that $R \to S^{-1}R$ is initial among homomorphisms $f : R \to R'$ such that $f(s)$ is invertible in R' for $s \in S$, we need to define an induced homomorphism $\hat{f} : S^{-1}R \to R'$ such that the diagram

$$\begin{tikzcd}
S^{-1}R \arrow[rr, "\hat{f}"] & & R' \\
& R \arrow[ul, "\ell"] \arrow[ur, "f"'] &
\end{tikzcd}$$

commutes, and we must require that $\hat{f}$ is unique. Note that if $\hat{f}$ exists then we must have

$$\hat{f}\left(\frac{a}{s}\right) = \hat{f}\left(\frac{a}{1}\right)\hat{f}\left(\frac{1}{s}\right) = \hat{f}(\ell(a))\hat{f}(\ell(s)^{-1}) = f(a)f(s)^{-1}$$

so the definition of $\hat{f}$ is unique. Furthermore, the definition $\hat{f}\left(\frac{a}{s}\right) = f(a)f(s)^{-1}$ is in fact a well-defined ring homomorphism from $S^{-1}R$ to R', showing that ℓ is initial.

Suppose that $S^{-1}R$ is not an integral domain. That is, there exist nonzero $\frac{a_1}{s_1}, \frac{a_2}{s_2}$ whose product is zero. That is, we have

$$\frac{a_1a_2}{s_1s_2} = \frac{0}{1} \Longrightarrow (\exists t \in S), t(a_1a_2) = 0$$

which can only occur if R is not an integral domain. The contrapositive is that if R is an integral domain then so is $S^{-1}R$.

First assume $0 \in S$. Then $\ell(0)$ is invertible in $S^{-1}R$, say its inverse is r. But then we have $\ell(0)r = 0 \cdot r = 1$ so $0 = 1$ implying that $S^{-1}R$ is the zero-ring. Now suppose $0 \notin S$. Then 0 is not invertible in $S^{-1}R$ so $S^{-1}R$ is not the zero ring. $\square$

Exercise V.4.8. Let S be a multiplicative subset of a commutative ring R, as in Exercise 4.7. For every R-module M, define a relation $\sim$ on the set of pairs (m, s), where $m \in M$ and $s \in S$:

$$(m, s) \sim (m', s') \Longleftrightarrow (\exists t \in S), t(s'm - sm') = 0.$$

Prove that this is an equivalence relation, and define an $S^{-1}R$-module structure on the set $S^{-1}M$ of equivalence classes, compatible with the R-module structure on M. The module $S^{-1}M$ is the *localization* of M at S.

Solution. This can be shown to be an equivalence relation in the same manner as above. To define an $S^{-1}R$-module structure on $S^{-1}M$, let

$$\frac{r}{s} \cdot \frac{m}{t} = \frac{r \cdot m}{st}.$$

Clearly this satisfies the definition of a module as

$$\frac{r}{s} \cdot \left(\frac{m_1}{t_1} + \frac{m_2}{t_2} \right) = \frac{r}{s} \cdot \frac{t_2 m_1 + t_1 m_2}{t_1 t_2} = \frac{r}{s} \cdot \frac{m_1}{s_1} + \frac{r}{s} \cdot \frac{m_2}{s_2}$$

The remaining axioms can be checked similarly. Furthermore, it is compatible with the R-module structure on M. $\square$

Exercise V.4.9. Let S be a multiplicative subset of a commutative ring R, and consider the localization operation introduced in Exercises 4.7 and 4.8.

- Prove that if I is an ideal of R such that $I \cap S = \emptyset$, then $I^e := S^{-1}I$ is a proper ideal of $S^{-1}R$.
- If $\ell : R \to S^{-1}R$ is the natural homomorphism, prove that if J is a proper ideal of $S^{-1}R$, then $J^c := \ell^{-1}(J)$ is an ideal of R such that $J^c \cap S = \emptyset$.
- Prove that $(J^c)^e = J$, while $(I^e)^c = \{a \in R \mid (\exists s \in S) sa \in I\}$.
- Find an example showing that $(I^e)^c$ need not equal I, even if $I \cap S = \emptyset$. (Hint: Let $S = \{1, x, x^2, \ldots\}$ in $R = \mathbb{C}[x, y]$. What is $(I^e)^c$ for $I = (xy)$?)

Solution. Clearly $0 \in S^{-1}I$ since $0 \in I$. Now let $\frac{a}{s}, \frac{b}{t} \in I^e$. Then

$$\frac{a}{s} - \frac{b}{t} = \frac{ta - sb}{st} \in I^e$$

since $ta - sb \in I$ and $st \in S$. Furthermore, let $\frac{r}{s} \in S^{-1}R$. Then

$$\frac{r}{s} \cdot \frac{a}{s'} = \frac{ra}{ss'} \in I^e$$

because $ra \in I$. Thus I^e is an ideal of $S^{-1}R$. Clearly it is proper because I does not contain any elements in S. Otherwise we would have $1 = \frac{s}{s} \in I^e$ and I^e would be all of $S^{-1}R$.

Now let J be a proper ideal of $S^{-1}R$. Since $0 \in J$, we have $\ell(0) = 0$ so $0 \in \ell^{-1}(J)$. Now suppose $a, b \in J^c$. Then $a - b = \ell^{-1}(\frac{a}{1}) - \ell^{-1}(\frac{b}{1}) \in J^c$. Similarly, it is closed under multiplication by R. Finally, suppose $J^c \cap S$ is nonempty. Then $\frac{s}{1} \in J$. But then $1 = \frac{1}{s} \cdot \frac{s}{1} \in J$ so J is all of $S^{-1}R$, a contradiction to it being proper. Thus, $J^c \cap S = \emptyset$.

Let $\frac{a}{s} \in (J^c)^e$. Then $\frac{a}{s} \in S^{-1}\ell^{-1}(J)$. In particular, $a \in \ell^{-1}(J)$ so $\frac{a}{1} \in J$. Therefore $\frac{a}{s} \in J$ so $(J^c)^e \subseteq J$. Now suppose $\frac{a}{s} \in J$. Then $a \in \ell^{-1}(J) = J^c$. It follows that $\frac{a}{s} \in (J^c)^e$ so $(J^c)^e = J$. Given an ideal $I \subseteq R$, suppose $a \in (I^e)^c$. Then $\ell(a) = \frac{a}{1} \in I^e = S^{-1}I$. In particular, $a \in I$ so $\subseteq$ holds. Now let $a \in R$ such that there is an $s \in S$ with $sa \in I$. Then $\ell(sa) \in I^e$ so $\frac{a}{1} \in I^e$. But then $a \in \ell^{-1}(I^e)$ showing that $\supseteq$ holds, meaning the two sets are equal.

Using the hint, consider the set $S = \{1, x, x^2, \ldots\}$ in the ring $R = \mathbb{C}[x, y]$. Clearly the ideal $I = (xy)$ does not intersect S since every nonzero element of I contains a factor of y. In fact, this means that $(I^e)^c = (y)$. $\square$

Exercise V.4.10. With notation as in Exercise 4.9, prove that the assignment $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$ gives an inclusion-preserving bijection between the set of *prime* ideals of R disjoint from S and the set of prime ideals of $S^{-1}R$. (Prove that $(\mathfrak{p}^e)^c = \mathfrak{p}$ if $\mathfrak{p}$ is a prime ideal disjoint from S.)

Solution. Let $\mathfrak{p}$ be a prime ideal disjoint from S. First we will show that $\mathfrak{p}^e$ is a prime ideal. Let $\frac{r}{s} \cdot \frac{a}{t} \in \mathfrak{p}^e$ with $\frac{r}{s} \notin \mathfrak{p}^e$. That is, $ra \in \mathfrak{p}$ but $r \notin \mathfrak{p}$ so $a \in \mathfrak{p}$. Since $t \in S$, we have $\frac{a}{t} \in \mathfrak{p}^e$, showing that it is prime. Now we must show the assignment is a bijection. Recall that $(\mathfrak{p}^e)^c = \{a \in R \mid (\exists s \in S) sa \in \mathfrak{p}\}$. However, since $s \notin \mathfrak{p}$, $sa \in \mathfrak{p}$ if and only if $a \in \mathfrak{p}$. In particular, $(\mathfrak{p}^e)^c = \mathfrak{p}$. Since $(\mathfrak{p}^c)^e = \mathfrak{p}$ as well, the assignment has a two-sided inverse and is a bijection. Finally, we show the bijection preserves inclusion. Suppose $\mathfrak{p} \subseteq \mathfrak{p}'$. Let $\frac{a}{s} \in \mathfrak{p}^e$. Since $a \in \mathfrak{p}'$ and $s \in S$, we have $\frac{a}{s} \in \mathfrak{p}'^e$. Thus, the inclusion is preserved. □

Exercise V.4.11. A ring is said to be *local* if it has a single maximal ideal.

Let R be a commutative ring, and let $\mathfrak{p}$ be a prime ideal of R. Prove that the set $S = R \setminus \mathfrak{p}$ is multiplicatively closed. The localization $S^{-1}R, S^{-1}M$ are then denoted $R_\mathfrak{p}, M_\mathfrak{p}$.

Prove that there is an inclusion-preserving bijection between the prime ideals of $R_\mathfrak{p}$ and the prime ideals of R contained in $\mathfrak{p}$. Deduce that $R_\mathfrak{p}$ is a local ring.

Solution. Since $\mathfrak{p}$ is a proper ideal, we have $1 \in R \setminus \mathfrak{p}$. Suppose $s, t \in S$. If $st \in \mathfrak{p}$ then one of $s, t \in \mathfrak{p}$, a contradiction. Thus, $st \in S$ so it is multiplicatively closed.

The assignment defined in Exercise 4.10 yields the desired inclusion-preserving bijection since a prime ideal contained in $\mathfrak{p}$ is obviously disjoint from S. Thus, the only maximal ideal is $\mathfrak{p}^e$. To show this, let I be an ideal in $R_\mathfrak{p}$. Then I is contained in some maximal ideal. If $\frac{a}{b} \in I$ with $a, b \in R \setminus \mathfrak{p}$ then $\frac{b}{a} \in R \setminus p$ so $\frac{a}{b} \cdot \frac{b}{a} = 1 \in I$ so $I = R_\mathfrak{p}$. Thus, $\mathfrak{p}R_\mathfrak{p}$ is the unique maximal ideal, meaning $R_\mathfrak{p}$ is a local ring. □

Exercise V.4.12. Let R be a commutative ring, and let M be an R-module. Prove that the following are equivalent:

- $M = 0$.
- $M_\mathfrak{p} = 0$ for every prime ideal $\mathfrak{p}$.
- $M_\mathfrak{m} = 0$ for every maximal ideal $\mathfrak{m}$.

(Hint: For the interesting implication, suppose that $m \neq 0$ in M; then the ideal $\{r \in R \mid rm = 0\}$ is proper. By Proposition 3.5, it is contained in a maximal ideal $\mathfrak{m}$. What can you say about $M_\mathfrak{m}$.

Solution. Suppose $M = 0$. For a prime ideal $\mathfrak{p}$, we have $M_{\mathfrak{p}} = \{\frac{a}{b} \mid a \in M, b \in R \setminus \mathfrak{p}\} = \{0\}$ since the only element of M is 0. The second statement clearly implies the third since every maximal ideal $\mathfrak{m}$ is prime. To show the third point implies the first, suppose $m \neq 0$ in M. The ideal specified in the hint is proper so it is contained in a maximal ideal $\mathfrak{m}$. Then $M_{\mathfrak{m}} = \{\frac{a}{b} \mid a \in M, b \in R \setminus \mathfrak{m}\}$ contains the nonzero element $\frac{m}{1}$. Thus, if $M_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$, then $M = 0$, showing that all of the listed properties are equivalent. □

Exercise V.4.13. Let k be a field, and let v be a discrete valuation on k. Let R be the corresponding DVR, with local parameter t (see Exercise 2.20).

- Prove that R is local, with maximal ideal $\mathfrak{m} = (t)$. (Hint: Note that every element of $R \setminus \mathfrak{m}$ is invertible.)
- Prove that k is the field of fractions of R.
- Now let A be a PID, and let $\mathfrak{p}$ be a prime ideal in A. Prove that the localization $A_{\mathfrak{p}}$ is a DVR. (Hint: If $\mathfrak{p} = (p)$, define a valuation on the field of fractions of A in terms of 'divisibility by p'.)

Solution. First, recall that a local parameter $t \in R$ is an element such that $v(t) = 1$. We have shown in Exercise 2.20 that local parameters have the property that for any nonzero ideal I of R, we have $I = (t^k)$ for some $k \geq 1$. Thus, $I \subseteq (t)$ so (t) is the unique maximal ideal and R is local. Alternatively, suppose $a \in I$ is not divisible by t. If $v(a) > 0$ then $v(a/t) = v(a) - v(t) \geq 0$ so $a/t \in R$. Thus, $v(a) = 0$. Furthermore, $v(a^{-1}) = -v(a) = 0$ so $a^{-1} \in R$ and a is invertible. Therefore, $1 = a \cdot a^{-1} \in I$ so $I = R$.

Let K denote the field of fractions of R. There is an obvious embedding $f : R \to k$ so by the universal property of the field of fractions, there is an injective homomorphism $\hat{f} : K \to k$. To show the fields are isomorphic, we construct an explicit isomorphism. Consider $g : k \to K$ letting $g(a) = \frac{a}{1}$. Clearly g is a homomorphism so it is injective. To show that it is surjective, let $\frac{a}{b} \in K$. Then $\frac{a}{b} = \frac{ab^{-1}}{bb^{-1}} = g(ab^{-1})$ so the image of g is all of K. Thus, k is the field of fractions of R.

Let $\mathfrak{p} = (p)$. The localization $A_{\mathfrak{p}} = \{\frac{a}{b} \mid a \in A, b \in A \setminus \mathfrak{p}\}$. Since A is a PID, it is also a UFD so elements of $A_{\mathfrak{p}}$ can be expressed as $\frac{p^k a'}{b}$ for some $k \geq 0$. This is a generalization of the p-adic valuation defined over the rationals in Exercise 2.19. □

Exercise V.4.14. With notation as in Exercise 4.8, define operations $N \mapsto N^e$ and $\hat{N} \mapsto \hat{N}^c$ for submodules $N \subseteq M$, $\hat{N} \subseteq S^{-1}M$, respectively, analogously to the operations defined in Exercise 4.9. Prove that $(\hat{N})^c)^e = \hat{N}$. Prove that every localization of a Noetherian module is Noetherian.

In particular, all localizations $S^{-1}R$ of a Noetherian ring are Noetherian.

Solution. Let $\frac{a}{s} \in \hat{N}$. Then $a \in \ell^{-1}(\hat{N})$ so $\frac{a}{s} \in (\hat{N}^c)^e$. Now suppose $\frac{a}{s} \in (\hat{N}^c)^e$. Then $a \in \hat{N}^c$ so $a \in \ell^{-1}(\hat{N})$. That is, $\frac{a}{1} \in \hat{N}$. But then $\frac{1}{s} \cdot \frac{a}{1} = \frac{a}{s} \in \hat{N}$. Thus, $(\hat{N}^c)^e = \hat{N}$.

Consider a chain of ascending submodules

$$S^{-1}M_1 \subset S^{-1}M_2 \subset \cdots$$

of $S^{-1}N$ for some Noetherian module N. Then we can take the mapping $\hat{N} \mapsto \hat{N}^c$ for each submodule in the chain to obtain the chain

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

which stabilizes since N is Noetherian. Thus, the original chain also stabilizes and $S^{-1}N$ is Noetherian. □

Exercise V.4.15. Let R be a UFD, and let S be a multiplicatively closed subset of R (cf. Exercise 4.7).

- Prove that if q is irreducible in R, then $q/1$ is either irreducible or a unit in $S^{-1}R$.
- Prove that if a/s is irreducible in $S^{-1}R$, then a/s is an associate of $q/1$ for some irreducible element q of R.
- Prove that $S^{-1}R$ is also a UFD.

Solution. Let q be an irreducible element of R. If q divides some element of S, say $s = qr$, then $q/1$ is a unit because

$$\frac{q}{1} \cdot \frac{r}{s} = \frac{qr}{s} = 1.$$

Now suppose q does not divide any element of S. If $q/1$ factorizes in $S^{-1}R$, then we have $\frac{q}{1} = \frac{a}{s} \cdot \frac{b}{s'}$. That is, there is some $t \in S$ such that

$$tqss' = tab.$$

Since R is a UFD, and there is only one factor of q on the left hand side, there is also only one factor of q on the right hand side. WLOG, say q divides a. Then the irreducible elements in the factorization of b divide elements of S. Thus $\frac{b}{s'}$ is a unit (by case one) and $\frac{1}{q}$ is irreducible.

Consider a factorization $\frac{a}{s} = \frac{q}{1} \cdot \frac{b}{t}$ for some irreducible element q. Since $\frac{a}{s}$ is irreducible, one of the factors is a unit. If $\frac{b}{t}$ is a unit, then $(\frac{q}{1}) = (\frac{a}{s})$. If $\frac{q}{1}$ is a unit, then so is $\frac{q}{t}$. In particular, we can rewrite the factorization as $\frac{a}{s} = \frac{q}{t} \cdot \frac{b}{1}$. Finally, b is irreducible in R because if it were not then $\frac{b}{1}$ would not be irreducible in $S^{-1}R$. Thus, $(\frac{a}{s}) = (\frac{b}{1})$ for an irreducible b.

Let $\frac{a}{s} \in S^{-1}R$. Suppose $a = u(p_1^{b_1} \cdots p_r^{b_r})(q_1^{c_1} \cdots q_t^{c_t})$ where the p_i are irreducible elements which divide elements in S and the q_i are irreducible elements which do not divide elements in S. Then we have

$$\frac{a}{s} = \frac{u}{s} \cdot \frac{p_1^{b_1}}{1} \cdots \frac{p_r^{b_r}}{1} \cdot \frac{q_1^{c_1}}{1} \cdots \frac{q_t^{c_t}}{1}$$

is a factorization of $\frac{a}{s}$ into a unit multiplied by a product of irreducibles (by the first point). Uniqueness follows from multiplying factors by a unit and using the second point. $\square$

Exercise V.4.16. Let R be a Noetherian integral domain, and let $s \in R$, $s \neq 0$, be a prime element. Consider the multiplicatively closed subset $S = \{1, s, s^2, \ldots\}$. Prove that R is a UFD if and only if $S^{-1}R$ is a UFD. (Hint: By Exercise 2.10, it suffices to show that every prime of height 1 is principal. Use Exercise 4.10 to relate prime ideals in R to prime ideals in the localization.)

On the basis of results such as this and of Exercise 4.15, one might suspect that being factorial is a local property, that is, that R is a UFD if and only if $R_{\mathfrak{p}}$ is a UFD for all primes $\mathfrak{p}$, if and only if $R_{\mathfrak{m}}$ is a UFD for all maximals $\mathfrak{m}$. This is regrettably not the case. A ring R is *locally factorial* if $R_{\mathfrak{m}}$ is a UFD for all maximal ideals $\mathfrak{m}$; factorial implies locally factorial by Exercise 4.15, but locally factorial rings that are not factorial do exist.

Solution. We have shown that if R is a UFD then $S^{-1}R$ is also a UFD. To show the converse, let $\mathfrak{p}$ be a prime ideal of height 1 in R. There is a corresponding prime ideal $\mathfrak{p}^e \in S^{-1}R$ which also has height 1. If $S^{-1}R$ is a UFD then $\mathfrak{p}^e$ is principal. But then $\mathfrak{p}$ is principal as well, so R is a UFD. $\square$

Exercise V.4.17. Let F be a field, and recall the notion of *characteristic* of a ring; the characteristic of a field is either 0 or a prime integer (Exercise III.3.14.)

- Show that F has characteristic 0 if and only if it contains a copy of $\mathbb{Q}$ and that F has characteristic p if and only if it contains a copy of the field $\mathbb{Z}/p\mathbb{Z}$.
- Show that (in both cases) this determines the smallest subfield of F; it is called the *prime subfield* of F.

Solution. Recall that the characteristic of a ring is the smallest nonnegative integer such that $n \cdot 1 = 0$. Suppose a field F contains a copy of $\mathbb{Q}$ and consider the homomorphism $f : \mathbb{Z} \to F$, $f(a) = a \cdot 1$. Let n denote the characterstic of the ring. If $n > 0$ then $f(n) = n \cdot 1 = 0$. However, $n \neq 0$ in F since $n \neq 0$ in $\mathbb{Q}$. Therefore, $n = 0$. Now suppose F has characteristic 0. Then there is an injective homomorphism $f : \mathbb{Z} \to F$. That is, there is an embedding of $\mathbb{Z}$ into K so K contains the inverses of the integers as well. Thus, K contains the field of fractions of $\mathbb{Z}$ which is isomorphic to $\mathbb{Q}$.

Now suppose a field F contains $\mathbb{Z}/p\mathbb{Z}$ and consider the homomorphism $f : \mathbb{Z} \to F, f(a) = a \cdot 1$. Let n denote the characteristic of F. Then $n \leq p$ since $f(p) = p \cdot 1 = 0$. If $n < p$ and $n \cdot 1 = 0$, we arrive at a contradiction since this does not hold in $\mathbb{Z}/p\mathbb{Z}$. Thus, $n = p$. Now suppose F has characteristic p and consider the homomorphism $f : \mathbb{Z} \to F$. The homomorphism has kernel $p\mathbb{Z}$. By the first isomorphism theorem,

$$\frac{\mathbb{Z}}{p\mathbb{Z}} \cong \mathrm{im} f \subseteq F$$

completing the proof. Note that in both cases, the desired subfield is generated by 1.

Consider the intersection of all subfields of F, denoted by K. Certainly $1 \in K$. If $\mathrm{char}(F) = p$ then K contains the subfield generated by 1 which we have shown is isomorphic $\mathbb{Z}/p\mathbb{Z}$. Similarly, if $\mathrm{char}(F) = 0$ then K contains $\mathbb{Z}$ and its multiplicative inverses which is isomorphic to $\mathbb{Q}$. The reverse inclusion is obvious, completing the proof. □

Exercise V.4.18. Let R be an integral domain. Prove that the invertible elements in $R[x]$ are the units of R, viewed as constant polynomials.

Solution. Certainly the units of R are invertible in $R[x]$. To show that these are the only invertible elements, suppose $fg = 1$. Since R is a domain, we have the identity $\deg(fg) = \deg(f) + \deg(g)$. It follows that f and g are constant and thus are units in R. □

Exercise V.4.19. An element $a \in R$ in a ring is said to be *nilpotent* if $a^n = 0$ for some $n \geq 0$. Prove that if a is nilpotent, then $1 + a$ is a unit in R.

Solution. Suppose a is nilpotent, say $a^n = 0$. Then

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

so $1 + a$ is invertible. □

Exercise V.4.20. Generalize the result of Exercise 4.18 as follows: let R be a commutative ring, and let $f = a_0 + a_1x + \cdots + a_dx^d \in R[x]$; prove that f is a unit in $R[x]$ if and only if a_0 is a unit in R and $a_1, \ldots, a_d$ are nilpotent. (Hint: If $b_0 + b_1x + \cdots + b_ex^e$ is the inverse of f, show by induction that $a_d^{i+1}b_{e-i} = 0$ for all $i \geq 0$, and deduce that a_d is nilpotent.)

Solution. First, note that if an element a is nilpotent, then so is ra for all $r \in R$. Furthermore, given a unit a_0 and a nilpotent element a_1, we have $a_0 + a_1 = a_0(1 + a_0^{-1}a_1)$ which is the product of two units and thus a unit itself.

We do a proof by induction for both directions. Suppose a_0 is a unit and a_i is nilpotent for $i > 0$. In the case $n = 1$, we have shown above that $a_0 + a_1x$ is a unit. Now suppose this holds for $n = k$ and let $n = k + 1$. Consider the polynomial $p(x) = a_0 + a_1x + \cdots a_{k+1}x^{k+1}$. By the hypothesis, $f(x) = a_0 + a_1x + \cdots a_kx^k$ is a unit. Furthermore, $a_{k+1}x^{k+1}$ is nilpotent. Since the sum of a unit and a nilpotent element is a unit, $p(x)$ must be a unit.

For the reverse direction, suppose f is a unit with inverse g. Clearly $a_0b_0 = 1$. Thus, a_0 and b_0 are both units. To show that $a_d^{i+1}b_{e-i} = 0$ for $i \geq 0$, we induct on i. For the case $i = 0$, the statement clearly holds as a_db_e is the leading term of fg. For $i > 0$, the coefficient of x^{d+e-i} is

$$a_db_{e-i} + a_{d-1}b_{e-i+1} + \cdots + a_{d-i}b_e.$$

Multiplying through by a_d^i and applying the induction hypothesis proves the result. In particular, letting $i = e$ and using the fact that b_0 is a unit shows that a_d is nilpotent. Therefore $f - a_dx^d$ is a unit (by the first part of this solution). Repeating allows us to conclude that all a_i for $i > 0$ are nilpotent. $\square$

Exercise V.4.21. Establish the characterization of irreducible polynomials over a UFD given in Corollary 4.17.

Corollary 4.17. *Let R be a UFD and K the field of fractions of R. Let $f \in R[x]$ be a nonconstant polynomial. Then f is irreducible in $R[x]$ if and only if it is irreducible in $K[x]$ and primitive.*

Solution. One direction is proven in the chapter so we prove the other to establish the characterization. Suppose $f \in R[x]$ is irreducible in $K[x]$ and primitive. Assume $f = gh$ for $g, h \in R[x]$. The irreducibility of f in $K[x]$ implies that one of g, h is a unit in $K[x]$, say g. By Exercise 4.18, g has degree 0 so $\text{cont}(g) = g$. But then $1 = \text{cont}(f) = \text{cont}(g)\text{cont}(h)$ so g is a unit in R, implying that f is irreducible in $R[x]$. $\square$

Exercise V.4.22. Let k be a field, and let f, g be two polynomials in $k[x, y] = k[x][y]$. Prove that if f and g have a nontrivial common factor in $k(x)[y]$, then they have a nontrivial common factor in $k[x, y]$.

Solution. Recall that $k(x)$ is the field of fractions of $k[x]$. Suppose f and g have a nontrivial common factor in $k(x)[y]$, say h. We can choose $c \in k(x)$ such that $h = ch'$ where $h' \in k[x, y]$. But then h' is a nontrivial factor of f and g. $\square$

Exercise V.4.23. Let R be a UFD, K its field of fractions, $f(x) \in R[x]$, and assume $f(x) = \alpha(x)\beta(x)$ with $\alpha(x), \beta(x)$ in $K[x]$. Prove that there exists a $c \in K$ such that $c\alpha(x) \in R[x]$, $c^{-1}\beta(x) \in R[x]$, so that

$$f(x) = (c\alpha(x))(c^{-1}\beta(x))$$

splits $f(x)$ as a product of factors in $R[x]$.

Deduce that if $\alpha(x)\beta(x) = f(x) \in R[x]$ is monic and $\alpha(x) \in K[x]$ is monic, then $\alpha(x), \beta(x)$ are both in $R[x]$ and $\beta(x)$ is also monic.

Solution. First note that if f is not primitive then we can factor out the content and let $c = 1$ so we may assume f is primitive. Let $a, b \in K$ such that

$$\alpha = a\underline{\alpha}, \quad \beta = b\underline{\beta}$$

where $\underline{\alpha}, \underline{\beta}$ are primitive in $R[x]$. Note that by Gauss' lemma, ab is a unit in R. Then there exists a unit $u \in R$ such that $a = b^{-1}u$. Now let $c = a^{-1}$ and $c^{-1} = b^{-1}u$. Then we find $c\alpha = a^{-1}\alpha = \underline{\alpha} \in R[x]$. Similarly, $c^{-1}\beta = b^{-1}u\beta = u\underline{\beta} \in R[x]$. Then we find

$$(c\alpha)(c^{-1}\beta) = u\underline{\alpha}\underline{\beta} = ab\underline{\alpha}\underline{\beta} = f$$

so we are done.

We deduce that if f and α are monic, then β is monic as well so that the leading coefficient of f is 1. Furthermore, suppose $\alpha \notin R[x]$. Then there exists an element $c \in K$ such that $c\alpha \in R[x]$. Note that c is not a unit in R or else $\alpha \in R[x]$. But then the leading coefficient of $c^{-1}\beta$ is c^{-1} so $c^{-1}\beta \notin R[x]$. Similar reasoning shows that both $\alpha, \beta \in R[x]$. □

Exercise V.4.24. In the same situation as in Exercise 4.23, prove that the product of any coefficient of α with any coefficient of β lies in R.

Solution. Let α_i, β_i denote the i-th coefficient of α, β respectively. Using the result of the previous exercise, we have $c\alpha_i, c^{-1}\beta_i \in R$ for all i. Then $\alpha_i\beta_j = c\alpha_i \cdot c^{-1}\beta_j \in R$ for all i, j. □

Exercise V.4.25. Prove *Fermat's last theorem for polynomials:* the equation

$$f^n + g^n = h^n$$

has no solutions in $\mathbb{C}[t]$ for $n > 2$ and f, g, h not all constant. (Hint: First, prove that f, g, h may be assumed to be relatively prime. Next, the polynomial $1 - t^n$ factorizes in $\mathbb{C}[t]$ as $\prod_{i=1}^n (1-\zeta^i t)$ for $\zeta = e^{2\pi i/n}$; deduce that $f^n = \prod_{i=1}^n (h-\zeta^i g)$. Use unique factorization in $\mathbb{C}[t]$ to conclude that each of the factors $h - \zeta^i g$ is an n-th power. Now let $h - g = a^n$, $h - \zeta g = b^n$, $h - \zeta^2 g = c^n$ (this is where the $n > 2$ hypothesis enters). Use this to obtain a relation $(\lambda a)^n + (\mu b)^n = (\nu c)^n$, where λ, μ, ν are suitable complex numbers. What's wrong with this?)

The same pattern of proof would work in any environment where unique factorization is available; if adjoining to $\mathbb{Z}$ a primitive n-th root of 1 and roots of other elements as needed in this argument led to a unique factorization domain, the full-fledged Fermat's last theorem would be as easy to prove as indicated in this exercise. This is not the case, a fact famously missed by G. Lamé as he announced a 'proof' of Fermat's last theorem to the Paris Academy on March 1, 1847.

Solution. First, note that if f, g, h have a common factor c then $(f/c)^n + (g/c)^n = (h/c)^n$ is another solution. Thus, we may assume that f, g, h are relatively prime. If we consider K to be the field of fractions of $\mathbb{C}[t]$ then we have

$$1 - \left(\frac{g}{h}\right)^n = \prod_{i=1}^{n} \left(1 - \zeta^i \frac{g}{h}\right).$$

Multiplying both sides by h^n yields the factorization $f^n = h^n - g^n = \prod_{i=1}^{n}(h - \zeta^i g)$. Now we show that $(h - \zeta^i g)$ is coprime to $(h - \zeta^j g)$ for $i \neq j$. Indeed, we find that

$$h - \zeta^i g - (h - \zeta^j g) = (\zeta^j - \zeta^i) g$$
$$h - \zeta^i g + \frac{\zeta^i}{\zeta^j - \zeta^i} \left(\zeta^j - \zeta^i\right) g = h$$

Since $\mathbb{C}[t]$ is a Euclidean domain, we have $\gcd(h - \zeta^i g, h - \zeta^j g) = \gcd(g, h) = 1$. Thus, the factors are all coprime.

In any UFD, if the product of coprime factors is an n-th power, then each factor is an n-th power. We prove this by induction on the number of prime factors of c which we denote by k. Indeed, suppose a, b are coprime and let $ab = c^n$. If $k = 0$ then c is a unit so a, b are units multiplied by 1^n. If $k > 0$ then there is a prime $p \mid c$ so $p^n \mid c^n = ab$. Therefore, $p^n \mid a$ or $p^n \mid b$ since a, b are coprime. WLOG, assume the latter. We find $a(b/p^n) = (c/p)^n$. Since c/p has fewer prime factors than c, the inductive hypothesis applies and $a = r^n, b/p^n = s^n \implies b = (ps)^n$. Thus, we have shown that we can write $h - g = a^n, h - \zeta g = b^n, h - \zeta^2 g = c^n$ for $a, b, c \in \mathbb{C}[t]$.

With this, we can derive the following.

$$g = \frac{1}{1 - \zeta}(b^n - a^n)$$
$$h = \frac{1}{1 - \zeta}(b^n - \zeta a^n)$$

$$\zeta a^n + (1 + \zeta) b^n = c^n$$

Since $\mathbb{C}$ is an algebraically closed field, there exist $x, y \in \mathbb{C}$ such that $x^n = \zeta$ and $y^n = 1 + \zeta$. Thus, we can write $(ax)^n + (by)^n = c^n$. But then we find $\max(\deg a, \deg b, \deg c) \leq \max(\deg f, \deg g, \deg h)/n < \max(\deg f, \deg g, \deg h)$. If we take a solution f, g, h to the initial equation such that the maximum degree is minimal among all solutions, then we arrive at a contradiction since we have constructed another solution of lower degree. □

V.5 Irreducibility of polynomials

Exercise V.5.1. Let $f(x) \in \mathbb{C}[x]$. Prove that $a \in \mathbb{C}$ is a root of f with multiplicity r if and only if $f(a) = f'(a) = \cdots = f^{(r-1)}(a) = 0$ and $f^{(r)}(a) \neq 0$, where $f^{(k)}(a)$ denotes the value of the k-th derivative of f at a. Deduce that $f(x) \in \mathbb{C}[x]$ has multiple roots if and only if $\gcd(f(x), f'(x)) \neq 1$.

Solution. First suppose that $f(a) = f'(a) = \cdots = f^{(r-1)}(a) = 0$ and $f^{(r)}(a) \neq 0$. Then $(x-a)^{(r)} \mid f(x)$. If $(x-a)^{(r+1)} \mid f(x)$, then repeated differentiation shows that $(x-a) \mid f^{(r)}(x)$ which we know not to be true. Thus, r is the highest power of $(x-a)$ dividing f, showing that a is a root with multiplicity r. For the other direction, suppose a is a root of f with multiplicity r. Then $(x-a)^r \mid f$. Repeatedly differentiation shows that $(x-a) \mid f^{(i)}$ for $0 \leq i < r$. Furthermore, since $(x-a) \nmid f^{(r)}$, we have $f(a) \neq 0$.

Now let $f(x) \in \mathbb{C}[x]$ with multiple roots (that is, roots with multiplicity > 1). If a is a multiple root of f, then $(x-a) \mid f$. Furthermore, we can write $f = (x-a) \cdot g$. Since a is a multiple root, we also have $(x-a) \mid g$. That is, we can write $g = (x-a) \cdot h$. But then we have

$$f'(x) = g(x) + (x-a) \cdot g'(x) = (x-a) \cdot h + (x-a) \cdot g'$$

That is, $\gcd(f, f') \neq 1$ since $(x-a)$ divides both. To prove the reverse direction, suppose all roots of f are simple. Then $f = (x-a_1)(x-a_2)\cdots(x-a_n)$. Taking the derivative shows that the two have no common factors so $\gcd(f, f') = 1$. The contrapositive yields the desired statement. □

Exercise V.5.2. Let F be a subfield of $\mathbb{C}$, and let $f(x)$ be an irreducible polynomial in $F[x]$. Prove that $f(x)$ has no multiple roots in $\mathbb{C}$. (Use Exercises 2.22 and 5.1).

Solution. Suppose $f(x)$ is irreducible in $F[x]$. In particular, $\gcd(f, f') = 1$ in $F[x]$. By Exercise 2.22, $\gcd(f, f') = 1$ in $\mathbb{C}[x]$ as well. But then Exercise 5.1 shows that $f(x)$ has no multiple roots. □

Exercise V.5.3. Let R be a ring, and let $f(x) = a_{2n}x^{2n} + a_{2n-2}x^{2n-2} + \cdots + a_2x^2 + a_0 \in R[x]$ be a polynomial only involving *even* powers of x. Prove that if $g(x)$ is a factor of $f(x)$, so is $g(-x)$.

Solution. Suppose $g(x)$ is a factor of $f(x)$. That is, $f(x) = g(x) \cdot h(x)$. But then

$$f(x) = f(-x) = g(-x) \cdot h(-x)$$

where the first equality follows from the fact that $(-1)^2 = 1$. Thus, $g(-x)$ also divides f. □

Exercise V.5.4. Show that $x^4 + x^2 + 1$ is reducible in $\mathbb{Z}[x]$. Prove that it has *no* rational roots, without finding its (complex) roots.

Solution. Clearly we have

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

so it is reducible in $\mathbb{Z}[x]$. To see that it has no rational roots, we use the rational roots test. The only potential rational roots are ± 1, and it is easily checked that neither are roots. Thus, its roots are not rational. $\square$

Exercise V.5.5. Prove Proposition 5.3.

Proposition 5.3. *Let k be a field. A polynomial $f \in k[x]$ of degree 2 or 3 is irreducible if and only if it has no roots.*

Solution. Let f be a polynomial of degree 2 or 3. If f has a root a, then clearly $(x - a) \mid f$ so f is reducible. The contrapositive yields the statement that if f is irreducible then it has no roots. Now suppose f is reducible. If f has degree 2 then its nontrivial factor must be linear of the form $(x - a)$, making a a root of f. If f has degree 3, then it has a nontrivial factor which is either linear or quadratic. If it is linear then it is a root by the above reasoning. If it is quadratic, then the remaining factor is linear so there is a corresponding root. Thus, we have shown that if f has no roots then it is irreducible. $\square$

Exercise V.5.6. Construct fields with 27 elements and with 121 elements.

Solution. Let $\mathbb{Z}_3$ denote the field with 3 elements and consider the ring $\mathbb{Z}_3[x]$. Consider the polynomial $f(x) = x^3 + 2x + 1$. It can be easily observed that $f(x)$ has no roots in $\mathbb{Z}_3$ and thus is irreducible. Then we can consider the field

$$F := \frac{\mathbb{Z}_3[x]}{x^3 + 2x + 1}.$$

It can be seen to have 27 elements by noting that its elements are quadratic polynomials. That is, each polynomial has three coefficients, and there are three possibilites for each (namely, the elements of $\mathbb{Z}_3$).

Now let $\mathbb{Z}_1 1$ denote the field with 11 elements. Consider the polynomial $f(x) = x^2 + 1$ which has no roots in this field. Then the field

$$F := \frac{\mathbb{Z}_{11}[x]}{x^2 + 1}$$

has elements which are linear polynomials. There are two coefficients in each polynomial and 11 possibilities for each, leading to a total of $11^2 = 121$ elements in this field. $\square$

Exercise V.5.7. Let R be an integral domain, and let $f(x) \in R[x]$ be a polynomial of degree d. Prove that $f(x)$ is determined by its value at any $d + 1$ distinct elements of R.

Solution. Let $g \in R[x]$ be a polynomial of degree d which agrees with f at $d+1$ distinct points. That is, $f(a_1) = g(a_1), \ldots, f(a_{d+1}) = g(a_{d+1})$. Since R is an integral domain, if $f - g$ is nonzero, then it must have degree less than d. Now consider $f - g = c(x-a_1)\cdots(x-a_{d+1})$. We find that $f-g$ has degree $d+1 > d$. Therefore, $f - g = 0$ so $f = g$. ☐

Exercise V.5.8. Let K be a field and let $a_0, \ldots, a_d$ be distinct elements of K. Given any elements $b_0, \ldots, b_d$ in K, construct explicitly a polynomial $f(x) \in K[x]$ of degree at most d such that $f(a_0) = b_0, \ldots, f(a_d) = b_d$, and show that this polynomial is unique. (Hint: First solve the problem assuming that only one b_i is not equal to zero.) This process is called *Lagrange interpolation*.

Solution. Consider the polynomial

$$\ell_j(x) = \prod_{\substack{0 \le i \le d \\ i \ne j}} \frac{x - a_i}{a_j - a_i}.$$

Then we may define the Lagrange polynomial as

$$L(x) = \sum_{j=0}^{k} b_j \ell_j.$$

Clearly this polynomial satisfies the desired properties. Uniqueness can be verified in a similar manner to the previous problem. ☐

Exercise V.5.9. Pretend you can factor integers, and then use Lagrange interpolation (cf. Exercise 5.8) to give a finite algorithm to factor *polynomials* with integer coefficients over $\mathbb{Q}[x]$. Use your algorithm to factor $(x-1)(x-2)(x-3)(x-4)+1$.

Solution. Consider a polynomial $p(x) \in \mathbb{Z}[x]$ of degree d. We can evaluate it at d points, say $p(a_1) = b_1, \ldots, p(a_d) = b_d$. Now factor each b_i over $\mathbb{Z}$. From here, we can use Lagrange Interpolation to construct a polynomial $q(x) \in \mathbb{Q}[x]$ such that $q(a_i) = c_i$ for some factor c_i of b_i. Finally, one may check if $q(x)$ divides p via polynomial division. The key observation is that if q has degree less than d, then it is uniquely determined by the choice of c_i. As a result, there are only finiely many choices for q.

Applying the algorithm to the given polynomial is incredibly tedious but ultimately yields a factorizaiton of $(-x^2 + 5x - 5)^2$. ☐

Exercise V.5.10. Prove that the polynomial $(x-1)(x-2)\cdots(x-n) - 1$ is irreducible in $\mathbb{Q}[x]$ for all $n \ge 1$. (Hint: Think along the lines of Exercise 5.9.)

Solution. Note that $f(x) = (x-1)(x-2)\cdots(x-n) - 1$ is monic. Suppose $f = gh$ has a nontrivial factorization into two monic polynomials of strictly lower degrees. Then, for $1 \leq k \leq n$, we have $f(k) = g(k)h(k) = -1$ so $g(k), h(k) = \pm 1$ and we must have $g(k) = -h(k)$. Now consider the polynomial $p(x) = g(x) + h(x)$. Clearly p has strictly lower degree than f since we are working over an integral domain. However, $p(k) = 0$ for all $1 \leq k \leq n$ so necessarily $f = -g$, a contradiction since we assumed that f and g were both monic. Thus, f must be irreducible. □

Exercise V.5.11. Let F be a finite field. Prove that there are irreducible polynomials in $F[x]$ of arbitrarily high degree. (Hint: Exercise 2.24.)

Solution. Suppose otherwise. That is, suppose there are only finitely many irreducible polynomials in $F[x]$, say $p_1(x), \ldots, p_n(x)$. Consider the polynomial $f(x) = p_1(x)\cdots p_n(x) + 1$. By assumption, $f(x)$ is not irreducible so it is divisibly by one of our irreducible polynomials, say $p_i(x)$. But then $p_i(x)$ divides 1, a contradiction. Therefore, there must be infinitely many irreducible polynomials and they are necessarily of arbitrarily high degree since there are only finitely many polynomials of a fixed degree. □

Exercise V.5.12. Prove that applying the construction in Proposition 5.7 to an irreducible *linear* polynomial in $k[x]$ produces a field isomorphic to k.

Solution. Let f be an irreducible linear polynomial in $k[x]$ and define

$$F = \frac{k[x]}{(f(x))}.$$

Consider the valuation function which sends $g(x) \to g(0) \in F$ (recall that F can be seen as an extension of k). Clearly this mapping preserves sums and products so it suffices to check what the kernel is. The kernel is the set of polynomials such that $g(0) \in (f(x))$. However, note that the valuation functions maps to a constant and the only constant in this ideal is 0. Thus, the kernel is the set of polynomials such that $g(0) = 0$, but this is only the case if $g = 0$ or g has no constant term. Therefore, the kernel is the ideal (x). By the First Isomorphism Theorem, we find

$$F \cong \frac{k[x]}{(x)} \cong k,$$

showing the fields are isomorphic. □

Exercise V.5.13. Let k be a field, and let $f \in k[x]$ be any polynomial. Prove that there is an extension $k \subseteq F$ in which f factors completely as a product of linear terms.

Solution. We can factor f into a product of irreducibles since $k[x]$ is a UFD. For each irreducible element $g_i(t)$ in the factorization of f, we can consider the quotient

$$F_i := \frac{k[t]}{(g_i(t))}$$

where F_i is an extension of k containing a root of $g_i(t)$. Repeating this process for each irreducible factor of f yields a field extension F in which f factors completely. □

Exercise V.5.14. How many different embeddings of the field $\mathbb{Q}[t]/(t^3 - 2)$ are there in $\mathbb{R}$? How many in $\mathbb{C}$?

Solution. There is only one embedding of the field in $\mathbb{R}$, namely $\mathbb{Q}[\sqrt[3]{2}]$. This is because there is only one cube root of 2 in $\mathbb{R}$. However, the field $\mathbb{C}$ contains the roots of unity, solutions to the equation $x^n - 1 = 0$. Thus, there are three embeddings of the field in $\mathbb{C}$, namely $\mathbb{Q}[\sqrt[3]{2}], \mathbb{Q}[\zeta\sqrt[3]{2}], \mathbb{Q}[\zeta^2\sqrt[3]{2}]$, where $\zeta^3 = 1$. □

Exercise V.5.15. Prove Lemma 5.10.

Lemma 5.10. *A field k is algebraically closed if and only if every polynomial $f \in k[x]$ factors completely as a product of linear factors, if and only if every nonconstant polynomial $f \in k[x]$ has a root in k.*

Solution. Suppose k is algebraically closed. That is, every irreducible polynomial has degree 1. Since $k[x]$ is a UFD, every polynomial $f \in k[x]$ factors into irreducibles and thus factors into linear polynomials.

Now suppose that every polynomial $f \in k[x]$ factors completely as a product of linear factors. Then every polynomial has at least one factor of the form $(x - a)$, which occurs if and only if a is a root of f. Therefore, every polynomial has a root in k.

Finally, suppose that every nonconstant polynomial $f \in k[x]$ has a root in k and consider an irreducible polynomial f. Suppose f has degree greater than 1. Since f has a root a, we can factor out a linear polynomial $(x - a)$, contradicting that f is irreducible. Thus f has degree 1 so k is algebraically closed. □

Exercise V.5.16. If you know about the 'maximum modulus principle' in complex analysis: formulate and prove the 'mimimum modulus princile' used in the sketch of the proof of the fundamental theorem of algebra.

Solution. I do not know complex analysis. □

Exercise V.5.17. Let $f \in \mathbb{R}[x]$ be a polynomial of *odd* degree. Use the intermediate value theorem to give an 'algebra-free' proof of the fact that f has real roots.

Solution. We have $\lim_{x\to+\infty} f(x) = +\infty$ and $\lim_{x\to-\infty} f(x) = -\infty$. In particular, for some a, $f(a) < 0$ and for some b, $f(b) > 0$. Since f is a polynomial, it is continuous over $[a, b]$. Thus, the intermediate value theorem applies and there exists some $c \in [a, b]$ such that $f(c) = 0$. That is, c is a real root of f. $\square$

Exercise V.5.18. Let $f \in \mathbb{Z}[x]$ be a cubic polynomial such that $f(0)$ and $f(1)$ are odd and with odd leading coefficient. Prove that f is irreducible in $\mathbb{Q}[x]$.

Solution. Suppose f is reducible. Then it must have a linear factor. However, consider that $x \equiv y \pmod{n} \implies f(x) \equiv f(y) \pmod{n}$. In particular, for any integer x, if $x \equiv 0 \pmod 2$ then $f(x) \equiv 0 \pmod 2$. Similarly, if $x \equiv 1 \pmod 2$ then $f(x) \equiv 1 \pmod 2$. Since $0 \equiv 0 \pmod 2$, it is clear that no integer x is a root of f. Thus, f is irreducible over $\mathbb{Z}[x]$ and hence over $\mathbb{Q}[x]$. $\square$

Exercise V.5.19. Give a proof of the fact that $\sqrt{2}$ is not rational by using Eisenstein's criterion.

Solution. Suppose $\sqrt{2} \in \mathbb{Q}$. Then $(x + \sqrt{2})(x - \sqrt{2}) = x^2 - 2$ is reducible in $\mathbb{Z}[x]$. However, consider the prime ideal $\mathfrak{p} = (2)$. Since $1 \notin (2)$ and $2 \notin (2)^2$, Eisenstein's criterion applies and the polynomial is irreducible in $\mathbb{Z}[x]$. Thus, it must be the case that $\sqrt{2} \notin \mathbb{Q}$. $\square$

Exercise V.5.20. Prove that $x^6 + 4x^3 + 1$ is irreducible by using Eisenstein's criterion.

Solution. Note that there is no prime p which divides 1 so Eisenstein's criterion does not apply to this specific polynomial. However, we can make the substitution $x = y+1$ which yields the polynomial $y^6+6y^5+15y^4+24y^3+27y^2+18y+6$. Note that this polynomial *does* satisfy Eisenstein's criterion with the prime ideal $\mathfrak{p} = (3)$. That is, the polynomial after transformation is irreducible in the ring $\mathbb{Q}[y+1]$. However, this ring is isomorphic to $\mathbb{Q}[x]$. Thus, the original polynomial is also irreducible. $\square$

Exercise V.5.21. Prove that $1 + x + x^2 + \cdots + x^{n-1}$ is reducible over $\mathbb{Z}$ if n is *not* prime.

Solution. Suppose n is not prime so it can be written as $n = pq$. Recall that we have

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{x^n - 1}{x - 1} = \frac{x^{pq} - 1}{x - 1}.$$

However, we find that

$$\frac{(x^p)^q - 1}{x^p - 1} = 1 + x^p + x^{2p} + \cdots + x^{(q-1)p}$$

which yields the factorization

$$\frac{x^n - 1}{x - 1} = \frac{x^n - 1}{x^p - 1} \cdot \frac{x^q - 1}{x - 1}.$$

Thus, the polynomial is reducible over $\mathbb{Z}[x]$. $\square$

Exercise V.5.22. Let R be a UFD, and let $a \in R$ be an element that is not divisible by the square of some irreducible element in its factorization. Prove that $x^n - a$ is irreducible for every integer $n \geq 1$.

Solution. Let q denote an irreducible element whose square does not divide a. Since R is a UFD, q is also prime. Then we have $1 \notin (q)$ and $a \notin (q)^2$. Therefore, Eisenstein's criterion applies and the polynomial is irreducible for all $n \geq 1$. $\square$

Exercise V.5.23. Decide whether $y^5+x^2y^3+x^3y^2+x$ is reducible or irreducible in $\mathbb{C}[x, y]$.

Solution. Consider the ideal $\mathfrak{p} = (x)$. Certainly this is a prime ideal since modding out the ideal yields the ring $\mathbb{C}[y]$ which is an integral domain. Furthermore, we have $1 \notin (x)$, $x^2y^3 \in (x)$, $x^3y^2 \in (x)$, and $x \notin (x)^2$. Thus, we may apply Eisenstein's criterion and conclude that the polynomial is irreducible in $\mathbb{C}[x, y]$. $\square$

V.6 Further remarks and examples

Exercise V.6.1. Generalize the CRT for two ideals, as follows. Let I, J be ideals in a commutative ring R; prove that there is an exact sequence of R-modules

$$0 \longrightarrow I \cap J \longrightarrow R \xrightarrow{\varphi} \frac{R}{I} \times \frac{R}{J} \longrightarrow \frac{R}{I+J} \longrightarrow 0$$

where φ is the natural map. (Also, explain why this implies the first part of Theorem 6.1, for $k = 2$.)

Solution. Let the map for $I \cap J \to R$ be the inclusion. Since it is injective, its kernel is 0 and the first part of the sequence is exact. Furthermore, its image is merely $I \cap J$. Now consider the map φ which sends $r \in R$ to $(r + I,\ r + J)$. Certainly the kernel of this map is the set of elements in R which are in both I and J; that is, the kernel is $I \cap J$. The image of this map is merely the set

$\{r+I,\ r+J) \mid r \in R\}$. Note that this may not be the entirety of $(R/I)\times(R/J)$. Define a map from $(R/I) \times (R/J)$ to $R/(I+J)$ which sends $(a+I, b+J)$ to $a-b+(I+J)$. One can easily verify that this is indeed a homomorphism of modules. Note that the kernel of this image is precisely the image of φ. Furthermore, the homomorphism is surjective; and arbitrary $a+(I+J)$ is mapped to by $(a+I, 0+J)$. With these homomorphisms, we have shown the existence of such an exact sequence of R-modules.

In the case where $I+J=(1)$, then the map φ is surjective. This can be seen by noting that there exist $i \in I$, $j \in J$ such that $i+j=1$. Then for all $(r+I, s+J)$, we have

$$\begin{aligned}
\varphi(rj+si) &= (rj+I, si+J) \\
&= (rj+ri+I, si+sj+J) \\
&= (r(j+i)+I, s(i+j)+J) \\
&= (r+I, s+J).
\end{aligned}$$

Thus, we have recovered the desired statement. □

Exercise V.6.2. Let R be a commutative ring, and let $a \in R$ be an element such that $a^2 = a$. Prove that $R \cong R/(a) \times R/(1-a)$.

Show that the multiplication in R endows the ideal (a) with a *ring* structure, with a as the identity. Prove that $(a) \cong R/(1-a)$ as rings. Prove that $R \cong (a) \times (1-a)$ as rings.

Solution. Consider the natural homomorphism φ from R to $R/(a) \times R/(1-a)$ which sends r to $(r+(a), r+(1-a))$. The kernel of this homomorphism is the set of elements in $(a) \cap (1-a)$. Let $x \in (a) \cap (1-a)$ so $x = ra = s(1-a)$ for some $r, s \in R$. Multiplying both sides by a yields $ra^2 = sa - sa^2$. But then we have

$$x = ra = sa - sa = 0.$$

Thus, $(a) \cap (1-a) = 0$ so φ is injective. To see that it is surjective, note that $(a)+(1-a)=(1)$. By Exercise 6.1, the natural homomorphism is surjective. Therefore, φ is a bijective ring homomorphism and thus an isomorphism.

The ideal (a) is already an abelian group under addition. To see that it is also a ring under multiplication in R with a as an identity, note that for $ax \in (a)$, we have $a \cdot ax = a^2x = ax$. Distributivity is inherited from R, making (a) a ring.

Consider the natural map from (a) to $R/(1-a)$ which sends ax to $ax+(1-a)$. This map is surjective as any $x+(1-a) = ax+(x-ax)+(1-a) = ax+(1-a) = \varphi(ax)$. Furthermore, the kernel of this map is the set of elements $ax \in (1-a)$. But $ax = (1-a)y \implies a(x+y) = y \implies a(x+y) = ay \implies ax = 0$ so $x = 0$ and the homomorphism is injective. Thus, we have a bijective homomorphism from $(a) \to R/(1-a)$ so the rings are isomorphic. The third isomorphism is relatively similar to show. □

Exercise V.6.3. Recall (Exercise III.3.15) that a ring R is called *Boolean* if $a^2 = a$ for all $a \in R$. Let R be a finite Boolean ring; prove that $R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$.

Solution. Suppose R has only two elements; then $R \cong \mathbb{Z}/2\mathbb{Z}$. If R has more than two elements, then there is some idempotent $e \notin \{0, 1\}$. Per Exercise 6.2, we can split R into $(e) \times (1 - e)$, both of which have strictly fewer elements than R. Repeating this process will eventually yield a direct product in which each component is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. $\square$

Exercise V.6.4. Let R be a finite commutative ring, and let p be the smallest prime dividing $|R|$. Let $I_1, \ldots, I_k$ be proper ideals such that $I_i + I_j = (1)$ for $i \neq j$. Prove that $k \leq \log_p |R|$. (Hint: Prove $|R|^{k-1} \leq |I_1| \cdots |I_k| \leq (|R|/p)^k$.)

Solution. To do. $\square$

Exercise V.6.5. Show that the map $\mathbb{Z}[x] \to \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x)$ is not surjective.

Solution. Consider the element $(1, 2) \in \mathbb{Z}[x]/(2) \times \mathbb{Z}[x]/(x)$. Suppose some polynomial $f \in \mathbb{Z}[x]$ is sent to this element. Since $f \equiv 2(\mod x)$, this forces the constant term of f to be 2. However, if this were the case then the constant term of $f \mod 2$ would be 0, a contradiction. Thus, there is no polynomial mapped to this element and the mapping is not surjective. $\square$

Exercise V.6.6. Let R be a UFD.

- Let $a, b \in R$ such that $\gcd(a, b) = 1$. Prove that $(a) \cap (b) = (ab)$.
- Under the hypotheses of Corollary 6.4 (but only assuming that R is a UFD) prove that the function φ is injective.

Solution. Certainly $(ab) \subseteq (a) \cap (b)$ since any element $r \cdot ab = (rb) \cdot a = (ra) \cdot b$. To show the other direction, consider the least common multiple m of a and b. That is, for any other multiple n of a and b, we have $m \mid n$. Certainly $(a) \cap (b) \subseteq (m)$ so we must show that $m = ab$. Indeed, suppose $ab \nmid m$. Then we find $x = ab/m \neq 1$. But then we have

$$a = \frac{ab}{m} \cdot \frac{m}{b} = x \cdot \frac{m}{b}.$$

Similarly, $x \mid b$ so $\gcd(a, b) \neq 1$, a contradiction. Thus, it must be the case that $m = ab$ and $(a) \cap (b) = (ab)$.

For the second part, note that the kernel of φ is clearly $(a_1) \cap \cdots \cap (a_k)$. But by the first part, this ideal is equal to $(a1 \cdots a_k) = (a)$. Thus, the kernel of φ is equal to the identity in $R/(a)$ and the function is injective. $\square$

Exercise V.6.7. Find a polynomial $f \in \mathbb{Q}[x]$ such that $f \equiv 1 \mod (x^2+1)$ and $f \equiv x \mod x^{100}$.

Solution. First note that $x^{100} \equiv 1 \mod (x^2+1)$. From this, consider the polynomial $f(x) = x + x^{100}(1-x) = x + x^{100} - x^{101}$. We find that $f \equiv x \mod x^{100}$ and $f \equiv x + 1 - x \equiv 1 \mod (x^2+1)$. □

Exercise V.6.8. Let $n \in \mathbb{Z}$ be a positive integer and $n = p_1^{a_1} \cdots p_r^{a_r}$ its prime factorization. By the classification theorem for finite abelian groups (or, in fact, simplier considerations; cf. Exercise II.4.9)

$$\frac{\mathbb{Z}}{(n)} \cong \frac{\mathbb{Z}}{(p_1^{a_1})} \times \cdots \times \frac{\mathbb{Z}}{(p_r^{a_r})}$$

as abelian groups.

- Use the CRT to prove that this is in fact a *ring* isomorphism.
- Prove that
$$\left(\frac{\mathbb{Z}}{(n)}\right)^* \cong \left(\frac{\mathbb{Z}}{(p_1^{a_1})}\right)^* \times \cdots \times \left(\frac{\mathbb{Z}}{(p_r^{a_r})}\right)^*$$
(recall that $(\mathbb{Z}/n\mathbb{Z})^*$ denotes the group of units of $\mathbb{Z}/n\mathbb{Z}$).
- Recall (Exercise II.6.14) that *Euler's ϕ-function* $\phi(n)$ denotes the number of positive integers $\leq n$ that are relatively prime to n. Prove that
$$\phi(n) = p_1^{a_1-1}(p_1-1)\cdots p_r^{a_r-1}(p_r-1).$$

Solution. To do. □

Exercise V.6.9. Let I be a nonzero ideal of $\mathbb{Z}[i]$. Prove that $\mathbb{Z}[i]/I$ is finite.

Solution. Note that $\mathbb{Z}[i]$ is a Euclidean domain so it is a PID. That is, there exists some $\alpha \in \mathbb{Z}[i]$ such that $I = (\alpha)$. Let $a + bi + I$ be an element of $\mathbb{Z}[i]/I$. By the Division Algorithm, there exist $q, r \in \mathbb{Z}[i]$ such that

$$a + bi = q\alpha + r$$

with $N(r) < N(\alpha)$. But then $a + bi - r = q\alpha \in I$ so $a + bi + I = r + I$. That is, every element of the quotient ring is represented by some element r with norm less that $N(\alpha)$. There are only finitely many elements with such a norm (since there are only finitely many integers a, b such that $a^2 + b^2 < N(\alpha)$. Thus, the quotient ring $\mathbb{Z}[i]/I$ is finite. □

Exercise V.6.10. Let $z, w \in \mathbb{Z}[i]$. Show that if z and w are associates, then $N(z) = N(w)$. Show that if $w \in (z)$ and $N(z) = N(w)$, then z and w are associates.

Solution. Recall that z and w are associates if and only if $z = uw$ for some unit $u \in \mathbb{Z}[i]$. But then we have $N(z) = N(uw) = N(u)N(w) = N(w)$ (since $N(u) = 1$).

Now suppose $w \in (z)$ and $N(z) = N(w)$. Let $w = uz$. Clearly $N(u) = 1$. But by Lemma 6.6, this implies that u is a unit so w and z are associates. $\square$

Exercise V.6.11. Prove that the irreducible elements in $\mathbb{Z}[i]$ are, up to associates: $1 + i$; the integer primes congruent to $3 \mod 4$; and the elements $a \pm bi$ with $a^2 + b^2$ an integer prime congruent to $1 \mod 4$.

Solution. Let $q \in \mathbb{Z}[i]$ be irreducible. Certainly $N(q) \neq 1$ so $N(q)$ is a product of primes in $\mathbb{Z}$. First consider the case where $N(q)$ is prime. If it is even, then it must be that case that $N(q) = 2$, in which case we have $q = 1 + i$ or one of its associates (there are only four solutions to $a^2 + b^2 = 2$. If $N(q)$ is odd then by the classification of primes which split in $\mathbb{Z}[i]$ we must have $N(q) \equiv 3 \mod 4$. Now suppose $N(q)$ is not prime. If there is a prime $p \equiv 3 \mod 4$ which divides $N(q) = \bar{q}q$ then $p \mid q$. But since q is irreducible, it must be the case that $(p) = (q)$ and the elements are associate. We are reduced to the case where $N(q)$ is a product of primes $p \equiv 1 \mod 4$. Let p be one such prime. Then p splits in $\mathbb{Z}[i]$ as $z\bar{z}$ for some prime element z. Therefore $z \mid q$ and $(z) = (q)$ so $N(q) = N(z) = p$, a contradiction. $\square$

Exercise V.6.12. Prove Lemma 6.5 without any 'visual' aid. (Hint: Let $z = a + bi$, $w = c + di$ be Gaussian integers with $w \neq 0$. Then $z/w = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$. Find integers e, f such that $|e - \frac{ac+bd}{c^2+d^2}| \leq \frac{1}{2}$ and $|f - \frac{bc-ad}{c^2+d^2}| \leq \frac{1}{2}$, and set $q = e + if$. Prove that $|\frac{z}{w} - q| < 1$. Why does this do the job?)

Solution. Denote $c^2 + d^2$ by $N(w)$ since they are equivalent. By Euclidean division in the integers, there exist $e, r_1 \in \mathbb{Z}$ such that

$$ac + bd = eN(w) + r_1$$

where $|r_1| \leq \frac{N(w)}{2}$. The inequality follows from the fact that if $r_1 > 0$ then $e > 1$ so we are at least dividing by 2. Similarly, we have $bc - ad = fN(w) + r_2$ with $|r_2| \leq \frac{N(w)}{2}$. Now note that

$$\left| e - \frac{ac + bd}{c^2 + d^2} \right| \leq \frac{1}{2},$$
$$\left| f - \frac{bc - ad}{c^2 + d^2} \right| \leq \frac{1}{2}$$

and let $q = e + if$. Then we have

$$\frac{z}{w} = q + \frac{r_1 + r_2 i}{N(w)}.$$

which can be rearranged to yield

$$\left|\frac{z}{w} - q\right| = \left|\frac{r_1 + r_2 i}{N(w)}\right| \leq 1$$

where the last inequality follows from the division algorithm in $\mathbb{Z}$. I don't know why this is sufficient, or if I even did this correctly. However, we can see that

$$z = qw + \frac{r}{\bar{w}}$$

where $r = r_1 + r_2 i$. Furthermore, we have

$$N\left(\frac{r}{\bar{w}}\right) = \frac{r_1^2 + r_2^2}{N(w)} \leq \frac{\frac{N(w)^2}{4} + \frac{N(w)^2}{4}}{N(w)} = \frac{N(w)}{2} < N(w)$$

proving that this is in fact a Euclidean valuation. □

Exercise V.6.13. Consider the set $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$.

- Prove that $\mathbb{Z}[\sqrt{2}]$ is a ring, isomorphic to $\mathbb{Z}[t]/(t^2 - 2)$.
- Prove that the function $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ defined by $N(a + b\sqrt{2}) = a^2 - 2b^2$ is multiplicative: $N(zw) = N(z)N(w)$. (Cf. Exercise III.4.10.)
- Prove that $\mathbb{Z}[\sqrt{2}]$ has infinitely many units.
- Prove that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain, by using the absolute value of N as valuation. (Hint: Follow the same steps as in Exercise 6.12.)

Solution. It is easy to verify that $\mathbb{Z}[\sqrt{2}]$ is a ring. The isomorphism sends $a + bt \in \mathbb{Z}[t]/(t^2 - 2)$ to $a + b\sqrt{2}$. The map is clearly surjective. Furthermore, the kernel is the set of polynomials such that $a = b = 0$. But then $f \in (t^2 - 2)$ so the kernel is trivial in the quotient ring, making the map injective and hence an isomorphism.

Given the norm function and letting $z = a_0 + b_0\sqrt{2}, w = a_1 + b_1\sqrt{2}$, we have

$$\begin{aligned}
N(zw) &= (a_0a_1 + b_0b_1d)^2 - 2(a_0b_1 + a_1b_0) \\
&= \left((a_0a_1)^2 + 2(a_0a_1)(b_0b_1d) + (b_0b_1d)^2\right) - \left((a_0b_1)^2 + 2(a_0b_1)(a_1b_0) + (a_1b_0)^2\right) d \\
&= (a_0a_1)^2 + (b_0b_1d)^2 - (a_0b_1)^2 d - (a_1b_0)^2 d \\
&= (a_0^2 - b_0^2 d)(a_1^2 - b_1^2 d) \\
&= N(z)N(w)
\end{aligned}$$

showing that N is multiplicative.

Recall that if u is a unit in $\mathbb{Z}[\sqrt{2}]$ then $N(u)$ is a unit in $\mathbb{Z}$. Thus, we should consider solutions to $N(u) = a^2 - 2b^2 = \pm 1$. It is clear that the solution set is nonempty as $a = 1, b = 1$ produces a solution. Now suppose that $a + b\sqrt{2}$ is a unit in in $\mathbb{Z}[\sqrt{2}]$ so that $a^2 - 2b^2 = \pm 1$. Consider $z = (a + 2b) + (a + b)\sqrt{2}$. We have

$$\begin{aligned} N(z) &= (a + 2b)^2 - 2(a + b) \\ &= a^2 + 4ab + 4b^2 - 2a^2 - 4ab - 2b^2 \\ &= 2b^2 - a^2 \\ &= -(a^2 - 2b^2) = \pm 1 \end{aligned}$$

so we can construct a distinct solution, proving that there are infinitely many units.

Let $x = a + b\sqrt{2}$ and $y = c + d\sqrt{2}$. We have

$$\frac{x}{y} = \frac{(ac - 2bd) + (bc - ad)\sqrt{2}}{c^2 - 2d^2} = r + s\sqrt{2}.$$

Let n be the closest integer to r and m be the closest integer to s so that $|r - n| \leq \frac{1}{2}$ and $|s - m| \leq \frac{1}{2}$. Define $t = (r - n) + (s - m)\sqrt{2}$ so that we have

$$t = r + s\sqrt{2} - (n + m\sqrt{2}) = \frac{x}{y} - (n + m\sqrt{2}).$$

Multiplying by y and rearranging yields

$$x = yt + (n + m\sqrt{2})y$$

where

$$\begin{aligned} N(yt) &= N(y)N(t) \\ &= N(y)\left|(r - n)^2 - 2(s - m)^2\right| \\ &\leq N(y)\left(\left|\frac{1}{4}\right| + 2\left|\frac{1}{4}\right|\right) \\ &= \frac{3}{4}N(y) \end{aligned}$$

Thus, the valuation of the remainder is less than that of the divisor, proving the valuation is Euclidean. □

Exercise V.6.14. Working as in Exercise 6.13, prove that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain. (Use the norm $N(a + b\sqrt{-2} = a^2 + 2b^2$.)

If you are particularly adventurous, prove that $\mathbb{Z}[(1 + \sqrt{d})/2]$ is also a Euclidean domain for $d = -3, -7, -11$. (You can still use the norm defined by

$N(a+b\sqrt{d}) = a^2 - db^2$; note that this is still an integer on $\mathbb{Z}[(1+\sqrt{d})/2]$, if $d \equiv 1 \mod 4$.)

The five values $d = -1, -2$, resp., $-3, -7, -11$, are the only ones for which $\mathbb{Z}[\sqrt{d}]$, resp., $\mathbb{Z}[(1+\sqrt{d})/2]$, is Euclidean. For the values $d = -19, -43, -67, -163$, the ring $\mathbb{Z}[(1+\sqrt{d})/2]$ is still a PID (cf. §2.4 and Exercise 2.18 for $d = -19$); the fact that there are no other negative values for which the ring of integers in $\mathbb{Q}(\sqrt{d})$ is a PID was conjectured by Gauss and only proven by Alan Baker and Harold Stark around 1966. Also, keep in mind that $\mathbb{Z}[\sqrt{-5}]$ is not even a UFD, as you have proved all by yourself in Exercise 1.17.

Solution. We proceed in the same manner as in Exercise 6.13. Let $x = a + b\sqrt{-2}$ and $y = c + d\sqrt{2}$. We have

$$\frac{x}{y} = \frac{(ac+2bd)+(bc-ad)\sqrt{2}}{c^2+2d^2} = r + s\sqrt{2}.$$

Let n be the closest integer to r and m be the closest integer to s so that $|r-n| \leq \frac{1}{2}$ and $|s-m| \leq \frac{1}{2}$. Now define $t = (r-n)+(s-m)\sqrt{-2}$ so that we have

$$t = r + s\sqrt{-2} - (n + m\sqrt{-2}) = \frac{x}{y} - (n + m\sqrt{-2}).$$

We can transform this into the equation

$$x = yt + (n - m\sqrt{-2})y$$

where

$$\begin{aligned} N(yt) &= N(y)N(t) \\ &= N(y)\left((r-n)^2 + 2(s-m)^2\right) \\ &\leq N(y)\left(\frac{1}{4} + 2\frac{1}{4}\right) \\ &= \frac{3}{4}N(y) \\ &< N(y) \end{aligned}$$

Thus, the valuation of the remainder is less than the valuation of y so we have a Euclidean valuation.

I am not feeling particularly adventurous so I will not show the rings of integers are in fact Euclidean domains but I imagine the proofs are incredibly similar. □

Exercise V.6.15. Give an elementary proof (using modular arithmetic) of the fact that if an integer n is congruent to 3 modulo 4, then it is not the sum of two squares.

Solution. Consider the ring $\mathbb{Z}/4\mathbb{Z}$. Squaring each element in this ring yields the elements 0 and 1. Suppose $n = a^2 + b^2$. Clearly if $n \equiv 3 \mod 4$ then $a^2 + b^2 \equiv 3 \mod 4$. But we cannot add two elements among 0 and 1 to get 3. Thus, n cannot be the sum of two squares. $\square$

Exercise V.6.16. Prove that if m and n are two integers, both of which can be written as sums of two squares, then mn can also be written as the sum of two squares.

Solution. Suppose $m = a^2 + b^2$ and $n = c^2 + d^2$. Then we have

$$\begin{aligned} mn &= (a^2 + b^2)(c^2 + d^2) \\ &= (ac)^2 + (ad)^2 + (bc)^2 + (bd)^2 \\ &= (ac)^2 + 2abcd(bd)^2 + (ad)^2 - 2abcd + (bc)^2 \\ &= (ac + bd)^2 + (ad - bc)^2 \end{aligned}$$

so mn is also a sum of squares. $\square$

Exercise V.6.17. Let n be a positive integer.

- Prove that n is a sum of two squares if and only if it is the norm of a Gaussian integer $a + bi$.
- By factoring $a^2 + b^2$ in $\mathbb{Z}$ and $a + bi$ in $\mathbb{Z}[i]$, prove that n is a sum of two squares if and only if each integer prime factor p of n such that $p \equiv 3 \mod 4$ appears with an even power in n.

Solution. Suppose $n = N(a + bi)$. Clearly $N(a + bi) = a^2 + b^2 = n$ so n is the sum of two squares. Now suppose $n = a^2 + b^2$ and consider $z = a + bi$. Then $N(z) = a^2 + b^2 = n$ so n is the norm of a Gaussian integer.

Consider the factorization $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. First suppose that each prime factor $p_i \equiv 3 \mod 4$ has a corresponding even power α_i. Then we can write $n = s^2 m$ where m is not divisible by any squares. Therefore, all primes p which divide m must satisfy $p \equiv 1 \mod 4$ so each p is the sum of two squares and hence their product m is the sum of two squares, say $x^2 + y^2$. But then we have $n = s^2(x^2 + y^2) = (sx)^2 + (sy)^2$ so it is the sum of two squares.

Now suppose $n = x^2 + y^2$ is the sum of two squares. Again, consider the factorization of n over $\mathbb{Z}$. If all of the primes in this factorization are congruent to 1 modulo 4 then we are done so suppose there is a prime $p \equiv 3 \mod 4$. We must show that the largest power of p dividing n, call it α, is even. Indeed, we have $p^\alpha \mid n = (x + iy)(x - iy)$. But since p does not split in $\mathbb{Z}[i]$, it is prime over this ring and hence we have $p \mid x + yi$ or $p \mid x - yi$, both of which imply that $p \mid x$ and $p \mid y$. That is, $x = p^{\beta_1} a$ and $y = p^{\beta_2} b$. But then $x^2 = p^{2\beta_1} a^2$ and $y^2 = p^{2\beta_2} b^2$ so the power of p dividing $x^2 + y^2 = n$ must be even. $\square$

Exercise V.6.18. One ingredient in the proof of Lagrange's theorem on four squares is the following result, which can be proven by completely elementary means. Let $p > 0$ be an odd prime integer. Then there exists an integer n, $0 < n < p$, such that np may be written as $1 + a^2 + b^2$ for two integers a, b. Prove this result, as follows:

- Prove that the numbers a^2, $0 \le a \le (p-1)/2$, represent $(p+1)/2$ distinct congruence classes mod p.
- Prove the same for numbers of the form $-1 - b^2$, $0 \le b \le (p-1)/2$.
- Now conclude, using the pigeon-hole principle.

Solution. Let $c = a^2 \mod p$. Then a is a root of the polynomial $x^2 - c$ over $\mathbb{Z}/p\mathbb{Z}$, as is $p - a$ (which is distinct from a since p is odd). Since a polynomial of degree n over an integral domain can have at most n solutions, these two roots are all of the solutions of this polynomial. As a ranges from 0 to $(p-1)/2$, we have $1 + (p-1)/2$ distinct congruence classes represented by a^2 (we add 1 to account for $a = 0$). Thus, a^2 represents $(p+1)/2$ distinct congruence classes modulo p.

Similarly, the integers b^2 are distinct, so the integers $-1 - b^2$ are also distinct and represent $(p+1)/2$ congruence classes.

By the pigeonhole principle, there are a and b in this range such that a^2 and $-1 - b^2$ are congruent modulo p. That is, there exist $a, b \in \mathbb{Z}$ such that

$$p \mid a^2 + b^2 + 1 \Longleftrightarrow np = 1 + a^2 + b^2$$

proving the desired result. □

Exercise V.6.19. Let $\mathbb{I} \subseteq \mathbb{H}$ be the set of quaternions (cf. Exercise III.1.12) of the form $\frac{a}{2}(1 + i + j + k) + bi + cj + dk$ with $a, b, c, d \in \mathbb{Z}$.

- Prove that $\mathbb{I}$ is a (noncommutative) subring of the ring of quaternions.
- Prove that the norm $N(w)$ (Exercise III.2.5) of an integral quaternion $w \in \mathbb{I}$ is an integer and $N(w_1 w_2) = N(w_1)N(w_2)$.
- Prove $\mathbb{I}$ has exactly 24 units in $\mathbb{I}$: $\pm 1, \pm i, \pm j, \pm k$, and $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$.
- Prove that every $w \in \mathbb{I}$ is an associate of an element $a + bi + cj + dk \in \mathbb{I}$ with $a, b, c, d \in \mathbb{Z}$.

The ring $\mathbb{I}$ is called the ring of *integral quaternions.*

Solution. It is clear that $\mathbb{I}$ is closed additively and has an additive identity, namely 0. Furthermore, we can verify that $\mathbb{I}$ is closed under multiplication by writing down the product of two quaternions and substituting the coefficients of $1, i, j, k$ by half-integers (elements of the set $\mathbb{Z} + \frac{1}{2}$. Doing so shows that the product is still composed of half integers and is thus an element of $\mathbb{I}$. The multiplicative identity is 1. Thus, $\mathbb{I}$ is a subring of $\mathbb{H}$.

Recall that the norm of a quaternion $w = a + bi + cj + dk$ is given by $N(w) = a^2 + b^2 + c^2 + d^2$. Given an element $w \in \mathbb{I}$, we have

$$\begin{aligned} N(w) &= \frac{a^2}{4} + \left(\frac{a}{2} + b\right)^2 + \left(\frac{a}{2} + c\right)^2 + \left(\frac{a}{2} + d\right)^2 \\ &= a^2 + b^2 + c^2 + d^2 + ab + ac + ad \end{aligned}$$

which is an integer. The multiplicativity of the norm is inherited from $\mathbb{H}$.

Recall that if $u \in \mathbb{I}$ is a unit then there is some element $v \in \mathbb{I}$ such that $uv = 1$. But then $N(uv) = N(u)N(v) = 1$ so $N(u)$ is a unit in $\mathbb{Z}$ and we must have

$$a^2 + b^2 + c^2 + d^2 + ab + ac + ad = \pm 1.$$

Clearly $\pm 1, \pm i, \pm j, \pm k$ satisfy this, as do $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$. I'm not sure how to verify that these are the *only* units but they are certainly units.

Now we show that every $w \in \mathbb{I}$ is associate to a quaternion with integer coefficients. First note that if a is even then $a/2$ is an integer and we are done. Now suppose a is odd. Then we can multiply by $\frac{1}{2}(1 \pm i \pm j \pm k)$ where the sign is positive if the associated coefficient is odd and even if the associated coefficient is negative. It is tedious to show this case by case so just trust me. Since we are multiplying by a unit, the ideal generated by this product and w are the same, so the two are associate. $\square$

Exercise V.6.20. Let $\mathbb{I}$ be as in Exercise 6.19. Prove that $\mathbb{I}$ shares most good properties of a Euclidean domain, notwithstanding the fact that it is noncommutative.

- Let $z, w \in \mathbb{I}$, with $w \neq 0$. Prove that $\exists q, r \in \mathbb{I}$ such that $z = qw + r$, with $N(r) < N(w)$. (This is a little tricky; don't feel too bad if you have to cheat and look it up somewhere.)
- Prove that every left-ideal in $\mathbb{I}$ is of the form $\mathbb{I}w$ for some $w \in \mathbb{I}$.
- Prove that every $z, w \in \mathbb{I}$, not both zero, have a 'greatest common right-divisor' d in $\mathbb{I}$, of the form $\alpha z + \beta w$ for $\alpha, \beta \in \mathbb{I}$.

Solution. Consider the element $x = z/w$ and construct x_0 with each component of x rounded to the nearest integer so that $x \in \mathbb{I}$. Then we have $|x - x_0| \leq (1/2)^2 \cdot 4 = 1$. Let $r = x - x_0$. If $|r| < 1$ then we have $z = wx_0 + wr$, where $N(wr) = N(w)N(r) < N(w)$. If $|r| = 1$, then each component of r has absolute value $\frac{1}{2}$ so r is a unit in $\mathbb{I}$. But then $x' = x + r \in \mathbb{I}$ and we find

$$x = r + x_0 = x' \implies z = wx' + 0.$$

Since $N(0) = 0$, we are done.

Let I be an ideal of $\mathbb{I}$. Clearly if $I = 0$, then $w = 0$ so assume $I \neq 0$. Then pick $w \in I$ with minimal norm. Clearly $(w) \subseteq I$. Now let $z \in I$. By division in $\mathbb{I}$, there exist $q, r \in \mathbb{I}$ such that $z = qw + r$. If $r = 0$ then $z \in (w)$ and we are done. Otherwise, we have $r = z - qw \in I$ and $N(r) < N(w)$. However, we assumed w had minimal norm in I, a contradiction. Thus, $r = 0$ is the only case. That is, $I = (w)$.

Given $z, w \in \mathbb{I}$, consider an application of division with remainder.

$$\begin{aligned} z &= q_1 w + r_1 \\ w &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \end{aligned}$$

where $N(r_i) < N(q)$. Clearly this process must terminate so for some r_{n+1}, we have $N(r_{n+1}) = 0 \Longrightarrow r_{n+1} = 0$, or $r_{n-1} = q_{n+1} r_n$. We claim that $d = r_n$. It is easy to see that $r_n \mid z$ and $r_n \mid w$ so assume that x is any divisor of both z and w. We have $x \mid z - q_1 w = r_1$. Repeating this process for each step in the 'Euclidean algorithm' shows that $x \mid r_n$. Thus, r_n is the greatest common right-divisor for z and w. Furthermore, it can easily be rewritten in the form $\alpha z + \beta w$ by reversing the steps of the algorithm and substituting values for the remainders. $\square$

Exercise V.6.21. Prove Lagrange's theorem on four squares. Use notation as in Exercise 6.19 and 6.20.

- Let $z \in \mathbb{I}$ and $n \in \mathbb{Z}$. Prove that the greatest common right-divisor of z and n in $\mathbb{I}$ is 1 if and only if $(N(z), n) = 1$ in $\mathbb{Z}$. (If $\alpha z + \beta n = 1$, then $N(\alpha)N(z) = N(1 - \beta n) = (1 - \beta n)(1 - \bar{\beta} n)$, where $\bar{\beta}$ is obtained by changing the signs of the coefficients of i, j, k. Expand, and deduce that $(N(z), n) \mid 1$.)
- For an odd prime integer p, use Exercise 6.18 to obtain an integral quaternion $z = 1 + ai + bj$ such that $p \mid N(z)$. Prove that z and p have a common right-divisor that is not a unit and not an associate of p.
- Say that $w \in \mathbb{I}$ is *irreducible* if $w = \alpha\beta$ implies that either α or β is a unit. Prove that integer primes are *not* irreducible in $\mathbb{I}$. Deduce that every positive prime integer is the norm of some integral quaternion.
- Prove that every positive integer is the norm of some integral quaternion.
- Finally, use the last point of Exercise 6.19 to deduce that every positive integer may be written as the sum of four perfect squares.

Solution. First assume $(N(z), n) = 1$ and let w be a common divisor of z and n. Then $N(w) \mid N(z)$ and $N(w) \mid N(n) = n$ so $N(w) \mid 1$ and $N(w) = 1$. Thus,

w is a unit in $\mathbb{I}$ and is associate to 1. Now suppose the gcrd of z and n is 1. By Problem 6.20, we can write $1 = \alpha z + \beta n$ for $\alpha, \beta \in \mathbb{I}$. Then we find

$$N(\alpha)N(z) = N(1 - \beta n) = (1 - \beta n)(1 - \bar{\beta} n),$$

where $\bar{\beta}$ is obtained by reversing the signs of i, j, k. Expanding this yields

$$N(\alpha)N(z) = 1 - bn + N(\beta)n^2$$

where b is the real component of β. Since $N(\alpha)$ and $N(\beta)n - b$ are elements of $\mathbb{Z}$, we can find $a_1, a_2 \in \mathbb{I}$ to represent them. Thus, we can rearrange the above equation to yield

$$a_1 N(z) + a_2 n = 1,$$

implying that $\gcd(N(z), n) = 1$.

By Exercise 6.18, there is some n, $0 < n < p$ such that $np = 1 + a^2 + b^2$. That is, $p \mid 1 + a^2 + b^2$. Now consider the integral quaternion $z = 1 + ai + bj$. Clearly $N(z) = 1 + a^2 + b^2$ so $p \mid N(z)$. By the above point, the greatest common right-divisor of p and z is not 1 because $\gcd(p, N(z)) = p$. Furthermore, since z is a proper integral quaternion, $p \nmid z$ and the two are not associate.

As shown above, an odd integer prime p divides the norm of some integral quaternion z, and the two have a common right-divisor, say w. Then we can write $p = wx$ for some $x \in \mathbb{I}$ where neither are units. For every positive prime integer, we have $p \mid 1 + a^2 + b^2$. Let $\alpha = 1 + ai + bj$ and w be the gcd of p and α. Then $p = z_1 w$ and $\alpha = 1 + ai + bj = z_2 w$ and we can write

$$N(p) = N(z_1)N(w) = p^2.$$

Since $N(w) \neq 1$ and $N(w) \neq p^2$, we must have $N(z_1) = N(w) = p$. Thus, p is the norm of some integral quaternion.

To see that every postitive integer is the norm of some integral quaternion, it suffices to show that the product of any two primes is the norm of an integral quaternion. Indeed, if $p_1 = N(z_1)$ and $p_2 = N(z_2)$, then

$$p_1 p_2 = N(z_1)N(z_2) = N(z_1 z_2)$$

so $p_1 p_2$ is the norm of an integral quaternion. Since any postive integer n has a decomposition into primes, n is the norm of some integral quaternion.

Finally, let n be a positive integer and suppose $n = N(z)$ for some $z \in \mathbb{I}$. By Exercise 6.19, z is associate to some integral quaternion w of the form $a + bi + cj + dk$ with $a, b, c, d \in \mathbb{Z}$. But then $N(z) = N(w)$ so

$$n = a^2 + b^2 + c^2 + d^2$$

proving that every positive integer is a sum of four perfect squares. $\square$

Chapter VI

Linear algebra

VI.1 Free modules revisited

Exercise VI.1.1. Prove that $\mathbb{R}$ and $\mathbb{C}$ are isomorphic as $\mathbb{Q}$-*vector spaces.* (In particular, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are isomorphic as groups.)

Solution. Observe that $\dim_{\mathbb{Q}} \mathbb{R}$ is uncountable (and in particular, is the cardinality of the continuum). This is equal to $\dim_{\mathbb{Q}} \mathbb{C}$. Since the two vector spaces have equal dimension, they are isomorphic as $\mathbb{Q}$-vector spaces and hence are isomorphic as groups. □

Exercise VI.1.2. Prove that the sets listed in Exercise III.1.4 are all $\mathbb{R}$-vector spaces, and compute their dimensions.

Solution. Recall that we only need to show that each set is a module over $\mathbb{R}$. We start with $\mathfrak{sl}_n(\mathbb{R}) = \{M \in \mathfrak{gl}_n(\mathbb{R}) \mid \operatorname{tr}(M) = 0\}$ and define the action of $\mathbb{R}$ on a matrix as multiplication by each entry. Given $A, B \in \mathfrak{sl}_n(\mathbb{R})$, $r_1, r_2 \in \mathbb{R}$, we have

- $(r_1 + r_2)A = r_1 A + r_2 A$
- $1A = A$ and $(r_1 r_2)A = r_1(r_2 A)$
- $r_1(A + B) = r_1 A + r_1 B$

so $\mathfrak{sl}_n(\mathbb{R})$ is a $\mathbb{R}$-vector space. To find its dimension, we are tasked with finding a basis. First note that the elementary matrices $e_{i,j}$ for $i \neq j$ all have zero trace so they are in $\mathfrak{sl}_n(\mathbb{R})$. For $e_{i,i}$, we require another element on the diagonal to force the trace to be zero. The most convenient choice is to let $h_i = e_{i,i} - e_{i+1,i+1}$. Certainly, this set of matrices generates $\mathfrak{sl}_n(\mathbb{R})$ and it contains $n^2 - n + (n-1) = n^2 - 1$ elements so the dimension of this vector space is $n^2 - 1$. Presumably, we use a similar, if not the same, basis for $\mathfrak{sl}_n(\mathbb{C})$.

We define the action of $\mathbb{R}$ on $\mathfrak{so}_n(\mathbb{R}) = \{M \in \mathfrak{sl}_n(\mathbb{R}) \mid M + M^t = 0\}$ in exactly the same manner as above. It is easy to verify that this is also a vector space. Again, we are tasked with computing a basis. First, we construct a set of basis matrices with zero entries on the diagonal. Let $g_{i,j}$ denote the matrix with entry 1 at i, j, entry -1 at j, i, and zero everywhere else, where $i \neq j$. Then $g_{i,j} \in \mathfrak{so}_n(\mathbb{R})$. To consider the diagonal, note that if any entry on the diagonal is nonzero, then summing the matrix with its transpose makes a nonzero matrix. Thus, the entries on the diagonal must be zero. This set generates $\mathfrak{so}_n(\mathbb{R})$ and contains $\frac{n(n-1)}{2}$ elements, so this is the dimension of the Lie algebra.

The action of $\mathbb{R}$ on $\mathfrak{su}(n) = \{M \in \mathfrak{sl}_n(\mathbb{C}) \mid M + M^* = 0\}$ is again the same as above. To compute a basis for this vector space, first note that the diagonals must not include reals because the complex transpose matrix will not sum to zero. Therefore, we redefine h_i to use $i, -i$ instead of $1, -1$. Furthermore, the basis matrices with zeros on the diagonals must be separated into real and imaginary components. Therefore, we include the $g_{i,j}$ from above and also define $g^*_{i,j}$ to be matrices with the imaginary unit i at i, j and j, i for $i \neq j$, and zero elsewhere. This is a basis for the vector space and has $n(n-1)+(n-1) = n^2-1$ elements, so this is the dimension of the vector space. □

Exercise VI.1.3. Prove that $\mathfrak{su}(2) \cong \mathfrak{so}_3(\mathbb{R})$ as $\mathbb{R}$-vector spaces. (This is immediate, and not particularly interesting, from the dimension computation of Exercise 1.2. However, these two spaces may be viewed as the tangent spaces to $SU(2)$, resp., $SO_3(\mathbb{R})$, at I; the surjective homomorphism $SU(2) \to SO_3(\mathbb{R})$ you constructed in Exercise II.8.9 induces a more 'meaningful' isomorphism $\mathfrak{su}(2) \to \mathfrak{so}_3(\mathbb{R})$. Can you find this isomorphism?)

Solution. Since $\mathfrak{su}(2)$ and $\mathfrak{so}_3(\mathbb{C})$ have the same dimension, namely 3, the two are isomorphic as $\mathbb{R}$-vector spaces. Admittedly, I don't know how to interpret the surjection from $SU(2) \to SO_3(\mathbb{R})$, nor do I have any clue how to work with Lie algebras. □

Exercise VI.1.4. Let V be a vector space over a field k. A *Lie bracket* on V is an operation $[\cdot,\cdot] : V \times V \to V$ such that

- $(\forall u, v, w \in V), (\forall a, b \in k)$,
$$[au + bv, w] = a[u, w] + b[v, w], \quad [w, au + bv] = a[w, u] + b[w, v],$$
- $(\forall v \in V), [v, v] = 0$,
- and $(\forall u, v, w \in V), [[u, v], w] + [[v, w], u] + [[w, u], v] = 0$.

(This axiom is called the *Jacobi identity*.) A vector space endowed with a Lie bracket is called a *Lie algebra*. Define a category of Lie algebras over a given field. Prove the following:

- In a Lie algebra V, $[u, v] = -[v, u]$ for all $u, v \in V$.
- If V is a k-algebra (Definition III.5.7), then $[v, w] := vw - wv$ defines a Lie bracket on V, so that V is a Lie algebra in a natural way.
- This makes $\mathfrak{gl}_n(\mathbb{R})$, $\mathfrak{gl}_n(\mathbb{C})$ into Lie algebras. The sets listed in Exercise III.1.4 are all Lie algebras, with respect to a Lie bracket induced from $\mathfrak{gl}$.
- $\mathfrak{su}_2(\mathbb{C})$ and $\mathfrak{so}_3(\mathbb{R})$ are isomorphic as Lie algebras over $\mathbb{R}$.

Solution. First, let $u, v \in V$. We find

$$\begin{aligned}
0 &= [u + v, u + v] \\
&= [u, u + v] + [v, u + v] \\
&= [u, u] + [u, v] + [v, u] + [v, v] \\
&= [u, v] + [v, u]
\end{aligned}$$

so $[u, v] = -[v, u]$.

Recall that a k-algebra V is a k-vector space with a compatible ring structure. We merely need to verify that the axioms hold. We find that for $u, v, w \in V$, $a, b \in k$,

$$\begin{aligned}
[au + bv, w] &= (au + bv)w - w(au + bv) \\
&= a(uw - wu) + b(vw - wv) \\
&= a[u, w] + b[v, w].
\end{aligned}$$

The other axiom in the first point is easy to verify. Clearly, we have $[v, v] = v^2 - v^2 = 0$. Finally, the Jacobi identity also holds, though it's tedious to typeset. □

Exercise VI.1.5. Let R be an integral domain. Prove or disprove the following:

- Every linearly independent subset of a free R-module may be completed to a basis.
- Every generating subset of a free R-module contains a basis.

Solution. The first statement is false. Consider $\mathbb{Z}$ as a module over itself. The set $B = \{2\}$ is linearly independent, yet it cannot be extended to a basis. Indeed, including another element x forces the set to be linearly dependent as $x \cdot 2 - 2 \cdot x = 0$. (Note that we use 2 and x as both elements of the ring and the module.)

The second statement is also false. Consider $\mathbb{Z}$ as a module over itself. The set $B = \{2, 3\}$ is a generating set for $\mathbb{Z}$ because $\gcd(2, 3) = 1$. In particular, every integer is a linear combination of the two. However, neither $\{2\}$ nor $\{3\}$ are a basis for $\mathbb{Z}$. □

Exercise VI.1.6. Prove Lemma 1.8.

Lemma 1.8. *Let $R = k$ be a field, and let V be a k-vector space. Let B be a* minimal *generating set for V; then B is a basis of V.*

Every set generating V contains a basis of V.

Solution. Let B be a minimal generating set for V. Suppose B is not linearly independent. That is, there exists a linear combination

$$c_1 b_1 + \cdots c_t b_t = 0.$$

Since k is a field, we can rearrange the above as

$$b_t = (-c_t^{-1} c_1 b_1) + \cdots + (-c_t^{-1} c_{t-1} b_{t-1}).$$

Then $B' = B \setminus \{b_t\}$ is also a generating set for V, contradicting the minimality of B. Thus, our assumption is incorrect and B must be linearly independent, meaning it is a basis of V. The proof details a procedure for reducing a generating set to a basis by repeatedly removing elements contained in the span of existing elements in the set. $\square$

Exercise VI.1.7. Let R be an integral domain, and let $M = R^{\oplus A}$ be a free R-module. Let K be the field of fractions of R, and view M as a subset of $V = K^{\oplus A}$ in the evident way. Prove that a subset $S \subseteq M$ is linearly independent in M (over R) if and only if it is linearly independent in V (over K). Conclude that the rank of M (as an R-module) equals the dimension of V (as a K-vector space). Prove that if S generates M over R, then it generates V over K. Is the converse true?

Solution. We prove both directions via the contrapositive. Suppose S is linearly dependent in M. That is, there is a linear combination

$$a_1 s_1 + \cdots + a_t s_t = 0.$$

Since $S \subseteq M \subseteq V$, this linear combination also exists in V so S is linearly dependent in V. Thus, if S is linearly independent in V then it must also be linearly independent in M. Now suppose S is linearly dependent in V. Then there is a linear combination

$$\frac{a_1}{b_1} s_1 + \cdots + \frac{a_t}{b_t} s_t = 0.$$

Multiply this linear combination by $b_1 \cdots b_t$ (this exists since the linear combination must be finite). This yields the equation

$$(b_2 \cdots b_t) a_1 s_1 + \cdots + (b_1 \cdots b_{t-1}) a_t s_t = 0$$

which is a linear combination over R, showing that S is linearly dependent in M. Therefore, if S is linearly independent in M then it must be linearly independent in V.

That is, if B is a maximal linearly independent subset of M then it is also a maximal linearly independent subset of V (AKA a basis) so the rank of M and the dimension of V are equal.

Suppose S generates M over R and let $\frac{a}{b} \in V$. There exists a linear combination

$$r_1 s_1 + \cdots + r_t s_t = a.$$

Since $\frac{r_i}{b} \in K$, we find that

$$\frac{r_1}{b} s_1 + \cdots + \frac{r_t}{b} s_t = \frac{a}{b}$$

so S generates V over K.

The converse is not true. Consider $R = \mathbb{Z}$, $K = \mathbb{Q}$, $M = V = \mathbb{Z}$. Certainly $S = \{2\}$ generates V over K since for any element $n \in \mathbb{Z}$ we have $n = \frac{n}{2} \cdot 2$. However, S does not generate M over R. $\square$

Exercise VI.1.8. Deduce Corollary 1.11 from Proposition 1.9.

Corollary 1.11. *Let R be an integral domain, and let A, B be sets. Then*

$$F^R(A) \cong F^R(B) \iff \textit{there is a bijection } A \cong B.$$

Solution. Clearly if $A \cong B$ then the two sets have the same order so $F^R(A)$ and $F^R(B)$ are merely $|A|$ copies of R, so they must be isomorphic. For the other direction, let A be a basis for $F^R(A)$ and let B be a basis for $F^R(B)$. Then A is also a basis for $F^R(B)$, just as B is a basis for $F^R(A)$. But by Proposition 1.9, we have $|A| \leq |B|$ and $|B| \leq |A|$ so $|A| = |B|$ and the two sets are isomorphic. $\square$

Exercise VI.1.9. Let R be a commutative ring, and let M be an R-module. Let $\mathfrak{m}$ be a maximal ideal in R, such that $\mathfrak{m}M = 0$ (that is, $rm = 0$ for all $r \in \mathfrak{m}, m \in M$). Define in a natural way a vector space structure over $R/\mathfrak{m}$ on M.

Solution. For M to be a vector space over $R/\mathfrak{m}$, we require multiplication to be well-defined. That is, we should have $rm = (r + \mathfrak{m})m$, or $\mathfrak{m}m = 0$. Since this is the case, M inherits a vector space structure from the module structure on R. In particular, recall that $M/\mathfrak{m}M$ has a module structure over $R/\mathfrak{m}$. However, we also have that $\mathfrak{m}M = 0$ so $M \cong M/\mathfrak{m}M$. $\square$

Exercise VI.1.10. Let R be a commutative ring, and let $F = R^{\oplus B}$ be a free module over R. Let $\mathfrak{m}$ be a maximal ideal of R, and let $k = R/\mathfrak{m}$ be the quotient field. Prove that $F/\mathfrak{m}F \cong k^{\oplus B}$ as k-vector spaces.

Solution. Consider the natural homomorphism $\varphi : F \to k^{\oplus B}$ which sends each component to its residue class mod $\mathfrak{m}$. The kernel of this homomorphism is the set of elements in F which are in $\mathfrak{m}$, or $\mathfrak{m}F$. Thus, by the first isomorphism theorem for modules, we have

$$\frac{F}{\mathfrak{m}F} \cong k^{\oplus B}$$

and we are done. □

Exercise VI.1.11. Prove that commutative rings satisfy the IBN property. (Use Proposition V.3.5 and Exercise 1.10.)

Solution. Recall that the IBN (Invariant Basis Number) property is the property that $R^m \cong R^n \iff m = n$. One direction is trivial so we only consider the other direction. Let R be a commutative ring and suppose $R^m \cong R^n$. Furthermore, let $\mathfrak{m}$ be a maximal ideal of R^m (its existence is guaranteed by Proposition V.3.5). The isomorphism of modules $R^m \cong R^n$ induces an isomorphism of vector spaces $(R/\mathfrak{m})^m \cong (R/\mathfrak{m})^n$. Since these two finite-dimensional vector fields are isomorphic, it must be the case that $m = n$. □

Exercise VI.1.12. Let V be a vector space over a field k, and let $R = \mathrm{End}_{k\text{-Vect}}(V)$ be its ring of endomorphisms (cf. Exercise III.5.9). (Note that R is *not* commutative in general.)

- Prove that $\mathrm{End}_{k\text{-Vect}}(V \oplus V) \cong R^4$ as an R-module.
- Prove that R does not satisfy the IBN property if $V = k^{\oplus \mathbb{N}}$.

(Note that $V \cong V \oplus V$ if $V = k^{\oplus \mathbb{N}}$.)

Solution. The endomorphism ring $\mathrm{End}_{k\text{-Vect}}(V \oplus V)$ may be thought of as the set of 2×2 matrices whose entries are themselves endomorphisms of V. That is, we have the picture

$$\mathrm{End}_{k\text{-Vect}}(V \oplus V) \cong \begin{bmatrix} \mathrm{End}_{k\text{-Vect}}(V) & \mathrm{End}_{k\text{-Vect}}(V) \\ \mathrm{End}_{k\text{-Vect}}(V) & \mathrm{End}_{k\text{-Vect}}(V) \end{bmatrix}$$

and clearly the set of matrices on the right are isomorphic to R^4. This interpretation of the endomorphism of a direct product comes from thinking of mapping the basis of each copy of V, except they can interact with each other.

If $V = k^{\oplus \mathbb{N}}$, then we find $R \cong \mathrm{End}_{k\text{-Vect}}(V \oplus V) \cong R^4$ so R does not satisfy the IBN property. □

Exercise VI.1.13. Let A be an abelian group such that $\mathrm{End}_{\mathrm{Ab}}(A)$ is a field of characteristic 0. Prove that $A \cong \mathbb{Q}$. (Hint: Prove that A carries a $\mathbb{Q}$-vector space structure; what must its dimension be?)

Solution. Recall that a field of characteristic 0 must contain a copy of $\mathbb{Q}$ (Exercise V.4.17). Thus, A has the structure of a $\mathbb{Q}$-vector space. Recall that $\mathrm{End}(A \oplus B)$ can be thought of as the set of 2×2 matrices of the form

$$\begin{bmatrix} \mathrm{End}(A) & \mathrm{Hom}(B, A) \\ \mathrm{Hom}(A, B) & \mathrm{End}(B) \end{bmatrix}$$

so that homomorphisms from A and B interact with each other. Suppose $\dim(A) > 1$ so we can write $\mathrm{End}(A) = \mathrm{End}(\mathbb{Q}^m \oplus \mathbb{Q}^n)$ with $m, n \geq 1$. Note that the description of $\mathrm{End}(A \oplus B)$ means this ring is not a field. Indeed, consider the matrix

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

which is nilpotent and has determinant zero. It is clearly non-invertible, so this contradicts the assumption that $\mathrm{End}(A)$ is a field. Hence, it must be the case the $\dim(A) = 1$ so $A \cong \mathbb{Q}$. $\square$

Exercise VI.1.14. Let V be a finite-dimensional vector space, and let $\varphi : V \to V$ be a homomorphism of vector spaces. Prove that there is an integer n such that $\ker \varphi^{n+1} = \ker \varphi^n$ and $\mathrm{im}\ \varphi^{n+1} = \mathrm{im}\ \varphi^n$.

Show that both claims may fail if V has infinite dimension.

Solution. Consider the following chain of vector spaces

$$V \supseteq \varphi(V) \supseteq \varphi^2(V) \supseteq \cdots$$

where each step either preserves or lowers the dimension of the vector space. Since V is finite-dimensional, the dimension cannot keep decreasing. Thus, there exists some integer m such that $\varphi^m(V) = \varphi^{m+1}(V)$.

Similarly, we have the chain of vector spaces

$$0 \subseteq \ker \varphi \subseteq \ker \varphi^2 \subseteq \cdots$$

where each step either preserves or increases the dimension of the vector space. Since V is finite-dimensional, the dimension cannot keep increasing. Thus, there exists some integer m' such that $\ker \varphi^{m'} = \ker \varphi^{m'+1}$. Finally, we only need to set $n = \max\{m, m'\}$.

For a counterexample in the case of infinite dimension, let $V = \mathbb{Q}^{\oplus \mathbb{N}}$ and consider φ which maps a_i to a_{i+1}. Clearly the image of φ is smaller each iteration, but it never terminates for a finite integer. Similarly, the kernel of φ increases each iteration, but it doesn't terminate for a finite integer. $\square$

Exercise VI.1.15. Consider the question of Exercise 1.14 for free R-modules F of finite rank, where R is an integral domain that is not a field. Let $\varphi : F \to F$ be an R-module homomorphism.

What property of R immediately guarantees that $\ker \varphi^{n+1} = \ker \varphi^n$ for $n \gg 0$?

Show that there is an R-module homomorphism $\varphi : F \to F$ such that $\operatorname{im} \varphi^{n+1} \subsetneq \operatorname{im} \varphi^n$ for all $n \geq 0$.

Solution. To do. $\square$

Exercise VI.1.16. Let M be a module over a ring R. A *finite composition series* for M (if it exists) is a decreasing sequence of submodules

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$

in which all quotients M_i/M_{i+1} are *simple* R-modules (cf. Exercise III.5.4). The *length* of a series is the number of strict inclusions. The *composition factors* are the quotients M_i/M_{i+1}.

Prove a Jordan-Hölder theorem for modules; any two finite composition series of a module have the same length and the same (multiset of) composition factors. (Adapt the proof of Theorem IV.3.2.)

We say that M has *length* m if M admits a finite composition series of length m. This notion is well-defined as a consequence of the result you just proved.

Solution. Let

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$

be a composition series. We prove this by induction on m. If $m = 0$, then M is trivial so there is nothing to prove. Assume $m > 0$ and let

$$M = M'_0 \supsetneq M'_1 \supsetneq \cdots \supsetneq M'_m = \langle 0 \rangle$$

be another composition series for M. If $M_1 = M'_1$ then the result follows from the induction hypothesis since M_1 has length $m - 1 < m$.

Thus, we may assume $M_1 \neq M'_1$. Then, since M_1 and M'_1 are maximal in M, we must have $M_1 + M'_1 = M$. Let $K = M_1 \cap M'_1$ and consider the composition series

$$K \supsetneq K_1 \supsetneq \cdots \supsetneq K_r = \langle 0 \rangle.$$

By the isomorphism theorems for modules, we have

$$\frac{M_1}{K} = \frac{M_1}{M_1 \cap M'_1} \cong \frac{M_1 + M'_1}{M'_1} = \frac{M}{M'_1}, \quad \frac{M'_1}{K} \cong \frac{M}{M_1}$$

are simple modules. Then we can construct new composition series for M, namely

$$M \supsetneq M_1 \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq \langle 0 \rangle$$

and

$$M \supsetneq M'_1 \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq \langle 0 \rangle$$

which only differ in the first step. These two series have the same length and the same quotients.

Now we show that the first of these two series has the same length and quotients as the original series. We can see that

$$M_1 \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq K_r$$

is a composition series for M_1. By the induction hypothesis, it must have the same length and quotients as

$$M_1 \supsetneq M_2 \supsetneq \cdots \supsetneq M_m$$

proving our claim.

Similarly, we can show that

$$M_1' \supsetneq K \supsetneq K_1 \supsetneq \cdots \supsetneq K_r$$

has the same length and quotients as

$$M_1' \supsetneq M_2' \supsetneq \cdots \supsetneq M_m'.$$

Thus, the statement follows. □

Exercise VI.1.17. Prove that a k-vector space V has finite length as a module over k (cf. Exercise 1.16) if and only if it is finite-dimensional and that in this case its length equals its dimension.

Solution. Suppose V is finite-dimensional and let B be a basis for V. Then we may construct the composition series

$$V = \operatorname{span}(B) \supsetneq \operatorname{span}(B \setminus \{b_1\}) \supsetneq \operatorname{span}(B \setminus \{b_1, b_2\}) \supsetneq \cdots \supsetneq \operatorname{span}(\emptyset) = \langle 0 \rangle$$

which has finite length this B is finite. It is evident from this construction that the length of V is equal to its dimension.

If V has finite length as a module over k, consider a composition series

$$V = V_0 \supsetneq V_1 \supsetneq \cdots \supsetneq V_n = \langle 0 \rangle$$

of length n. Suppose V is not finite dimensional and let $B = \{v_1, \dots, v_n\}$ be a linearly independent set. Then there exists a $v_{k+1} \in V \setminus B$ such that $B \cup \{v_{k+1}\}$ is still linearly independent. But then we may repeat this and construct a composition series for V of infinite length, contradicting our assumption that V has finite length. Thus, V must be finite dimensional (and as shown above, its dimension is equal to its length). □

Exercise VI.1.18. Let M be an R-module of finite length m (cf. Exercise 1.16).

- Prove that every submodule N of M has finite length $n \leq m$. (Adapt the proof of Proposition IV.3.4.)
- Prove that the 'descending chain condition' (d.c.c.) for submodules holds in M. (Use induction on the length.)
- Prove that if R is an integral domain that is not a field and F is a free R-module, then F has finite length if and only if it is the 0-module.

Solution. Assume M has a composition series

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$

and let N be a submodule of M. Consider the series

$$N = M \cap N \supsetneq M_1 \cap N \supsetneq \cdots \supsetneq M_m \cap N = \langle 0 \rangle.$$

We claim that this is a composition series for N. To verify this, we only need to show that

$$\frac{M_i \cap N}{M_{i+1} \cap N}$$

is either trivial or isomorphic to M_{i+1}/M_i. To see that this is true, consider the homomorphism

$$M_i \cap N \hookrightarrow M_i \twoheadrightarrow \frac{M_i}{M_{i+1}}$$

which clearly has kernel $M_{i+1} \cap N$. By the first isomorphism theorem, we have an injective homomorphism

$$\frac{M_i \cap N}{M_{i+1} \cap N} \hookrightarrow \frac{M_i}{M_{i+1}}$$

which identifies the former with a submodule of the latter. Since the latter is a simple module, our claim follows. Furthermore, removing the trivial quotients forces the length of N to be less than or equal to that of M.

Now we prove that M satisfies the d.c.c. for submodules. We show the much stronger result that every chain of submodules of M can be refined to a composition series for M. Let

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_k = \langle 0 \rangle$$

be a chain of submodules of M. We know $k \leq m$ by the Jordan-Hölder theorem for modules. If $k = m$ then we already have a composition series so suppose $k < n$. Then there exists some i such that M_i/M_{i+1} is not a simple module. That is, there exists a submodule M_i' such that $M_i \supsetneq M_i' \supsetneq M_{i+1}$ and we obtain a chain of length $k + 1$. If $k + 1 = n$, then we are done. Otherwise, we may repeat until we have constructed a chain of length n, at which point we have constructed a composition series for M. This result implies our claim because for any descending chain of submodules of M, we may extend it into a composition series of M. This series is certainly bounded, so the original descending chain must stabilize.

Finally, suppose R is an integral domain that is not a field and let F be a free $R-$ module. Clearly if $F = \langle 0 \rangle$ then it has finite length. Now suppose F has finite length and recall that $F \cong R^n$. Suppose $n \geq 1$. Since F has finite length, it satisfies the d.c.c. for submodules. In particular, it satisfies the d.c.c. for ideals of R, so R is an Artinian ring. However, by Exercise V.1.10, an integral domain is Artinian if and only if it is a field, contradicting our hypothesis. Thus, $F \cong R^0 = \langle 0 \rangle$. □

Exercise VI.1.19. Let k be a field, and let $f(x) \in k[x]$ be any polynomial. Prove that there exists a multiple of $f(x)$ in which all exponents of nonzero monomials are *prime* integers. (Example: for $f(x) = 1 + x^5 + x^6$,

$$(1 + x^8 + x^6)(2x^2 - x^3 + x^5 - x^8 + x^9 - x^{10} + x^{11}) \\ = 2x^2 - x^3 + x^5 + 2x^7 + 2x^{11} - x^{13} + x^{17}.)$$

(Hint: $k[x]/(f(x))$ is a finite-dimensional k-vector space.)

Solution. The vector space $V = k[x]/(f(x))$ has finite dimension, say n. Take the monomials

$$x^{p_1}, x^{p_2}, \ldots, x^{p_{n+1}}$$

where p_i is an arbitrary prime integer and consider their remainders mod f as elements of V. Since there are $n+1$ elements, they must be linearly dependent. That is, there exist $a_i \in k$ such that

$$h(x) = a_1 x^{p_1} + a_2 x^{p_2} + \cdots + a_{n+1} x^{p_{n+1}}$$

where $h(x) \in (f(x))$. That is, $h(x)$ is a multiple of $f(x)$ in which all exponents of nonzero monomials are prime integers. □

Exercise VI.1.20. Let A, B be sets. Prove that the free groups $F(A), F(B)$ are isomorphic if and only if there is a bijection $A \cong B$. (For the interesting direction: remember that $F(A) \cong F(B) \implies F^{ab}(A) \cong F^{ab}(B)$, by Exercise II.7.12). This extends the result of Exercise II.7.13 to possibly infinite sets A, B.

Solution. It is clear that if $A \cong B$, then the corresponding free groups are isomorphic. Suppose $F(A) \cong F(B)$ and recall that this implies $F^{ab}(A) \cong F^{ab}(B)$. Note that both of these groups are free $\mathbb{Z}$-modules. However, if they are isomorphic, then it must the case that there is a bijection between their bases. That is, $A \cong B$. □

VI.2 Homomorphisms of free modules, I

Exercise VI.2.1. Prove that the subset of $\mathcal{M}_2(R)$ consisting of matrices of the form

$$\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$$

is a group under matrix multiplication and is isomorphic to $(R, +)$.

Solution. It is evident that the identity of this group is the identity matrix I_2. Furthermore, it is closed under multiplication:

$$\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ r+s & 1 \end{pmatrix}$$

and since R is closed under addition, this matrix is contained in the group. The multiplication makes it evident that inverse elements have the form

$$\begin{pmatrix} 1 & 0 \\ -r & 1 \end{pmatrix}$$

where $-r$ is the additive inverse of $r \in R$. The isomorphism is also evident; simply identify

$$r \to \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$$

and the inverse homomorphism is just as clear. □

Exercise VI.2.2. Prove that matrix multiplication is associative.

Solution. Let A be a $m \times n$ matrix, B a $n \times p$ matrix, and C a $p \times q$ matrix. Let $R = AB$ and $S = (AB)C$. We have

$$\begin{aligned} s_{ij} &= \sum_{k=1}^{p} r_{ik} c_{kj} \\ &= \sum_{k=1}^{p} \left(\sum_{l=1}^{n} a_{il} b_{lk} \right) c_{kj} \\ &= \sum_{k=1}^{p} \sum_{l=1}^{n} a_{il} b_{lk} c_{kj} \end{aligned}$$

where the third equality follows from distributivity of multiplication over addition in R. Now let $R = BC$ and $S = A(BC)$. We have

$$\begin{aligned} s_{ij} &= \sum_{l=1}^{n} a_{il} r_{lj} \\ &= \sum_{l=1}^{n} a_{il} \left(\sum_{k=1}^{p} b_{lk} c_{kj} \right) \\ &= \sum_{l=1}^{n} \sum_{k=1}^{p} a_{il} b_{lk} c_{kj} \end{aligned}$$

where the last equality follows from distributivity of multiplication over addition. Finally, the associativity of multiplication and commutativity of addition in R shows that these two sums are equal, so $(AB)C = A(BC)$. $\square$

Exercise VI.2.3. Prove that both $\mathcal{M}_n(R)$ and $\mathrm{Hom}_R(R^n, R^n)$ are R-algebras in a natural way and the bijection $\mathrm{Hom}_R(R^n, R^n) \cong \mathcal{M}_n(R)$ of Corollary 2.2 is an isomorphism of R-algebras. In particular, if the matrix M corresponds to the homomorphism $\varphi : R^n \to R^n$, then M is invertible in $\mathcal{M}_n(R)$ if and only if φ is an isomorphism.

Solution. Indeed, $\mathcal{M}_n(R)$ is a ring under component addition and matrix multiplication. It is an R-algebra because for all $r \in R$ and $A, B \in \mathcal{M}_n(R)$, we have

$$r \cdot (AB) = (r \cdot A)B = A(r \cdot B)$$

by the properties of scalar multiplication of matrices. Showing that $\mathrm{Hom}_R(R^n, R^n)$ is an R-algebra amounts to a similar, but more notationally heavy, computation. Recall that the bijection ϕ between the two sets sends a matrix A to the homomorphism φ defined as $\varphi(v) = Av$. To show it is an isomorphism, we only need to show that it is an algebra homomorphism. Indeed, we have (with slight abuse of notation at some points)

- $\phi(I_n)(v) = I_n v = \mathrm{id}$
- $\phi(r \cdot A)(v) = (r \cdot A)(v) = r \cdot (Av) = r \cdot \varphi(A)$
- $\phi(A + B)(v) = (A + B)(v) = Av + Bv = \varphi(A) + \varphi(B)$
- $\phi(AB)(v) = (AB)(v) = A(Bv) = \varphi(A) \circ \varphi(B)$

so the bijection is a homomorphism of R-algebras, making it an isomorphism. The statement regarding when a matrix is invertible follows immediately. I am curious as to how this aligns with the determinant. $\square$

Exercise VI.2.4. Prove Corollary 2.2.

Corollary 2.2. *The correspondence introduced in Lemma 2.1 gives an isomorphism of R-modules*

$$\mathcal{M}_{m,n}(R) \cong \mathrm{Hom}_R(R^n, R^m).$$

Solution. Indeed, the correspondence in Lemma 2.1 is bijective; all matrices $M \in \mathcal{M}_{m,n}(R)$ are mapped to a homomorphism $\varphi \in \mathrm{Hom}_R(R^n, R^m)$ and all homomorphisms are mapped to a matrix. We checked above that the two sets are isomorphic as R-algebras so they must be isomorphic as R-modules. □

Exercise VI.2.5. Give a formal argument proving Proposition 2.7.

Proposition 2.7. *Two matrices $P, Q \in \mathcal{M}_{m,n}(R)$ are equivalent if Q may be obtained from P be a sequence of elementary operations.*

Solution. We will only treat the case of elementary row operations. To switch the i- and j-th rows of an $m \times n$ matrix, consider the identity matrix with the i- and j-th rows switched. Similarly, to add a multiple of the i-th row to the j-th row, consider the identity matrix with the entry c at position i, j. To multiply all entries in the i-th row of a matrix by a unit of R, consider the identity matrix with the entry in the i-th row replaced by a unit r. We verify that each of these matrices is invertible.

In the first case, we show the corresponding homomorphism is an isomorphism. Suppose we have two vectors u and v such that $\varphi(u) = \varphi(v)$. Then certainly switching the corresponding rows of these vectors preserves equality. Similarly, all vectors in R^n are in the image of φ by simply switching the rows of the desired elements.

In the second case, we explicitly construct an inverse matrix. Namely, consider the identity matrix with the entry $-c$ at position i, j. Clearly this subtracts the multiple of the i-th row from the j-th row and hence inverts the transformation of the original matrix.

For the third example, we use the fact that r is a unit and hence has an inverse r^{-1}. Then the identity matrix with the entry in the i-th row replaced by r^{-1} is an explicit realization of the inverse.

Since each of these matrices is invertible, the corresponding homomorphisms are all isomorphisms and preserve the "action" of matrices P and Q. □

Exercise VI.2.6. A matrix with entries in a field is in *row echelon form* if

- its nonzero rows are all above the zero rows and
- the leftmost nonzero entry of each row is 1, and it is strictly to the right of the leftmost nonzero entry of the row above it.

The matrix is further in *reduced* row echelon form if

- the leftmost nonzero entry of each row is the only nonzero entry in its column.

The leftmost nonzero entries in a matrix in row echelon form are called *pivots*.

Prove that any matrix with entries in a field can be brought into reduced echelon form by a sequence of elementary operations on *rows*. (This is what is more properly called *Gaussian elimination*.)

Solution. Let $A = (a_{ij})$ be a $m \times n$ matrix over a field. We start by appropriately switching all zero rows to the bottom of the matrix. Recalling our elementary row operations, we may multiply the first row by a_{11}^{-1} and subtract necessary multiples of the first row, yielding

$$\begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

From here, we may repeat by multiplying the second row by a_{22}^{-1} and subtracting necessary multiples from all rows below it, switching zero rows to the bottom as they appear. This process eventually terminates and yields a matrix in row echelon form. □

Exercise VI.2.7. Let M be a matrix with entries in a field and in reduced row echelon form (Exercise 2.6). Prove that if a row vector $\boldsymbol{r}$ is a linear combination $\sum a_i r_i$ of the nonzero rows of M, then a_i equals the component of $\boldsymbol{r}$ at the position corresponding to the pivot on the i-th row of M. Deduce that the nonzero rows of M are linearly independent.

Solution. Let b_i be the component of $\boldsymbol{r}$ at the position corresponding to the pivot of the i-th row of M. Suppose the pivot of the i-th row is located in the j-th column. Then $b_i = a_i \cdot 1$ because the only nonzero entry in the j-th column is 1 (since M is in reduced echelon form). Thus, $a_i = b_i$.

If $\boldsymbol{r}$ is the zero vector, then it must be the case that each a_i is 0. That is, the nonzero rows of M are linearly independent. Thus, □

Exercise VI.2.8. Two matrices M, N are *row-equivalent* if $M = PN$ for an invertible matrix P. Prove that this is indeed an equivalence relation, and that two matrices with entries in a field are row-equivalent if and only if one may be obtained from the other by a sequence of elementary operations on rows.

Solution. Let $M \sim N$ denote row-equivalent matrices. Clearly $M \sim N$ as $M = IM$. If $M \sim N$ then we have $M = PN$ for some invertible matrix P. But then we have $N = P^{-1}M$ so $N \sim P$. Finally, if $M \sim N$ and $N \sim P$, we have

$M = RN$ and $P = SN$. Then $M = RS^{-1}P$, and RS^{-1} is clearly invertible so $M \sim P$. Thus, row-equivalence is an equivalence relation.

The second part of the claim follows from the fact that $GL_n(k)$, the group of invertible matrices of a field, is generated by elementary matrices, which are themselves invertible (obviously). $\square$

Exercise VI.2.9. Let k be a field, and consider row-equivalence (Exercise 2.8) on the set of $m \times n$ matrices $\mathcal{M}_{m,n}(k)$. Prove that each equivalence class contains exactly one matrix in reduced row echelon form (Exercise 2.6). (Hint: To prove uniqueness, argue by contradiction. Let M, N be different row-equivalent reduced row echelon matrices; assume that they have the minimum number of columns with this property. If the leftmost column at which M and N differ is the k-th column, use the minimality to prove that M, N may be assumed to be of the form

$$\left(\begin{array}{c|c} I_{k-1} & * \\ \hline 0 & * \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c} I_{k-1} & * \end{array}\right).$$

Use Exercise 2.7 to obtain a contradiction.)

The unique matrix in reduced row echelon form that is row-equivalent to a given matrix M is called the *reduced echelon form* of M.

Solution. Certainly each each equivalence class is nonempty as it contains a matrix of the form

$$\left(\begin{array}{c|c} I_{k-1} & * \\ \hline 0 & 0 \end{array}\right)$$

Now suppose M, N are different row equivalent matrices in reduced row echelon form with the minimum number of columns. Suppose the leftmost column at which M and N differ is the k-th column. Construct two matrices M' and N' by selecting all columns with pivot elements to the left of the k-th column, along with the k-th column. Then we have M' and N' are of the form

$$\left(\begin{array}{c|c} I_{k-1} & * \\ \hline 0 & * \end{array}\right) \quad \text{or} \quad \left(\begin{array}{c|c} I_{k-1} & * \end{array}\right)$$

(the case depends on whether $k > n$). Then M' and N' are row equivalent since we are only adjusting columns and we assumed M and N are row equivalent. In either case, the rows of M' and N' are linearly independent so it must be the case that $M' = N'$ and $M = N$. $\square$

Exercise VI.2.10. The *row space* of a matrix M is the span of its rows; the *column space* of M is the span of its columns. Prove that row-equivalent matrices have the same row space and isomorphic column spaces.

Solution. Recall that M and N are row-equivalent if there exists an invertible matrix P such that $M = PN$. Then the rows of M are a linear combination of the rows of N. If x is in the span of the rows of M then it is a linear combination of the rows of M. But then it is also a linear combination of the rows of N so the row space of M is a subset of the row space of N. Similarly, since $N = P^{-1}M$, the row space of N is a subset of the row space of M so the two are equal.

By Exercise 2.9, M and N have the same reduced echelon form. Furthermore, the dimension of the column space of a matrix is given by the number of pivot columns in its reduced echelon form since row operations preserve linear relations between columns. Thus, the column space of M and N have the same dimension so they are isomorphic as vector spaces. □

Exercise VI.2.11. Let k be a field and $M \in \mathcal{M}_{m,n}(k)$. Prove that the dimension of the space spanned by the rows of M equals the number of nonzero rows in the reduced echelon form of M (cf. Exercise 2.9).

Solution. Note that the reduced echelon form of M can be obtained through a sequence of elementary operations. That is, if N is the reduced echelon form of M, then we have $N = PM$ so the two are row-equivalent. By Exercise 2.10, the two matrices have the same row space. Finally, the dimension of the row space is equal to the number of nonzero rows in the reduced echelon form of M (since the nonzero rows contain pivot elements). Thus, the dimension of the row space of M is equal to the number of nonzero rows in N. □

Exercise VI.2.12. Let k be a field, and consider row-equivalence on $\mathcal{M}_{m,n}(k)$ (Exercise 2.8). By Exercise 2.10, row-equivalent matrices have the same row space. Prove that, conversely, there is exactly one row-equivalence class in $\mathcal{M}_{m,n}(k)$ for each subspace of k^n of dimension $\leq m$.

Solution. Given a subspace V of dimension $d \leq n$, we know the row-equivalence class is nonempty since it contains the matrix whose rows are a basis of V, call it A. Suppose we have a second matrix B whose row space is V. Since the two are row-equivalent, we have that for all $x \in k^n$, there exists $y \in k^n$ such that $x^t A = y^t B$. In particular, let $e_i \in k^n$ for $1 \leq i \leq n$ denote the standard basis of k^n and let $y_i \in k^n$ satisfy $e_i^t A = y_i^t B$ (in such a way that the y_i are linearly independent). Construct a matrix P such that the i-th row of P is y_i. Then clearly we have $A = PB$ for an invertible matrix P so the two are row-equivalent. □

Exercise VI.2.13. The set of subspaces of given dimension in a fixed vector space is called a *Grassmannian*. In Exercise 2.12 you have constructed a bijection between the Grassmannian of r-dimensional subspaces of k^n and the set of reduced row echelon matrices with n columns and r nonzero rows.

For $r = 1$, the Grassmannian is called the *projective space*. For a vector space V, the corresponding projective space $\mathbb{P}V$ is the set of 'lines' (1-dimensional subspaces) in V. For $V = k^n$, $\mathbb{P}V$ may be denoted $\mathbb{P}_k^{n-1}$, and the field k may be omitted if it is clear from the context. Show that $\mathbb{P}_k^{n-1}$ may be written as a union $k^{n-1} \cup k^{n-2} \cup \cdots \cup k^1 \cup k^0$, and describe each of these subsets 'geometrically'.

Thus, $\mathbb{P}^{n-1}$ is the union of n 'cells', the largest one having dimension $n-1$ (accounting for the choice of notation). Similarly, all Grassmannians may be written as unions of cells. These are called *Schubert cells*.

Prove that the Grassmannian of $(n-1)$-dimensional subspaces of k^n admits a cell decomposition entirely analogous to that of $\mathbb{P}_k^{n-1}$. (This phenomenon will be explained in Exercise VIII.5.17.)

Solution. Think of k^{n+1} as $k^n \times k$. Then each line through the origin either intersects $k^n \times \{1\}$ at a unique point or it lies in the hyperplane $k^n \times \{0\}$. Thus, the lines in k^{n+1} are a union of $k^n \times \mathbb{P}^{n-1}$. Repeating inductively shows that $\mathbb{P}_k^{n-1}$ is a union $k^{n-1} \cup \cdots \cup k^1 \cup k^0$ (where the last set is included for the origin itself). Each of these subsets is the hyperplane of lines in k^m. The most tangible example is $\mathbb{R}^3$ and $\mathbb{RP}^2$.

When working with the Grassmannian of n-dimensional subspaces of k^{n+1}, simply consider the line normal to the n-dimensional hyperplane. Clearly the two are in bijection so the cell decomposition is simply reversed. For a more explicit example, consider $\mathbb{R}^3$ and the Grassmannian of 2-dimensional subspaces, or planes. Each plane through the origin has a normal line, and this set of normal lines is equivalent to $\mathbb{RP}^2$. The lines which intersect $\mathbb{R}^2 \times \{0\}$ correspond to planes which contain the vertical copy of $\mathbb{R}$. The intersection of planes not in this set is $\mathbb{R}^0$, while the intersection of the planes in this set is $\mathbb{R}^1$. Repeating once more with the set of planes whose normal lines intersect $\mathbb{R} \times \{0\}$ yields $\mathbb{R}^2$ since there is only one such plane. $\square$

Exercise VI.2.14. Show that the Grassmannian $\mathrm{Gr}_k(2,4)$ of 2-dimensional subspaces of k^4 is the union of 6 Schubert cells: $k^4 \cup k^3 \cup k^2 \cup k^2 \cup k^1 \cup k^0$. (Use Exercise 2.12; list all the possible reduced echelon forms.)

Solution. A 2-dimensional subspace of k^4 corresponds to a reduced echelon matrix of rank 2. There are exactly 6 of these, namely:

$$\begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{pmatrix}, \quad \begin{pmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}, \quad \begin{pmatrix} 1 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Thus, $\mathrm{Gr}_k(2,4)$ decomposes into exactly 6 Schubert cells. Note that the matrix with m free elements corresponds to the Schubert cell k^m. This is because each subspace is characterized by the values of the free elements. In particular, the sixth matrix corresponds with k^0 while the third matrix corresponds with k^2. $\square$

Exercise VI.2.15. Prove that a square matrix with entries in a field is invertible if and only if it is equivalent to the identity, if and only if it is row-equivalent to the identity, if and only if its reduced echelon form is the identity.

Solution. Let M be a square matrix with entires in a field. If M is invertible, then it has an inverse M^{-1} such that $I = M^{-1}M$. Since M^{-1} is invertible, M is row-equivalent to the identity.

If M is row-equivalent to the identity, then there exists an invertible matrix P such that $I = PM$. Since P is invertible, it is a product of elementary matrices. That is, a sequence of row operations on P yields the identity, which is in reduced echelon form.

Finally, suppose the reduced echelon form of M is the identity. Then there is a sequence of row operations which transform M into the identity. This sequence of row operations can be expressed as a product of elementary matrices. This product of elementary matrices is the inverse of M, so M is invertible. $\square$

Exercise VI.2.16. Prove Proposition 2.10.

Proposition 2.10. *Over a field, every $m \times n$ matrix is equivalent to a matrix of the form*

$$\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right)$$

(where $r \leq \min(m, n)$ and '0' stands for null matrices of appropriate sizes).

Solution. Let M be an $m \times n$ matrix over a field with rank r. After appropriate row operations, we may assume the first r rows of M are linearly independent. Then we may apply Gaussian elimination to the first r rows to obtain a matrix of the form

$$\left(\begin{array}{c|c} I_r & * \\ \hline * & * \end{array}\right)$$

Add appropriate linear combinations of the first r columns to eliminate the top right block. Since the remaining $m - r$ rows are linearly dependent, they must be a linear combination of the first r rows. Thus, the bottom right block must also be zero. Finally, the proper linear combination of the first r rows will eliminate the bottom left block. What remains is a matrix of the form stated in the problem. $\square$

Exercise VI.2.17. Prove Proposition 2.11.

Proposition 2.11. *Let R be a Euclidean domain, and let $P \in \mathcal{M}_{m,n}(R)$. Then P is equivalent to a matrix of the form*

$$\left(\begin{array}{ccc|c} d_1 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & d_r & 0 \\ \hline 0 & \cdots & 0 & 0 \end{array}\right)$$

with $d_1 \mid \cdots \mid d_r$.

Solution. Let M be an $m \times n$ matrix over a Euclidean domain with rank r. After appropriate row operations, we may assume the first r rows of M are linearly independent. Following the Euclidean algorithm, we may add multiples of other rows to ensure that a_{11} is the gcd of the entries in the first column. Adding appropriate multiples of this row to the remaining rows and multiples of this column to the remaining columns yields a matrix of the form

$$\left(\begin{array}{c|ccc} d_1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & M' & \\ 0 & & & \end{array}\right)$$

where M' is an $(m-1) \times (n-1)$ matrix with rank $r-1$.

Repeating this process on M' and on subsequent matrices yields a matrix of the form stated in the problem. Now we only need to show that $d_1 \mid \cdots \mid d_r$, for which we take inspiration from the text. Indeed, suppose $d_i \nmid d_{i+1}$. Then we may add the $(i+1)$-th row to the i-th row and repeat the process. Ultimately, we must reach the condition $d_i \mid d_{i+1}$. □

Exercise VI.2.18. Suppose $\alpha : \mathbb{Z}^3 \to \mathbb{Z}^2$ is represented by the matrix

$$\begin{pmatrix} -6 & 12 & 18 \\ -15 & 36 & 54 \end{pmatrix}$$

with respect to the standard bases. Find bases of $\mathbb{Z}^3, \mathbb{Z}^2$ with respect to which α is given by a matrix of the form obtained in Proposition 2.11.

Solution. Applying the algorithm described above, we find that applying the following change of basis yields a matrix in the Smith normal form:

$$\begin{pmatrix} 2 & -1 \\ 10 & -4 \end{pmatrix} \begin{pmatrix} -6 & 12 & 18 \\ -15 & 36 & 54 \end{pmatrix} \begin{pmatrix} 1 & -2 & 0 \\ 0 & 1 & 3 \\ 0 & -1 & -2 \end{pmatrix} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 12 & 0 \end{pmatrix}$$

so the above matrices are the bases with which α is given in the Smith normal form. Interestingly, the inverses of these matrices are not elements of $\mathbb{Z}^3$ or $\mathbb{Z}^2$ respectively. □

Exercise VI.2.19. Prove Corollary IV.6.5 again as a corollary of Proposition 2.11. In fact, prove the general fact that every *finitely generated* abelian group is a direct sum of cyclic groups.

Solution. Let G be a finitely generated abelian group. Then G is a quotient of $\mathbb{Z}^n$ by a finitely generated free abelian group, say F, and F is a free $\mathbb{Z}$-module. Consider a matrix M whose rows are composed of a basis for F. By Proposition 2.11, M is equivalent to a matrix in the Smith normal form. That is, there is a basis $\{d_1e_1, \ldots, d_re_r\}$ for F such that $d_i \mid d_{i+1}$. Then

$$F = d_1\mathbb{Z} \oplus d_2\mathbb{Z} \oplus \cdots \oplus d_r\mathbb{Z}$$

so we find

$$G = \frac{\mathbb{Z}^n}{F} = \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}}$$

and G is a direct sum of cyclic groups. $\square$

VI.3 Homomorphisms of free modules, II

Exercise VI.3.1. Use Gaussian elimination to find all integer solutions of the system of equations

$$\begin{cases} 7x - 36y + 12z = 1, \\ -8x + 42y - 14z = 2. \end{cases}$$

Solution. Transforming the system of equations into a matrix and applying Gaussian elimination yields the factorization

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 7 & 6 \\ -8 & -7 \end{pmatrix} \cdot \begin{pmatrix} 7 & -36 & 12 \\ -8 & 42 & -14 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 4 & -3 \end{pmatrix},$$

or $D = M \cdot A \cdot N$. As we are trying to solve $A\boldsymbol{x} = \boldsymbol{b}$, we now can now solve $D\boldsymbol{y} = M\boldsymbol{b}$. Finally, we solve $\boldsymbol{x} = N\boldsymbol{y}$ for a solution of

$$\boldsymbol{x} = \begin{pmatrix} 19 \\ -11 - z \\ -44 - 3z \end{pmatrix}$$

so there are infinitely many solutions based on the free variable z. $\square$

Exercise VI.3.2. Provide details for the proof of Lemma 3.2.

Lemma 3.2. *Let A be a square matrix with entries in an integral domain R.*

- *Let A' be obtained from A by switching two rows or two columns. Then* $\det(A') = -\det(A)$.
- *Let A' be obtained from A by adding to a row (column) a multiple of another row (column). Then* $\det(A') = \det(A)$.

- *Let A' be obtained from A by multiplying a row (column) by an element $c \in R$. Then* $\det(A') = c\det(A)$.

In other words, the effect of an elementary operation on $\det A$ *is the same as multiplying* $\det A$ *by the determinant of the corresponding matrix.*

Solution. Switching two rows is equivalent to multiplying each $\sigma \in S_n$ by a fixed transposition. Then the sign of each permutation is switched so we have

$$\det(A') = \sum_{\sigma \in S_n} (-1)^{\sigma+1} \prod_{i=1}^{n} a_{i\sigma(i)} = -\det(A)$$

yielding the desired result.

For the third point, each product has exactly one c in it so we find

$$\det(A') = \sum_{\sigma \in S_n} (-1)^{\sigma} c \prod_{i=1}^{n} a_{i\sigma(i)} = c\det(A)$$

yielding the desired result.

For the second point, note that $A' = (a_1, a_2, \ldots, a_i + ka_j, \ldots, a_n)$ so A and A' differ at only one row. Then we have

$$\begin{aligned}\det(A') &= \det(A) + \det(a_1, a_2, \ldots, ka_j, \ldots, a_n)\\ &= \det(A) + k\det(a_1, a_2, \ldots, a_j, \ldots, a_n).\end{aligned}$$

But then rows i and j are identical in the second matrix so it follows that the determinant of that matrix is 0. Thus, we are left with $\det(A') = \det(A)$. $\square$

Exercise VI.3.3. Redo Exercise II.8.8.

Exercise II.8.8. Prove that $\mathrm{SL}_n(\mathbb{R})$ is a *normal subgroup* of $\mathrm{GL}_n(\mathbb{R})$, and 'compute' $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$ as a well-known group.

Solution. Recall that $\mathrm{SL}_n(\mathbb{R})$ is the set of $n \times n$ matrices with determinant 1. Certainly this is a normal subgroup of $\mathrm{GL}_n(\mathbb{R})$ since it is the kernel of the homomorphism induced by det from $\mathrm{GL}_n(\mathbb{R})$ to $\mathbb{R}^\times$. Then by the first isomorphism theorem, we find that $\mathbb{R}^\times \cong \mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R})$. $\square$

Exercise VI.3.4. Formalize the discussion of 'universal identities': by what cocktail of universal properties is it true that if an identity holds in $\mathbb{Z}[x_1, \ldots, x_r]$, then it holds over every commutative ring R, for every choice of $x_i \in R$? (Is the commutativity of R necessary?)

Solution. This holds because $Z[x_1, \ldots, x_r]$ is a free object in the category of commutative rings, or commutative $\mathbb{Z}$-algebras. In particular, for every commutative ring R and set function $f : A \to R$, there exists a unique $\mathbb{Z}$-algebra homomorphism from $\mathbb{Z}[x_1, \ldots, x_r]$ to R. If the identity is preserved by homomorphisms, then it will hold in every commutative ring. Furthermore, the commutativity of R is not necessary but it is necessary that given a set-function f, we have $f(a)$ commutes with every element of R for all $a \in A$. □

Exercise VI.3.5. Let A be an $n \times n$ square invertible matrix with entries in a field, and consider the $n \times (2n)$ matrix $B = (A \mid I_n)$ obtained by placing the identity matrix to the side of A. Perform elementary row operations on B so as to reduce A to I_n (cf. Exercise 2.15). Prove that this transforms B into $(I_n \mid A^{-1})$.

(This is a much more efficient way to compute the inverse of a matrix than by using determinants as in §3.2.)

Solution. Each elementary row operation on B can be encoded as an elementary matrix whose product reduces A to I_n. That is, we have $PA = I_n$. But then $P = A^{-1}$ and since $PI_n = P$, it must be the case that $B = (I_n \mid P) = (I_n \mid A^{-1})$. □

Exercise VI.3.6. Let R be a commutative ring and $M = \langle m_1, \ldots, m_r\rangle$ a finitely generated R-module. Let $A \in \mathcal{M}_r(R)$ be a matrix such that $A \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Prove that $\det(A)m = 0$ for all $m \in M$. (Hint: Multiply by the adjoint.)

Solution. Denote the adjoint matrix of A by A'. Recall that $A'A = \det(A)I_n$. Multiplying both sides of the equation by the adjoint yields

$$A'A \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = A' \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

$$\det(A)I_n \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

so $\det(A)m_i = 0$ for all $m_i \in \langle m_1, \ldots, m_r\rangle$. Since this is a generating set for M, all $m \in M$ are linear combinations of m_i. Thus, we have $\det(A)m = 0$ for all $m \in M$. □

Exercise VI.3.7. Let R be a commutative ring, M a finitely generated R-module, and let J be an ideal of R. Assume $JM = M$. Prove that there exists an element $b \in J$ such that $(1+b)M = 0$. (Let $m_1, \ldots, m_r$ be generators for M. Find an $r \times r$ matrix B with entries in J such that $\begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = B \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}$. Then use Exercise 3.6.)

Solution. Let $\langle m_1, \ldots, m_r \rangle$ be a set of generators for M. Since $JM = M$, for all m_j in the generating set, there exists a finite sum

$$m_j = \sum_{i=0}^{r} b_i m_i.$$

Thus, we can construct a matrix B with entries in J such that

$$\begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = B \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}$$

which can be rearranged to $(I_r - B)(m_i)^T = 0$. Let $d = \det(I_r - B)$. Then $d \in 1 + J$ since $B \equiv 0 \mod J$. By Exercise 3.7, $dm = 0$ for all $m \in M$. That is, there exists $b \in J$ such that $(1+b)M = 0$. □

Exercise VI.3.8. Let R be a commutative ring, M be a finitely generated R-module, and let J be an ideal of R *contained in the Jacobson radical* of R (Exercise V.3.14). Prove that $M = 0 \iff JM = M$. (Use Exercise 3.7. This is *Nakayama's lemma*, a result with important applications in commutative algebra and algebraic geometry. A particular case was given as Exercise III.5.16.)

Solution. If $M = 0$, then clearly for all $b \in J$, we have $bM = 0 = M$ so $JM = M$. Now suppose $JM = M$. Recall that the Jacobson radical of a ring is the intersection of its maximal ideals. By Exercise 3.7, there exists some $b \in J$ such that $(1+b)M = 0$. Then $1+b$ is a unit in R so multiplying both sides by its inverse yields $M = 0$. □

Exercise VI.3.9. Let R be a commutative local ring, that is, a ring with a single maximal ideal $\mathfrak{m}$, and let M, N be finitely generated R-modules. Prove that if $M = \mathfrak{m}M + N$, then $M = N$. (Apply Nakayama's lemma, that is, Exercise 3.8, to M/N. Note that the Jacobson radical of R is $\mathfrak{m}$.)

Solution. If $M = \mathfrak{m}M + N$, then $M/N = \mathfrak{m}M/N$. By Nakayama's lemma, $M/N = 0$ so $M = N$. □

Exercise VI.3.10. Let R be a commutative local ring, and let M be a finitely generated R-module. Note that $M/\mathfrak{m}M$ is a finite-dimensional vector space over the field $R/\mathfrak{m}$; let $m_1, \dots, m_r \in M$ be elements whose cosets mod $\mathfrak{m}M$ form a basis of $M/\mathfrak{m}M$. Prove that $m_1, \dots, m_r$ generate M.

(Show that $\langle m_1, \dots, m_r \rangle + \mathfrak{m}M = M$; then apply Nakayama's lemma in the form of Exercise 3.9.)

Solution. We have $\langle \bar{m}_1, \dots, \bar{m}_r \rangle = M/\mathfrak{m}M$, where $\bar{m}_i = m_i \mod \mathfrak{m}M$. That is, $\langle m_1, \dots, m_r \rangle + \mathfrak{m}M = M$. Then, by Exercise 3.9, $\langle m_1, \dots, m_r \rangle = M$. □

Exercise VI.3.11. Explain how to use Gaussian elimination to find bases for the row space and the column space of a matrix over a field.

Solution. Recall that Gaussian elimination does not change the row space of the matrix. Then reducing a matrix to reduced echelon form yields a matrix whose rows have the same span as the row space of the original matrix and are linearly independent. Thus, they form a basis for the row space. Similarly, applying Gaussian elimination to the transpose of the matrix yields a basis for the column space. □

Exercise VI.3.12. Let R be an integral domain, and let $M \in \mathcal{M}_{m,n}(R)$, with $m < n$. Prove that the columns of M are linearly dependent over R.

Solution. Recall that M represents a homomorphism $f : R^n \to R^m$ and the column space of M is equal to the span of im f. If the columns of M are linearly independent, then the standard basis vectors of R^n map to a linearly independent set in R^m. That is, the rank of R^m must be greater than or equal to that of R^n, or $m \geq n$. Thus, if $n < m$, it must be the case that the columns of M are linearly dependent. □

Exercise VI.3.13. Let k be a field. Prove that a matrix $M \in \mathcal{M}_{m,n}(k)$ has rank $\leq r$ if and only if there exist matrices $P \in \mathcal{M}_{m,r}(k), Q \in \mathcal{M}_{r,n}(k)$ such that $M = PQ$. (Thus the rank of M is the smallest such integer.)

Solution. Suppose there exist $P \in \mathcal{M}_{m,r}(k), Q \in \mathcal{M}_{r,n}(k)$ such that $M = PQ$. Let $s = \text{rank } P, t = \text{rank } Q$. Then

$$P = \left(\begin{array}{c|c} I_s & 0 \\ \hline 0 & 0 \end{array}\right), \quad Q = \left(\begin{array}{c|c} I_t & 0 \\ \hline 0 & 0 \end{array}\right).$$

Including zero rows (columns) to the smaller identity matrix to make block multiplication possible yields

$$M = \left(\begin{array}{c|c} I_{\min(s,t)} & 0 \\ \hline 0 & 0 \end{array}\right)$$

and since $\min(s,t) \leq r$, the rank of $M \leq r$.

Now suppose M has rank $r' \leq r$. Consider the matrices

$$P = \left(\begin{array}{c|c} I_{r'} & 0 \\ \hline 0 & 0 \end{array}\right), \quad Q = \left(\begin{array}{c|c} I_{r'} & 0 \\ \hline 0 & 0 \end{array}\right).$$

Note that P and Q can be defined for all $r \geq r'$. Then their product is equivalent to M (up to multiplication by invertible matrices on the left and right, both of which preserve the rank of M). $\square$

Exercise VI.3.14. Generalize Proposition 3.11 to the case of finitely generated free modules over any integral domain. (Embed the integral domain in its field of fractions.)

Proposition 3.11. *Let*

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

be a short exact *sequence of finite-dimensional vector spaces. Then*

$$\dim(V) = \dim(U) + \dim(W).$$

Solution. Let

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

be a short exact sequence of finitely generated free modules over an integral domain R. Embed R in its field of fractions K. By Exercise 1.7, each module is naturally mapped to a vector space over K. In particular, if A' denotes the vector space corresponding to the module A, we have $\operatorname{rank}(A) = \dim(A')$. Then, by Proposition 3.11, we have $\dim(B') = \dim(A') + \dim(C')$ which translates into $\operatorname{rank}(B) = \operatorname{rank}(A) + \operatorname{rank}(C)$. $\square$

Exercise VI.3.15. Prove Proposition 3.13 for the case $N = 1$.

Proposition 3.13. *With notation as above,*

$$\chi(V_\bullet) = \sum_{i=0}^{N} (-1)^i \dim(H_i(V_\bullet)).$$

In particular, if $V_\bullet$ is exact, then $\chi(V_\bullet) = 0$.

Solution. Let

$$V_\bullet : \ 0 \longrightarrow V_1 \xrightarrow{\alpha_1} V_0 \longrightarrow 0$$

be a complex of finite-dimensional vector spaces and linear maps. By definition, we have $\chi(V_\bullet) = \dim(V_0) - \dim(V_1)$. Furthermore, we find

$$H_0(V_\bullet) = \frac{V_0}{\operatorname{im}(\alpha_1)}, \quad H_1(V_\bullet) = \ker(\alpha_1).$$

By Proposition 3.11,

$$\begin{aligned}
\dim(H_0(V_\bullet)) &= \dim(V_0) - \dim(\mathrm{im}(\alpha_1)),\\
\dim(H_1(V_\bullet)) &= \dim(\ker(\alpha_1)),\\
\dim(V_1) &= \dim(\ker(\alpha_1)) + \dim(\mathrm{im}(\alpha_1))
\end{aligned}$$

so we find

$$\begin{aligned}
\sum_{i=0}^{1}(-1)^i \dim(H_i(V_\bullet)) &= \dim(H_0(V_\bullet)) - \dim(H_1(V_\bullet))\\
&= \dim(V_0) - \dim(\mathrm{im}(\alpha_1) - \dim(\ker(\alpha_1))\\
&= \dim(V_0) - \dim(V_1)\\
&= \chi(V_\bullet)
\end{aligned}$$

proving the desired result. □

Exercise VI.3.16. Prove Claim 3.14.

Claim 3.14. *With notation as above, we have the following:*

- χ_K *'is an Euler characteristic', in the sense that it satisfies the formula given in Proposition 3.13:*

$$\chi_K(V_\bullet) = \sum_i (-1)^i [H_i(V_\bullet)].$$

- χ_K *is a 'universal Euler characteristic', in the following sense. Let* G *be an abelian group, and let* δ *be a function associating an element of* G *to each finite-dimensional vector space, such that* $\delta(V) = \delta(V')$ *if* $V \cong V'$ *and* $\delta(V/U) = \delta(V) - \delta(U)$*. For* $V_\bullet$ *a complex, define*

$$\chi_G(V_\bullet) = \sum_i (-1)^i \delta(V_i).$$

Then δ *induces a (unique) group homomorphism*

$$K(k\text{-}\mathsf{Vect}^f) \to G$$

mapping $\chi_K(V_\bullet)$ *to* $\chi_G(V_\bullet)$*.*

- *In particular,* $\delta = \dim$ *induces a group homomorphism*

$$K(k\text{-}\mathsf{Vect}^f) \to \mathbb{Z}$$

such that $\chi_K(V_\bullet) \mapsto \chi(V_\bullet)$*.*

- *This is in fact an isomorphism.*

Solution. Recall that we define $F(k\text{-}\mathsf{Vect}^f)$ to be the set of isomorphism classes of finite-dimensional vector spaces $[V]$ over a field k. We let E be the subgroup generated by the elements $[V]-[U]-[W]$ for all short exact sequences

$$0 \longrightarrow U \longrightarrow V \longrightarrow W \longrightarrow 0$$

and define

$$K(k\text{-}\mathsf{Vect}^f) := \frac{F(k\text{-}\mathsf{Vect})}{E}$$

to be the Grothendieck group of the category $k\text{-}\mathsf{Vect}^f$. We also define

$$\chi_K(V_\bullet) := \sum_i (-1)^i [V_i] \in K$$

where summation is the direct sum.

First we prove that χ_k is an Euler characteristic. We adapt the proof by induction used to prove Propositoin 3.11, starting with the case $N=1$. Again, let

$$V_\bullet :\ 0 \longrightarrow V_1 \xrightarrow{\alpha_1} V_0 \longrightarrow 0$$

be a complex of finite-dimensional vector spaces and linear maps. By definition, we have $\chi_K(V_\bullet) = [V_0]-[V_1]$. Recall that, by the definition of homology,

$$H_0(V_\bullet) = \frac{V_0}{\mathrm{im}(\alpha_1)}, \quad H_1(V_\bullet) = \ker(\alpha_1)$$

so we have two exact sequences in $k\text{-}\mathsf{Vect}^f$:

$$0 \longrightarrow H_1(V_\bullet) \longrightarrow V_1 \longrightarrow \mathrm{im}(\alpha_1) \longrightarrow 0$$

and

$$0 \longrightarrow \mathrm{im}(\alpha_1) \longrightarrow V_0 \longrightarrow H_0(V_\bullet) \longrightarrow 0$$

so we have the relations $[H_1(V_\bullet)] = [V_1]-[\mathrm{im}(\alpha_1)]$ and $[H_0(V_\bullet)] = [V_0]-[\mathrm{im}(\alpha_1)]$. Thus, we find

$$\begin{aligned}
\sum_{i=0}^{1} [H_i(V_\bullet)] &= [H_0(V_\bullet)] - [H_1(V_\bullet)] \\
&= ([V_0] - [\mathrm{im}(\alpha_1)]) - [V_1] - [\mathrm{im}(\alpha_1)] \\
&= [V_0] - [V_1] \\
&= \chi_K(V_\bullet)
\end{aligned}$$

so the statement holds in the base case. Now we prove the inductive step. Given a complex

$$V_\bullet :\ 0 \longrightarrow V_N \xrightarrow{\alpha_N} V_{N-1} \xrightarrow{\alpha_{N-1}} \cdots \xrightarrow{\alpha_2} V_1 \xrightarrow{\alpha_1} V_0 \longrightarrow 0$$

we can consider the truncated complex

$$V'_\bullet :\ 0 \longrightarrow V_{N-1} \xrightarrow{\alpha_{N-1}} \cdots \xrightarrow{\alpha_2} V_1 \xrightarrow{\alpha_1} V_0 \longrightarrow 0$$

where the result is known to hold for $V'_\bullet$. Then

$$\chi_K(V_\bullet) = \chi_K(V'_\bullet) + (-1)^N[V_N]$$

and

$$H_i(V_\bullet) = H_i(V'_\bullet) \text{ for } 0 \leq i \leq N-2$$

while

$$H_{N-1}(V'_\bullet) = \ker(\alpha_{N-1}), \quad H_{N-1}(V_\bullet) = \frac{\ker(\alpha_{N-1}}{\mathrm{im}(\alpha_N)}, \quad H_N(V_\bullet) = \ker(\alpha_N).$$

Then we have exact sequences

$$0 \longrightarrow \ker(\alpha_N) \longrightarrow V_N \longrightarrow \mathrm{im}(\alpha_N) \longrightarrow 0$$

and

$$0 \longrightarrow \mathrm{im}(\alpha_N) \longrightarrow \ker(\alpha_{N-1}) \longrightarrow H_{N-1}(V_\bullet) \longrightarrow 0$$

which yield the relations $[V_N] = [\ker(\alpha_N)]+[\mathrm{im}(\alpha_N)]$ and $[H_{N-1}(V_\bullet)] = [\ker(\alpha_{N-1})]-[\mathrm{im}(\alpha_N)]$. Then we have

$$[H_{N-1}(V'_\bullet)] - [V_N] = [H_{N-1}(V_\bullet)] - [H_N(V_\bullet)]$$

so we find

$$\begin{aligned}
\chi_K(V_\bullet) &= \chi_K(V'_\bullet) + (-1)^N[V_N] \\
&= \sum_{i=0}^{N-1}(-1)^i[H_i(V'_\bullet)] + (-1)^N[V_N] \\
&= \sum_{i=0}^{N-2}(-1)^i[H_i(V'_\bullet)] + (-1)^{N-1}\left([H_{N-1}(V'_\bullet)] - [V_N]\right) \\
&= \sum_{i=0}^{N-2}(-1)^i[H_i(V_\bullet)] + (-1)^{N-1}([H_{N-1}(V_\bullet)] - [H_N(V_\bullet)]) \\
&= \sum_{i=0}^{N}(-1)^i[H_i(V_\bullet)]
\end{aligned}$$

which proves the desired result.

For the second part, let $\varphi : K(k\text{-}\mathsf{Vect}^f) \to G$ be the unique group homomorphism induced by δ. We claim that $\varphi([V]) = \delta(V)$ satisfies this universal property. First we check that it is well defined; suppose $[V] = [V']$. Then, since

$V \cong V'$, we have $\delta(V) = \delta(V')$. Now we show that this is a group homomorphism. Let $[U], [V] \in K(k\text{-}\mathsf{Vect}^f)$. Then

$$\varphi([V] - [U]) = \varphi([V/U]) = \delta(V/U) = \delta(V) - \delta(U) = \varphi([V]) - \varphi([U])$$

which verifies that this is a group homomorphism. Finally, let $V_\bullet$ be a complex of finite-dimensional vector spaces. Then

$$\begin{aligned}
\varphi(\chi_K(V_\bullet)) &= \varphi\left(\sum_i (-1)^i [V_i]\right) \\
&= \sum_i (-1)^i \varphi([V_i]) \\
&= \sum_i (-1)^i \delta(V_i) \\
&= \chi_G(V_\bullet)
\end{aligned}$$

where the second equality follows from φ being a group homomorphism.

The third point follows naturally from the second. Indeed, letting $\delta = \dim$ induces a group homomorphism from $K(k\text{-}\mathsf{Vect}^f)$ to $\mathbb{Z}$ such that $\chi_K(V_\bullet) = \chi(V_\bullet)$, where χ is the natural definition of the Euler characteristic.

To show that this is an isomorphism, we prove it is both injective and surjective. First note that for any non-negative integer n, we may consider the vector space $V = k^n$. Then $\varphi([V]) = n$. If n is negative, consider $V = k^{-n}$ such that $\varphi(-[V]) = -\varphi([V]) = n$. Thus, φ is surjective. Now suppose $\varphi([U]) = \varphi([V])$. That is, $\dim(U) = \dim(V)$. Then $U \cong V$ so $[U] = [V]$ and φ is injective. Thus, φ is an isomorphism and

$$K(k\text{-}\mathsf{Vect}^f) \cong \mathbb{Z}.$$

$\square$

Exercise VI.3.17. Extend the definition of Grothendieck group of vector spaces given in §3.4 to the category of vector spaces of *countable* (possibly infinite) dimension, and prove that it is the trivial group.

Solution. Consider the sequence

$$0 \longrightarrow k^{\oplus \mathbb{N}} \longrightarrow k^{\oplus \mathbb{N}} \longrightarrow k^n \longrightarrow 0$$

where $n \in \mathbb{N}$. Certainly, this sequence is exact because $k^{\oplus \mathbb{N}} \cong k^{\oplus \mathbb{N}} \oplus k^n$. But this implies that $[k^{\oplus \mathbb{N}}] = [k^{\oplus \mathbb{N}}] + [k^n]$ or $[k^n] = 0$. Since this also holds for $[k^{\oplus \mathbb{N}}]$, the group $K(k\text{-}\mathsf{Vect})$ is the trivial group. $\square$

Exercise VI.3.18. Let Ab^{fg} be the category of finitely generated abelian groups. Define a Grothendieck group of this category in the style of the construction of $K(k\text{-}\mathsf{Vect}^f)$, and prove that $K(\mathsf{Ab}^{fg}) \cong \mathbb{Z}$.

Solution. Note that every object G of Ab^{fg} determines an isomorphism class $[G]$. Let $F(\mathsf{Ab}^{fg})$ be the free abelian group on the set of these isomorphism classes. Furthermore, let E be the subgroup generated by the elements $[B]-[A]-[C]$ for all short exact sequences

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

in Ab^{fg}. Let

$$K(\mathsf{Ab}^{fg}) := \frac{F(\mathsf{Ab}^{fg})}{E}$$

be the Grothendieck group of this category.

Recall that every finitely generated abelian group is isomorphic to a direct sum of cyclic groups (Exercise 2.19). That is, for all finitely generated abelian groups G, we have

$$G \cong \mathbb{Z}^m \oplus \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_r\mathbb{Z}}$$

where $d_i \mid d_{i+1}$. Next, note that we may construct the exact sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\times n} \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

so that $[\mathbb{Z}/n\mathbb{Z}] = [\mathbb{Z}] - [\mathbb{Z}] = [0]$ for all $n \in \mathbb{Z}$. Thus, we may construct a homomorphism $\varphi : K(\mathsf{Ab}^{fg}) \to \mathbb{Z}$ which sends $[A]$ to m where $\mathbb{Z}^m$ is in the decomposition of A. Let $\text{rank}(A)$ denote the power of $\mathbb{Z}$ in the decomposition of A. First we verify that this homomorphism is well-defined: if $[A] = [B]$ then $A \cong B$ so
$textrank(A) = \text{rank}(B)$ and $\varphi([A]) = \varphi([B])$. Now we show it is a homomorphism. Let $[A], [B] \in K(\mathsf{Ab}^{fg})$ where $\text{rank}(A) = m$ and $\text{rank}(B) = n$. Then

$$\varphi([A] + [B]) = \varphi(A \oplus B) = m + n = \varphi([A]) + \varphi([B])$$

so φ is in fact a homomorphism. Finally, we verify that it is in fact an isomorphism. Certainly it is surjective since $\varphi([\mathbb{Z}^n]) = n$ for all $n \in \mathbb{Z}^{\geq 0}$ and one can use the additive inverse for negative integers. Lastly, the kernel of the homomorphism is the set of equivalence classes with rank 0. But if A has rank 0 then A is isomorphic to a direct sum of finite cyclic groups which are all isomorphic to $[0]$. That is, $\ker(\varphi) = [0]$ and the mapping is injective. Thus, it is a bijective homomorphism, proving that $K(\mathsf{Ab}^{fg}) \cong \mathbb{Z}$. $\square$

Exercise VI.3.19. Let Ab^f be the category of finite abelian groups. Prove that assigning to every finite abelian group its order extends to a homomorphism from the Grothendieck group $K(\mathsf{Ab}^f)$ to the multiplicative group $(\mathbb{Q}^*, \cdot)$.

Solution. First note that the sequence

$$0 \longrightarrow A \xrightarrow{i} A \oplus B \xrightarrow{\pi} B \longrightarrow 0$$

is exact. Let $\varphi : K(\mathsf{Ab}^f) \to \mathbb{Q}$ send a finite abelian group A to its order. To see that this is a homomorphism, let $[A], [B] \in K(\mathsf{Ab}^f)$ with $|A| = m, |B| = n$. Then

$$\varphi([A] + [B]) = \varphi([A \oplus B]) = mn = \varphi([A]) \cdot \varphi([B])$$

so it is in fact a homomorphism. Indeed, $\varphi([0]) = 1$ where 0 is the trivial group, and we can define φ for additive inverses accordingly. $\square$

Exercise VI.3.20. Let $R\text{-}\mathsf{Mod}^f$ be the category of modules of finite *length* (cf. Exercise 1.16) over a ring R. Let G be an abelian group, and let δ be a function assigning an element of G to every *simple* R-module. Prove that δ extends to a homomorphism from the Grothendieck group of $R\text{-}\mathsf{Mod}^f$ to G.

Explain why Exercise 3.19 is a particular case of this observation.

(For another example, letting $\delta(M) = 1 \in \mathbb{Z}$ for every simple module M shows that length itself extends to a homomorphism from the Grothendieck group of $R\text{-}\mathsf{Mod}^f$ to $\mathbb{Z}$.)

Solution. Recall that a module M has length m if it admits a composition series

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$

where each quotient M_i/M_{i+1} is simple. Let $\varphi : K(R\text{-}\mathsf{Mod}^f) \to G$ be defined as

$$\varphi([M]) = \sum i = 0^{m-1} \delta\left(\frac{M_i}{M_{i+1}}\right)$$

where the sum denotes the operation in G. Certainly this mapping is well-defined as isomorphic modules admit the same composition series (up to a re-ordering of the composition factors). To prove that it is a homomorphism, let $[M], [N] \in K(R\text{-}\mathsf{Mod}^f)$ where M has length m and N has length n. Then

$$\varphi([M] + [N]) = \varphi([M \oplus N]) = m + n = \varphi([M]) + \varphi([N])$$

by properties of the length of a module.

In particular, let $R = \mathbb{Z}$ and $G = (\mathbb{Q}^*, \cdot)$. Since simple finite abelian groups are cyclic groups of prime order $\mathbb{Z}/p\mathbb{Z}$, let $\delta(\mathbb{Z}/p\mathbb{Z}) = p$. Then φ is the extension of δ from $K(\mathbb{Z}\text{-}\mathsf{Mod}^f) \to \mathbb{Q}$. Indeed, given a finite abelian group

$$G = \frac{\mathbb{Z}}{p_1^{n_1}\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{p_r^{n_r}\mathbb{Z}}$$

we find

$$\begin{aligned}
\varphi([G]) &= \prod_i \delta\left(\frac{\mathbb{Z}}{p_i\mathbb{Z}}\right)^{n_i} \\
&= \prod_i p_i^{n_i} \\
&= |G|
\end{aligned}$$

which aligns with the definition given in Exercise 3.19. $\square$

VI.4 Presentations and resolutions

Exercise VI.4.1. Prove that if R is an integral domain and M is an R-module, then $\mathrm{Tor}(M)$ is a submodule of M. Give an example showing that the hypothesis that R is an integral domain is necessary.

Solution. Clearly $\mathrm{Tor}(M) \neq \emptyset$ since $0 \in \mathrm{Tor}(M)$. Now suppose $a, b \in \mathrm{Tor}(M)$. Then $\exists r, s \in R$ such that $ra = sb = 0$. Therefore, $rs(a+b) = s(ra) + r(sb) = 0$ so $a + b \in \mathrm{Tor}(M)$. Similarly, for all $s \in R$, we have $r(sa) = s(ra) = 0$ so $sa \in \mathrm{Tor}(M)$. Thus, $\mathrm{Tor}(M)$ is a submodule of M.

To see that R is an integral domain is necessary, consider $R = M = \mathbb{Z}/6\mathbb{Z}$. Then $\mathrm{Tor}(M) = \{0, 2, 3, 4\}$. But then $2 + 3 = 5 \notin \mathrm{Tor}(M)$ so $\mathrm{Tor}(M)$ is not a submodule of M. □

Exercise VI.4.2. Let M be a module over an integral domain R, and let N be a torsion-free module. Prove that $\mathrm{Hom}_R(M, N)$ is torsion-free. In particular, $\mathrm{Hom}_R(M, R)$ is torsion-free. (We will run into this fact again; see Proposition VIII.5.16.)

Solution. Let $f \in \mathrm{Hom}_R(M, N)$ and suppose $r \cdot f = 0$ for some $r \in R$. That is, for all $m \in M$,

$$r \cdot f(m) = 0.$$

But since $f(m) \in N$, $f(m)$ is not a torsion element and $r = 0$. Thus, $\mathrm{Hom}_R(M, N)$ is torsion-free. □

Exercise VI.4.3. Prove that an integral domain R is a PID if and only if every submodule of R itself is free.

Solution. Note that the submodules of R are its ideals. If R is a PID, then every submodule of R is generated by a single element. That is, every submodule of R has a basis, making it free. Now suppose every submodule of R is free. Recall that if M is a submodule of R, then $\dim(M) \leq \dim(R)$. In particular, $\dim(M) \leq 1$. Thus, every ideal of R is generated by at most one element so R is a PID. □

Exercise VI.4.4. Let R be a commutative ring and M an R-module.

- Prove that $\mathrm{Ann}(M)$ is an ideal of R.
- If R is an integral domain and M is finitely generated, prove that M is torsion if and only if $\mathrm{Ann}(M) \neq 0$.
- Give an example of a torsion module M over an integral domain, such that $\mathrm{Ann}(M) = 0$. (Of course this example cannot be finitely generated!)

Solution. Let $a, b \in \operatorname{Ann}(M)$. That is, for all $m \in M$, we have $am = bm = 0$. Then $(a+b)m = am + bm = 0$ so $a + b \in \operatorname{Ann}(M)$. Similarly, for all $r \in R$, we find $(ra) \cdot m = r \cdot (am) = r \cdot 0 = 0$ so $ra \in \operatorname{Ann}(M)$, proving that it is an ideal.

If $\operatorname{Ann}(M) \neq 0$, there exists an $r \in R$ such that $rm = 0$ for all $m \in M$. Thus, every element of M is torsion. Now suppose M is torsion. That is, for every element $m_i \in M$, there exists an $r_i \in R, r_i \neq 0$ such that $r_i m_i = 0$. In particular, there is such an r_i for each generator of M. Then we may consider s to be the product of these r_i. Since R is an integral domain, $s \neq 0$. Furthermore, since all $m \in M$ is a linear combination of these generators, we have $sm = 0$ for all $m \in M$. Thus, $s \in \operatorname{Ann}(M)$.

Let $R = \mathbb{Z}$ and consider the $\mathbb{Z}$-module

$$M = \bigoplus_{i=1}^{\infty} \frac{\mathbb{Z}}{2^i \mathbb{Z}}.$$

Then each element of M has the form

$$a = (a_1 + \mathbb{Z}/2\mathbb{Z}, a_2 + \mathbb{Z}/2^2\mathbb{Z}, \ldots, a_k + \mathbb{Z}/2^k\mathbb{Z}, 0, 0, \ldots)$$

so $2^k a = 0$ which makes M a torsion module. Now suppose $r \in \operatorname{Ann}(M)$. Choose $k \in \mathbb{Z}$ such that $r < 2^k$ and consider the element

$$a = (0, 0, \ldots, 1 + \mathbb{Z}/2^k\mathbb{Z}, 0, 0, \ldots).$$

Then $ra = 0$, but since $r < 2^k$, it must be the case that $r = 0$. Thus, $\operatorname{Ann}(M) = 0$. $\square$

Exercise VI.4.5. Let M be a module over a commutative ring R. Prove that an ideal I of R is the annihilator of an element of M if and only if M contains an isomorphic copy of R/I (viewed as an R-module).

The *associated primes* of M are the prime ideals among the ideals $\operatorname{Ann}(m)$, for $m \in M$. The set of the associated primes of a module M is denoted $\operatorname{Ass}_R(M)$. Note that every prime in $\operatorname{Ass}_R(M)$ contains $\operatorname{Ann}_R(M)$.

Solution. Let I be the annihilator of an element $m \in M$. That is, for all $r \in I$, $rm = 0$. Consider the map $\varphi : R \to M$ which sends r to rm. The kernel of this map is the set of r such that $rm = 0$. That is, $\ker(\varphi) = I$ so, by the isomorphism theorem,

$$\frac{R}{I} \cong \operatorname{im}(\varphi) \subseteq M.$$

Now suppose M contains a submodule $N \cong R/I$ for an ideal $I \subseteq R$ and let $\varphi : R \to M$ be the composition of the natural projection and inclusion. We claim that I is the annihilator of $m = \varphi(1)$. Indeed, if $r \in I$ then

$$rm = r\varphi(1) = \varphi(r) = i(\pi(r)) = i(0) = 0$$

so $r \in \text{Ann}(m)$ and $I \subseteq \text{Ann}(m)$. Similarly, if $r \in \text{Ann}(m)$ then

$$rm = 0 \Longrightarrow \varphi(r) = 0 \Longrightarrow \pi(r) = 0$$

so $r \in I$ and $\text{Ann}(m) = I$. $\square$

Exercise VI.4.6. Let M be a module over a commutative ring R, and consider the family of ideals $\text{Ann}(m)$, as m ranges over the nonzero elements of M. Prove that the maximal elements in this family are prime ideals of R. Conclude that if R is Noetherian, then $\text{Ass}_R(M) \neq \emptyset$ (cf. Exercise 4.5).

Solution. Let $\mathfrak{m}$ be a maximal element in this family of ideals, say $\mathfrak{m} = \text{Ann}(m)$. Suppose $rs \in \mathfrak{m}$. If $r \in \mathfrak{m}$ then there is nothing to prove so suppose otherwise. We know $rs \cdot m = 0$ but $rm \neq 0$. Thus, $s \in \text{Ann}(rm)$. Furthermore, it is clear that $\text{Ann}(m) \subseteq \text{Ann}(rm)$ since if $am = 0$ then $a(rm) = 0$. Then, by the maximality of $\text{Ann}(m)$, we have $\text{Ann}(m) = \text{Ann}(rm)$ so $s \in \mathfrak{m}$ and the ideal is prime.

If R is Noetherian, then every family of ideals has a maximal element. In particular, given a module M, the family of ideals $\text{Ann}(m)$ as m ranges over the nonzero elements of M has a maximal element which is a prime ideal. Such prime ideals are elements of $\text{Ass}_R(M)$, meaning the set is nonempty. $\square$

Exercise VI.4.7. Let R be a commutative Noetherian ring, and let M be a finitely generated module over R. Prove that M admits a finite series

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$

in which all quotients M_i/M_{i+1} are of the form $R/\mathfrak{p}$ for some prime ideal $\mathfrak{p}$ of R. (Hint: Use Exercises 4.5 and 4.6 to show that M contains an isomorphic copy M' of $R/\mathfrak{p}_1$ for some prime $\mathfrak{p}_1$. Then do the same with M/M', producing an $M'' \supsetneq M'$ such that $M''/M' \cong R/\mathfrak{p}_2$ for some prime $\mathfrak{p}_2$. Why must this process stop after finitely many steps?)

Solution. By Exercise 4.6, $\text{Ass}_R(M) \neq \emptyset$ so let $\mathfrak{p}_1 \in \text{Ass}_R(M)$. Then by Exercise 4.5, M contains a submodule $M' \cong R/\mathfrak{p}_1$. Now consider M/M', which is also an R-module. Thus, $\text{Ass}_R(M/M') \neq \emptyset$ and there is a submodule $M'' \supsetneq M'$ of M such that $M''/M' \cong R/\mathfrak{p}_2$ for some prime $\mathfrak{p}_2$. That is, we have a chain

$$M \supsetneq M'' \supsetneq M' \supsetneq \langle 0 \rangle$$

such that $M''/M' \cong R/\mathfrak{p}_2$ and $M'/0 \cong R/\mathfrak{p}_1$ for prime ideals of R. Since M is finitely generated over a Noetherian ring, it is a Noetherian module and all chains of submodules eventually stabilize. Thus, iterating this process yields a finite series whose quotients are isomorphic to $R/\mathfrak{p}$ for prime ideals. $\square$

Exercise VI.4.8. Let R be a commutative Noetherian ring, and let M be a finitely generated module over R. Prove that every prime in $\mathrm{Ass}_R(M)$ appears in the list of primes produced by the procedure presented in Exercise 4.7. (If $\mathfrak{p}$ is an associated prime, then M contains an isomorphic copy N of $R/\mathfrak{p}$. With notation as in the hint in Exercise 4.7, prove that either $\mathfrak{p}_1 = \mathfrak{p}$ or $N \cap M' = 0$. In the latter case, N maps isomorphically to a copy of $R/\mathfrak{p}$ in M/M'; iterate the reasoning.)

In particular, if M is a finitely generated module over a Noetherian ring, then $\mathrm{Ass}(M)$ is *finite*.

Solution. Let $\mathfrak{p} \in \mathrm{Ass}_R(M)$ and suppose $R/\mathfrak{p} \cong N \subseteq M$. In particular, if $x \in M$ such that $\mathrm{Ann}_R(x) = \mathfrak{p}$, then $N = Rx$. If $Rx \cap M' \neq 0$, say $rx = m$ is a nonzero element, then $\mathrm{Ann}_R(m) \subseteq \mathfrak{p}$. But by definition, $\mathrm{Ann}_R(m) = \mathfrak{p}_1$ so $\mathfrak{p}_1 \subseteq \mathfrak{p}$. The reverse inclusion can be shown similarly. Thus, if M' and N have nontrivial intersection, $\mathfrak{p} = \mathfrak{p}_1$. Otherwise, $M' \cap N = 0$. In the latter case, N is isomorphic to some $R/\mathfrak{p}$ in $M/M' \cong R/\mathfrak{p}_2$. Thus, we may repeat the above reasoning which eventually terminates. $\square$

Exercise VI.4.9. Let M be a module over a commutative Noetherian ring R. Prove that the union of all annihilators of nonzero elements equals the union of all associated primes of M. (Use Exercise 4.6)

Deduce that the *union* of the associated primes of a Noetherian ring R (viewed as a module over itself) equals the set of zero-divisors of R.

Solution. Certainly every associated prime is the annihilator of some element $m \in M$, so we only need to show the other direction. If $I \in \mathrm{Ann}_R(m)$ for some $m \in M$, then $I \subseteq \mathfrak{p}$ for some maximal element in the family of annihilators of elements of M. By Exercise 4.6, $\mathfrak{p}$ is prime in R so I is in the union of all associated primes, proving the result. $\square$

Exercise VI.4.10. Let R be a commutative Noetherian ring. One can prove that the minimal primes of $\mathrm{Ann}(M)$ (cf. Exercise V.1.9) are in $\mathrm{Ass}(M)$. Assuming this, prove that the *intersection* of the associated primes of a Noetherian ring R (viewed as a module over itself) equals the nilradical of R.

Solution. Recall that the nilradical of R is the set of elements $r \in R$ such that $r^n = 0$ for some $n > 0$. If $x \in \mathrm{nil}(R)$ then x is in the intersection of all prime ideals of R, particularly the intersection of associated primes of R. Now suppose x is in the intersection of the associated primes of R. Then it is in the minimal primes of $\mathrm{Ann}(R)$. Since every prime ideal contains a minimal prime ideal, the intersection of all prime ideals equals the intersection of all minimal prime ideals. Thus, $x \in \mathrm{nil}(R)$. $\square$

Exercise VI.4.11. Review the notion of presentation *of a group*, and relate it to the notion of presentation introduced in §4.2.

Solution. Recall that a presentation of a group G is an explicit isomorphism

$$G \cong \frac{F(A)}{R}$$

for a set A and a subgroup R of relations. A presentation of an R-module M is an exact sequence

$$R^n \longrightarrow R^m \longrightarrow M \longrightarrow 0$$

In particular, if G is an abelian group, then we have the exact sequence

$$R \longrightarrow F(A) \longrightarrow G$$

where R is also a free module since it is a submodule of $F(A)$. □

Exercise VI.4.12. Let $\mathfrak{p}$ be a prime ideal of a polynomial ring $k[x_1, \ldots, x_n]$ over a field k, and let $R = k[x_1, \ldots, x_n]/\mathfrak{p}$. Prove that every finitely generated module over R has a finite presentation.

Solution. Let M be a finitely generated module over R. Then there is a surjection $\pi : R^a \to M$ for some $a \in \mathbb{Z}$ where $\ker(\pi)$ is a submodule of R^a. Since k is a field, by Hilbert's basis theorem, $k[x_1, \ldots, x_n]$ is also Noetherian. But then R is a quotient of a Noetherian ring and is Noetherian itself. Thus, $\ker(\pi)$ is finitely generated and there is an exact sequence

$$R^b \longrightarrow \ker(\pi) \longrightarrow 0$$

which yields the exact sequence

$$R^b \longrightarrow R^a \longrightarrow M \longrightarrow 0$$

so M is finitely presented. □

Exercise VI.4.13. Let R be a commutative ring. A tuple $(a_1, a_2, \ldots, a_n)$ of elements of R is a *regular sequence* if a_1 is a non-zero-divisor in R, a_2 is a non-zero-divisor modulo (a_1), a_3 is a non-zero-divisor modulo (a_1, a_2), and so on.

For a, b in R, consider the following complex of R-modules:

$$(*) \qquad 0 \longrightarrow R \xrightarrow{d_2} R \oplus R \xrightarrow{d_1} R \xrightarrow{\pi} \frac{R}{(a,b)} \longrightarrow 0$$

where π is the canonical projection, $d_1(r, s) = ra + sb$, and $d_2(t) = (bt, -at)$. Put otherwise, d_1 and d_2 correspond, respectively, to the matrices

$$\begin{pmatrix} a & b \end{pmatrix}, \quad \begin{pmatrix} b \\ -a \end{pmatrix}.$$

- Prove that this is indeed a complex, for every a and b.
- Prove that if (a, b) is a regular sequence, this complex is *exact*.

The complex (*) is called the *Koszul complex* of (a, b). Thus, when (a, b) is a regular sequence, the Koszul complex provides us with a free resolution of the module $R/(a, b)$.

Solution. First we verify that this is a complex for all a and b. Certainly the image of the zero map is a subset of $\ker(d_2)$. Let $(r, s) \in \operatorname{im}(d_2)$. Then $(r, s) = (bt, -at)$ for some $t \in R$ and

$$d_1(bt, -at) = bta - bta = 0$$

so $\operatorname{im}(d_2) \subseteq \ker(d_1)$. Furthermore, let $ra + sb \in \operatorname{im}(d_1)$. Then $\pi(ra + sb) = 0 \in R/(a, b)$ so $\operatorname{im}(d_1) \subseteq \ker(\pi)$. Finally, the image of π is clearly a subset of the kernel of the zero map. Thus, we have verified that this is in fact a complex.

Now suppose (a, b) is a regular sequence. Let $t \in \ker(d_2)$. That is, $(bt, -at) = (0, 0)$. Since $a \neq 0$, it must be the case that $t = 0$ so t is in the image of the zero map, proving the two are equal.

Now suppose $(r, s) \in \ker(d_1)$. Then $ra + sb = 0$. Consider the equation mod a: $sb = 0$. Since b is not a zero-divisor in $R/(a)$, $s \in (a)$ so $s = at$ for some $t \in R$. Then we have $ra + atb = 0$, or $(r + tb)a = 0$. Since a is not a zero-divisor in R, it must be the case that $r + tb = 0$, or $r = -tb$. That is, $(r, s) = (-tb, at) \in \operatorname{im}(d_2)$ so the two sets must be equal.

Now let $x \in \ker(\pi)$ so $\pi(x) = 0 \Longrightarrow x = ra + sb$ for $r, s \in R$. Then $x = d_1(r, s) \in \operatorname{im}(d_1)$ and the two sets are equal.

Finally, the projection is surjective and the kernel of the zero map is all of its domain so the last map is exact. $\square$

Exercise VI.4.14. A Koszul complex may be defined for any sequence $a_1, \ldots, a_n$ of elements of a commutative ring R. The case $n = 2$ seen in Exercise 4.13 and the case $n = 3$ reviewed here will hopefully suffice to get a gist of the general construction; the general case will be given in Exercise VIII.4.22.

Let $a, b, c \in R$. Consider the following complex:

$$0 \longrightarrow R \xrightarrow{d_3} R \oplus R \oplus R \xrightarrow{d_2} R \oplus R \oplus R \xrightarrow{d_1} R \xrightarrow{\pi} \frac{R}{(a,b,c)} \longrightarrow 0$$

where π is the canonical projection and the matrices for d_1, d_2, d_3 are, respectively,

$$\begin{pmatrix} a & b & c \end{pmatrix}, \quad \begin{pmatrix} 0 & -c & -b \\ -c & 0 & a \\ b & a & 0 \end{pmatrix}, \quad \begin{pmatrix} a \\ -b \\ c \end{pmatrix}.$$

- Prove that this is indeed a complex, for every a, b, c.

- Prove that if (a, b, c) is a regular sequence, this complex is *exact*.

Koszul complexes are very important in commutative algebra and algebraic geometry.

Solution. Clearly the image of the zero map is in the kernel of d_3. Let $(ar, -br, cr) \in \mathrm{im}(d_3)$. Then

$$\begin{pmatrix} 0 & -c & -b \\ -c & 0 & a \\ b & a & 0 \end{pmatrix} \cdot \begin{pmatrix} ar \\ -br \\ cr \end{pmatrix} = \begin{pmatrix} bcr - bcr \\ -acr + acr \\ abr - abr \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

so $(ar, -br, cr) \in \ker(d_2)$. Now let $(-cs - bt, -cr + at, br + as) = d_2(r, s, t) \in \mathrm{im}(d_2)$. Then

$$\begin{pmatrix} a & b & c \end{pmatrix} \cdot \begin{pmatrix} -cs - bt \\ -cr + at \\ br + as \end{pmatrix} = -acs - abt - bcr + abt + bcr + acs = 0$$

so $\mathrm{im}(d_2) \subseteq \ker(d_1)$. Now consider $ra + sb + ct = d_1(r, s, t) \in \mathrm{im}(d_1)$. We have

$$\pi(ra + sb + ct) = 0$$

by definition of the projection to a quotient so $\mathrm{im}(d_1) \subseteq \ker(\pi)$. The image of projection is obviously a subset of the kernel of the zero map. Thus, this is indeed a complex.

Now suppose (a, b, c) is a regular sequence. If $r \in \ker(d_3)$ then $d_3(r) = (0, 0, 0)$. In particular, $ar = 0$ and since a is not a zero-divisor, we must have $r = 0$ so r is in the image of the zero map, hence it equals the image of d_3.

If $(r_1, r_2, r_3) \in \ker(d_2)$, then

$$\begin{pmatrix} 0 & -c & -b \\ -c & 0 & a \\ b & a & 0 \end{pmatrix} \cdot \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} -cr_2 - br_3 \\ -cr_1 + ar_3 \\ br_1 + ar_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

The third equation mod a yields $br_1 = 0$ in $R/(a)$. Since b is not a zero-divisor in this ring, we must have $r_1 = at$ for some $t \in R$. Substituting this back into the third equation, we have $abt + ar_2 = 0$, or $r_2 = -bt$ (since a is not a zero-divisor in R). Substituting this into the second equation yields $-act + ar_3 = 0$ so $r_3 = ct$ by the same reasoning as above. But then

$$(r_1, r_2, r_3) = (at, -bt, ct) = d_3(t)$$

so $\mathrm{im}(d_3) = \ker(d_2)$.

If $(r_1, r_2, r_3) \in \ker(d_1)$, then

$$\begin{pmatrix} a & b & c \end{pmatrix} \cdot \begin{pmatrix} r_1 \\ r_2 \\ r_3 \end{pmatrix} = ar_1 + br_2 + cr_3 = 0.$$

Considering this equation mod (a, b) yields $cr_3 = 0$ in $R/(a, b)$ and since c is not a zero-divisor in this ring, we must have $r_3 \in (a, b)$ or $r_3 = ar + bs$ for $r, s \in R$. Substituting this into the equation yields

$$ar_1 + br_2 + acr + bcs = 0$$

which we can consider mod a to yield $br_2 + bcs = 0$ in $R/(a)$, or $r_2 + cs = at$ for some $t \in R$. That is, $r_2 = at - cs$, which we can again substitute into the equation to obtain

$$ar_1 + abt - bcs + acr + bcs = 0$$

which yields $a(r_1 + bt + cs) = 0$ so $r_1 = -bt - cs$. But then

$$(r_1, r_2, r_3) = (-bt - cs, at - cs, ar + bs) = d_2(r, s, t)$$

so $\operatorname{im}(d_2) = \ker(d_1)$.

Finally, suppose $x \in \ker(\pi)$. That is, $x \in (a, b, c)$. Then $x = ra + bs + ct = d_1(r, s, t)$ and $\operatorname{im}(d_1) = \ker(\pi)$. The last equality is obvious. Thus, the complex is exact. $\square$

Exercise VI.4.15. View $\mathbb{Z}$ as a module over the ring $R = \mathbb{Z}[x, y]$, where x and y act by 0. Find a free resolution of $\mathbb{Z}$ over R.

Solution. Recall that a free resolution of an R-module M is an exact complex

$$\cdots \longrightarrow R^{m_3} \longrightarrow R^{m_2} \longrightarrow R^{m_1} \longrightarrow R^{m_0} \longrightarrow M \longrightarrow 0.$$

Consider the complex

$$0 \longrightarrow R \xrightarrow{d_2} R^2 \xrightarrow{d_1} R \xrightarrow{\pi} \mathbb{Z} \longrightarrow 0$$

where d_1 and d_2 correspond to the matrices

$$\begin{pmatrix} x & y \end{pmatrix}, \quad \begin{pmatrix} y \\ -x \end{pmatrix}$$

and π is the natural projection to the constant term. It is easy to see that this is in fact a complex. To see that it is exact, let $f(x, y) \in \ker(\pi)$. That is, f has no constant term, so it may be written as

$$f = \begin{pmatrix} x & y \end{pmatrix} \cdot \begin{pmatrix} f_1(y) \\ f_2(x) \end{pmatrix}$$

so $f \in \operatorname{im}(d_1)$. Similarly, if $(f, g) \in \ker(d_1)$ then $fx + gy = 0$. Gathering terms, this is only possible if $f = hy$ and $g = -hx$ for some $h \in R$. That is, $(f, g) = d_2(h)$ so $\ker(d_1) = \operatorname{im}(d_2)$ and the sequence is exact. Thus, this is a free resolution of $\mathbb{Z}$ over R. $\square$

Exercise VI.4.16. Let $\varphi : R^n \to R^m$ and $\psi : R^p \to R^q$ be two R-module homomorphisms, and let

$$\varphi \oplus \psi : R^n \oplus R^p \to R^m \oplus R^q$$

be the morphism induced on direct sums. Prove that

$$\operatorname{coker}(\varphi \oplus \psi) = \operatorname{coker}\varphi \oplus \operatorname{coker}\psi.$$

Solution. First note that

$$\operatorname{im}(\varphi \oplus \psi) = \operatorname{im}(\varphi) \oplus \operatorname{im}(\psi).$$

Now consider the map

$$R^m \oplus R^q \to \frac{R^m}{\operatorname{im}\varphi} \oplus \frac{R^q}{\operatorname{im}\psi}.$$

The kernel of this map is $\operatorname{im}(\varphi) \oplus \operatorname{im}(\psi)$ so by the first isomorphism theorem, we have

$$\frac{R^m \oplus R^q}{\operatorname{im}(\varphi \oplus \psi)} \cong \frac{R^m}{\operatorname{im}\varphi} \oplus \frac{R^q}{\operatorname{im}\psi}$$

and $\operatorname{coker}(\varphi \oplus \psi) = \operatorname{coker}(\varphi) \oplus \operatorname{coker}(\psi)$. □

Exercise VI.4.17. Determine (as a better known entity) the module represented by the matrix

$$\begin{pmatrix} 1+3x & 2x & 3x \\ 1+2x & 1+2x-x^2 & 2x \\ x & x^2 & x \end{pmatrix}$$

over the polynomial ring $k[x]$ over a field.

Solution. We perform Gaussian elimination to reduce the matrix to a simpler but equivalent form. Subtracting three times the third row from the first yields a unit in the $1,1$ position so we are reduced to the 2×2 matrix

$$\begin{pmatrix} 1+2x-x^2 & 2x \\ x^2 & x \end{pmatrix}.$$

Adding the second row to the first and subtracting $\frac{2}{3}$ times the second column from the first yields another unit in the $1,1$ position so we have reduced the matrix to

$$\begin{pmatrix} x \end{pmatrix}.$$

The module represented by the original matrix is isomorphic to the cokernel of the homomorphism

$$\varphi : k[x] \to k[x]$$

which maps 1 to x. That is,

$$M \cong \operatorname{coker}\varphi \cong \frac{k[x]}{(x)} \cong k.$$

□

VI.5 Classification of finitely generated modules over PID

Exercise VI.5.1. Let N, P be submodules of a module M, such that $N \cap P = \{0\}$ and $M = N + P$. Prove that $M \cong N \oplus P$. (This is a word-for-word repetition of Proposition IV.5.3 for modules.)

Solution. Consider the mapping

$$\varphi : N \oplus P \to N + P$$

defined by $\varphi(n, p) = n + p$. Certainly this is an R-module homomorphism. It is surjective since for all $m = n + p \in N + P$, we have $m = \varphi(n, p)$. Furthermore, the kernel of this mapping is

$$\ker \varphi = \{(n, p) \in N \oplus P \mid n + p = 0\}.$$

If $n + p = 0$ then $n = -p \in P$ so $n \in N \cap P$ and $n = 0$. Similarly, $p = 0$ so $\ker \varphi = \{0\}$ and the map is injective. Thus, this is an isomorphism and $M = N + P \cong N \oplus P$. $\square$

Exercise VI.5.2. Let R be an integral domain, and let M be a finitely generated R-module. Prove that M is torsion if and only if $\operatorname{rk} M = 0$.

Solution. The rank of M is 0 if and only if for all $m \in M$, the set $\{m\}$ is linearly dependent. This occurs if and only if there exists $r \in R$ such that $rm = 0$, but this is true if and only if M is torsion. $\square$

Exercise VI.5.3. Complete the proof of Corollary 5.3.

Corollary 5.3. *Let R be a PID, let F be a finitely generated free module over R, and let $M \subseteq F$ be a submodule. Then there exists a basis $(x_1, \ldots, x_n)$ of F and nonzero elements $a_1, \ldots, a_m$ of R ($m \le n$) such that $(a_1x_1, \ldots, a_mx_m)$ is a basis of M. Further, we may assume $a_1 \mid a_2 \mid \cdots \mid a_m$.*

Solution. We only need to show the existence of the bases. By Lemma 5.2, there exists $x \in F$ such that

$$F = \langle x_1 \rangle \oplus F^{(1)}.$$

If $F^{(1)} = 0$, then (x_1) is a basis for F. Otherwise we may repeat this process. Since F is a finitely generated free module, this process terminates and yields a basis $(x_1, \ldots, x_n)$ for F. Lemma 5.2 also guarantees the existence of $y_1 = a_1x_1$ such that

$$M = \langle y_1 \rangle \oplus M^{(1)}.$$

If $M^{(1)} = 0$, then $(y_1) = (a_1x_1)$ is a basis for M. Otherwise we may repeat this process. Since M is a submodule of F, $\operatorname{rk} M \le \operatorname{rk} F$ so this process also terminates at some $m \le n$. $\square$

Exercise VI.5.4. Let R be an integral domain, and assume that $a, b \in R$ are such that $a \neq 0$, $b \notin (a)$, and $R/(a), R/(a,b)$ are both integral domains.

- Prove that the Krull dimension of R is at least 2.
- Prove that if R satisfies the finiteness condition discussed in §5.2 for some n, then $n \geq 2$.

You can prove this second point by appealing to Proposition 5.4. For a more concrete argument, you should look for an R-module admitting a free resolution of length 2 which cannot be shortened.

- Prove that (a, b) is a regular sequence in R. (Exercise 4.13).
- Prove that the R-module $R/(a, b)$ has a free resolution of length exactly 2.

Can you see how to construct analogous situations with $n \geq 3$ elements $a_1, \dots, a_n$?

Solution. Since $R/(a)$ and $R/(a,b)$ are integral domains, (a) and (a,b) are both prime ideals. Thus, we may construct the chain of prime ideals

$$(0) \subsetneq (a) \subsetneq (a, b)$$

in R, so the Krull dimension of R is at least 2.

Now suppose every finitely generated R-module M admits a free resolution of finite length n. To show that $n \geq 2$, it suffices to construct a free resolution of length 2 which cannot be shortened. Consider the R-module $M = R/(a,b)$. Then we have an exact sequence

$$0 \longrightarrow R \xrightarrow{d_2} R^2 \xrightarrow{d_1} R \xrightarrow{\pi} M \longrightarrow 0$$

where $d_2(r) = (-br, ar)$, $d_1(r, s) = ra + sb$, and π is the natural projection. It is easy to check that this is an exact sequence, and it cannot be shortened to $n = 1$. To see this, note that $\ker \pi = (a, b)$. Any morphism whose image is (a, b) must have domain R^2 since there are two degrees of choice in the image. Since the kernel of a map from $R^2 \to R$ must be nontrivial, there must be another copy of R before R^2 in the free resolution and the free resolution cannot be shortened. It also follows from the fact that the Krull dimension of a PID is at most 1.

Recall that a regular sequence is a tuple $(a_1, a_2, \dots, a_n)$ where a_1 is not a zero-divisor of R, a_2 is not a zero-divisor of $R/(a_1)$, a_3 is not a zero-divisor of $R/(a_1, a_2)$ and so on. Since R is an integral domain, a is a non-zero-divisor of R. Furthermore, $b \notin (a)$ so $b \neq 0 \in R/(a)$. Then, since $R/(a)$ is an integral domain, b is not a zero divisor in $R/(a)$. Thus, (a, b) is a regular sequence in R.

The sequence constructed in part 2 of this exercise proves that $R/(a, b)$ has a free resolution of length 2. $\square$

Exercise VI.5.5. Recall (Exercise V.4.11) that a commutative ring is *local* if it has a single maximal ideal $\mathfrak{m}$. Let R be a local ring, and let M be a *direct summand* of a finitely generated free R-module: that is, there exists an R-module N such that $M \oplus N$ is a free R-module.

- Choose elements $m_1, \ldots, m_r \in M$ whose cosets mod $\mathfrak{m}M$ are a basis of $M/\mathfrak{m}M$ as a vector space over the field $R/\mathfrak{m}$. By Nakayama's lemma, $M = \langle m_1, \ldots, m_r \rangle$ (Exercise 3.10).
- Obtain a surjective homomorphism $\pi : F = R^{\oplus r} \to M$.
- Show that π splits, giving an isomorphism $F \cong M \oplus \ker \pi$. (Apply Exercise III.6.9 to the surjective homomorphism π and the free module $M \oplus N$ to obtain a splitting $M \to F$; then use Proposition III.7.5.)
- Show $\ker \pi / \mathfrak{m} \ker \pi = 0$. Use Nakayama's lemma (Exercise 3.8) to deduce that $\ker \pi = 0$.
- Conclude that $M \cong F$ is in fact free.

Summarizing, over a *local ring*, every *direct summand* of a finitely generated free R-module is free. Using the terminology we will introduce in Chapter VIII, we would say that 'projective modules over local rings are free'. This result has strong implications in algebraic geometry, since it underlies the notion of vector bundle.

Contrast this fact with Proposition 5.1, which shows that, over a *PID*, *every* submodule of a finitely generated free module is free.

Solution. The first point follows from Exercise 3.10.

Define $\pi : R^{\oplus r} \to M$ which sends e_i to m_i where e_i is an elementary basis vector. Certainly this is surjective as a projection.

There is a short exact sequence

$$0 \longrightarrow \ker \pi \longrightarrow F \xrightarrow{\pi} M \longrightarrow 0$$

and since π has a right-inverse (sending the basis of M to the basis of F), Proposition III.7.5 implies that this sequence is split and $F \cong M \oplus \ker \pi$.

Note that

$$\left(\frac{R}{\mathfrak{m}}\right)^r \cong \frac{M}{\mathfrak{m}M} \oplus \frac{\ker \pi}{\mathfrak{m} \ker \pi}$$

as vector spaces over $R/\mathfrak{m}$. Since the dimension of $M/\mathfrak{m}M$ is r, we must have $\ker \pi / \mathfrak{m} \ker \pi = 0$. Then, by Nakayama's lemma, $\ker \pi = 0$.

Thus, $F \cong M$ and M is a free module. $\square$

Exercise VI.5.6. Let R be an integral domain, and let $M = \langle m_1, \ldots, m_r \rangle$ be a finitely generated module. Prove that $\operatorname{rk} M \leq r$. (Use Exercise 3.12.)

Solution. Assume for the sake of contradiction that $k = \operatorname{rk} M > r$. There are surjections $f : R^r \to M$ and $g : R^k \to M$. Let $N \in \mathcal{M}_{r,k}(R)$ such that g maps the columns of N to a maximal linearly independent subset of M. By Exercise 3.12, the columns of N are linearly dependent. In particular, there exist $\{r_1, \ldots, r_k\}$ such that $r_1 n_1 + \cdots + r_k n_k = 0$ where the $n_i \in R^r$. Then

$$g(r_1 n_1 + \cdots + r_k n_k) = r_1 g(n_1) + \cdots + r_k g(n_k) = 0,$$

which contradicts the assumption that the image of the columns of N is linearly independent. Thus, $k = \operatorname{rk} M \leq r$. □

Exercise VI.5.7. Let R be an integral domain, and let M be a finitely generated module over R. Prove that $\operatorname{rk} M = \operatorname{rk}(M/\operatorname{Tor}(M))$.

Solution. First note that $\operatorname{rk}(M/\operatorname{Tor}(M)) \leq \operatorname{rk} M$ because any linearly independent subset of the former induces a linearly independent subset of the latter. Suppose $\operatorname{rk} M = r$ and let $S = \{m_1, \ldots, m_r\}$ be a maximal linearly independent subset of M. Consider $S + \operatorname{Tor}(M) = \{m_1 + \operatorname{Tor}(M), \ldots, m_r + \operatorname{Tor}(M)\}$. If this set is linearly dependent, then there exist $r_1, \ldots, r_r \in R$ such that $r_1 m_1 + \cdots + r_r m_r \in \operatorname{Tor}(M)$. That is, there exists an $s \in R, s \neq 0$ such that

$$s(r_1 m_1 + \cdots + r_r m_r) = 0.$$

Since R is an integral domain, this implies $r_1 m_1 + \cdots + r_r m_r = 0$ and S is linearly dependent in M, a contradiction. Thus, $S + \operatorname{Tor}(M)$ is also linearly independent and we have $\operatorname{rk} M = \operatorname{rk}(M/\operatorname{Tor}(M))$. □

Exercise VI.5.8. Let R be an integral domain, and let M be a finitely generated module over R. Prove that $\operatorname{rk} M = r$ if and only if M has a *free* submodule $N \cong R^r$, such that M/N is torsion.

If R is a PID, then N may be chosen so that $0 \to N \to M \to M/N \to 0$ splits.

Solution. Suppose $\operatorname{rk} M = r$ and let $S = \{m_1, \ldots, m_r\}$ be a linearly independent subset. Consider the free submodule $N = \langle S \rangle \cong R^r$. Indeed, an isomorphism is given by mapping corresponding basis elements $m_i \mapsto e_i$. Now let $x + N \in M/N$. If $x + N$ is not a torsion element then there is no $r \in R$ such that $rx \in N$. That is, x is linearly independent of S, but this contradicts that S is a maximal linearly independent set. Thus, $x + N$ is a torsion element and M/N is torsion.

Now suppose M has a free submodule $N \cong R^r$ such that M/N is torsion. Choose a linearly independent set $S = \{m_1, \ldots, m_r\}$ such that S is a basis for N. Let $x + N \in M/N$. Since this module is torsion, there exists an $r \in R$ such that $rx \in N$. That is, x is a linear combination of the elements of S. Since this holds for all elements of M, S is a maximal linearly independent subset of M and $\operatorname{rk} M = r$. □

Exercise VI.5.9. Let R be an integral domain, and let

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

be an exact sequence of finitely generated R-modules. Prove that $\operatorname{rk} M_2 = \operatorname{rk} M_1 + \operatorname{rk} M_3$.

Deduce that 'rank' defines a homomorphism from the Grothendieck group of the category of finitely generated R-modules to $\mathbb{Z}$.

Solution. Let $r_i = \operatorname{rk} M_i$. By the isomorphism theorems, $M_3 \cong M_2/M_1$. Let $\{u_1, \ldots, u_{r_1}\}$ be linearly independent in M_1 and $\{v_1 + M_1, \ldots, v_{r_3} + M_1\}$ be linearly independent in M_3. If

$$a_1u_1 + \cdots + a_{r_1}u_{r_1} + b_1v_1 + \cdots + b_{r_3}v_{r_3} = 0$$

in M_2, then reducing the equation modulo M_1 yields

$$b_1(v_1 + M_1) + \cdots + b_{r_3}(v_{r_3} + M_1) = 0 + M_1$$

so $b_1 = \cdots = b_{r_3} = 0$ by linear independence in M_3. But then $a_1 = \cdots = a_{r_1} = 0$ by linear independence in M_1 so $r_2 \geq r_1 + r_3$.

To show the other inequality, let N be a linearly independent subset of M_2. Let $X \subset N$ be maximal with respect to the property that $f(X)$ is linearly independent in M_3 (where f is the surjection from $M_2 \to M_3$). Now let $m \in N \setminus X$. The set $f(\{m\} \cup X)$ is linearly dependent in M_3 so there exist $r_m, s_{m,x} \in R$ such that

$$0 = r_m f(m) + \sum_{x \in X} s_{m,x} f(x) = f\left(r_m m + \sum_{x \in X} s_{m,x} x\right),$$

hence $r_m m + \sum_{x \in X} s_{m,x} x \in M_1$. Note that $r_m \neq 0$ since $f(X)$ is linearly independent. Now let $t_m \in R$ such that

$$\sum_{m \in N \setminus X} t_m(r_m m + \sum x \in X s_{m,x} x) = 0$$

and rearrange to yield

$$0 = \sum_{m \in N \setminus X} t_m r_m m + \sum_{x \in X} \sum_{m \in N \setminus X} t_m s_{m,x} x.$$

The linear independence of N shows that $t_m r_m = 0$, so $t_m = 0$ since $r_m \neq 0$ and R is an integral domain. Thus, the elements $(r_m m + \sum_{x \in X} s_{m,x} x)_{m \in N \setminus X}$ are linearly independent. This shows that N can be split into a disjoint union $N = (N \setminus X) \cup X$ such that the elements of $N \setminus X$ are linearly independent in M_1 and the elements of X are linearly independent in M_3. That is, $r_2 \leq r_1 + r_3$. Combining this with the above inequality yields $\operatorname{rk} M_2 = \operatorname{rk} M_1 + \operatorname{rk} M_3$. $\square$

Exercise VI.5.10. Let R be an integral domain, M an R-module, and assume $M \cong R^r \oplus T$, with T a torsion module. Prove directly (that is, without using Theorem 5.6) that $r = \operatorname{rk} M$ and $T \cong \operatorname{Tor}_R(M)$.

Solution. We have an exact sequence

$$0 \longrightarrow R^r \longrightarrow M \longrightarrow T \longrightarrow 0$$

and by the above exercise, $\operatorname{rk} M = \operatorname{rk} R^r + \operatorname{rk} T$. Since the rank of a torsion module is 0 (every element is linearly dependent), we have $\operatorname{rk} M = r$. We also have an isomorphism $T \cong M/R^r$. Note that $\operatorname{Tor}(M) = \{(s,t) \in M \mid \exists r \in R, (rs, rt) = (0,0)\}$. Since R^r is a free module, if $rs = 0$ with $s \in R^r$, we must have $r = 0$. Thus, $\operatorname{Tor}(M) = \{(0,t) \mid t \in T\}$, and clearly this is isomorphic to T. □

Exercise VI.5.11. Let R be an integral domain, let M, N be R-modules, and let $\varphi : M \to N$ be a homomorphism. For $m \in M$, show that $\operatorname{Ann}(\langle m \rangle) \subseteq \operatorname{Ann}(\langle \varphi(m) \rangle)$.

Solution. Let $a \in \operatorname{Ann}(\langle m \rangle)$ and consider $r\varphi(m) \in \langle \varphi(m) \rangle$. We have $a \cdot r\varphi(m) = r\varphi(am) = r\varphi(0) = 0$ so $a \in \operatorname{Ann}(\langle \varphi(m) \rangle)$. □

Exercise VI.5.12. Complete the proof of uniqueness in Theorem 5.6. (The hint in Exercise IV.6.1 may be helpful.)

Solution. Let R be a PID and suppose M_1, M_2 are isomorphic R-modules. In particular, we have $\operatorname{Tor}(M_1) \cong \operatorname{Tor}(M_2)$ and $\operatorname{rk} M_1 = \operatorname{rk} M_2$. It suffices to show that the decomposition of the torsion submodule is equivalent. We have

$$\operatorname{Tor}(M_1) \cong \frac{R}{(a_1)} \oplus \cdots \oplus \frac{R}{(a_m)} \cong \frac{R}{(b_1)} \oplus \cdots \oplus \frac{R}{(b_n)} \cong \operatorname{Tor}(M_2).$$

Since R is a PID and in particular a UFD, the decomposition of $\operatorname{Tor}(M_1)$ is unique up to associates so $m = n$. Thus, we can rearrange the factors such that the p_i are associate to the q_i for $i = 1, \ldots, n$. The uniqueness for form of elementary divisors follows easily. □

Exercise VI.5.13. Let M be a finitely generated module over a Noetherian ring R.

Prove that if R is a PID, then M is torsion-free if and only if it is free. Prove that this property characterizes PIDs. (Cf. Exercise 4.3.)

Solution. If M is torsion-free, then the structure theorem yields $M \cong R^{\operatorname{rk} M}$ so M is free. If M is free, then it has a basis E. Let $m = a_1 e_1 + \cdots a_n e_n \in M$. Then for $r \neq 0$ in R

$$rm = (ra_1)e_1 + \cdots + (ra_n)e_n \neq 0$$

since $a_i \neq 0 \Rightarrow ra_i \neq 0$. Thus, M is torsion-free.

Now suppose that R is merely a Noetherian domain and every finitely generated module M is torsion-free if and only if it is free. Clearly every ideal $I \subseteq R$ is torsion-free and finitely generated, so I must be free. Assume I is generated by more than one element, say a_1, a_2. Then $a_2a_1 - a_1a_2 = 0$ is a dependence relation in R so $a_1 = a_2 = 0$, contradicting the fact that they form a basis for I. Thus, I is generated by one element and R is a PID. □

Exercise VI.5.14. Give an example of a finitely generated module over an integral domain which is *not* isomorphic to a direct sum of cyclic modules.

Solution. Consider the integral domain $R = \mathbb{Z}[x]$ and the module $M = (2, x)$. Suppose M is a direct sum of cyclic $\mathbb{Z}[x]$ modules. If (N_a) is a family of cyclic submodules of M such that $M = \sum_{a \in A} N_a$ and $N_b \cap \sum_{a \neq b} N_a = 0$ for all $b \in A$, then each N_a is a principal ideal in $\mathbb{Z}[x]$. But clearly if $x_a \in N_a$ and $x_b \in N_b$ then $x_a x_b \in N_a \cap N_b$ so $N_a \cap N_b \neq 0$ and $|A| = 1$, which implies that M is a principal ideal, a contradiction. □

Exercise VI.5.15. Prove that the prime ideals appearing in the elementary divisor version of the classification theorem for a torsion module M over a PID are the prime ideals containing the characteristic ideal of M, as defined in Remark 5.8.

Solution. Recall that given a torsion module

$$M \cong \frac{R}{(a_1)} \oplus \cdots \oplus \frac{R}{(a_m)}$$

with $a_1 \mid \cdots \mid a_m$, we define

$$(a_1 \cdots a_m)$$

to be the characteristic ideal of M. To do. □

Exercise VI.5.16. Prove that the prime ideals appearing in the elementary divisor version of the classification theorem for a module M over a PID are the associated primes of M, as defined in Exercise 4.5.

Solution. To do. □

Exercise VI.5.17. Let R be a PID. Prove that the Grothendieck group of the category of finitely generated R-modules is isomorphic to $\mathbb{Z}$.

Solution. Let M be an R-module. By the structure theorem, we have $M \cong R^{\operatorname{rk} M} \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$. Next note that we may construct the exact sequence

$$0 \longrightarrow R \xrightarrow{\;a\;} R \longrightarrow \frac{R}{(a)} \longrightarrow 0$$

which implies that $[R/(a)] = [0]$ for all $a \in R$. Then we consider the homomorphism $\varphi : K(R\text{-}\mathsf{Mod}^{fg}) \to \mathbb{Z}$ which sends a module M to $\operatorname{rk} M$. It is easy to check that this morphism is well-defined, it is surjective, and the kernel is $[0]$, so it is injective. Thus, φ is an isomorphism. $\square$