Who is the happiest of men? He who values the merits of others,
And in their pleasure takes joy, even as though 'twere his own.

— Johann Wolfgang Von Goethe

In memory of Cláudio de Souza Leão.
1960 – 2018

CONTENTS

I

PRELIMINARIES: SET THEORY AND CATEGORIES

1 NAIVE SET THEORY

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

■ SOLUTION As Aluffi says in the second page, we often define a set by saying that its elements are exactly those which satisfy some property P. Russell's paradox shows that this characterization is not always well-defined. For example, consider

$$A = \{x \mid x \notin x\}.$$

This is the *axiom schema of (unrestricted) comprehension* from *naive set theory*

If A is really a set, we can ask whether A is an element of itself or not. If $A \in A$, then A should satisfy the property defining A. That is, $A \notin A$, which is absurd! However, if A is not an element of itself then it satisfies the defining property of A, which is also an absurd.

This shows that naive set theory is inconsistent. As a solution, Ernst Zermelo and Abraham Fraenkel developed a consistent axiomatic system for set theory. Their theory does not allow general entities of the form $\{x \mid P(x) \text{ is true}\}$ but only subsets of the form

$$\{x \in A \mid P(x) \text{ is true}\}$$

This is the *axiom schema of specification* in ZFC.

when A is already known to be a set. From now on, all sets will be defined in this way. ■

Remark. Russell's paradox is also intimately related to the *axiom of regularity*, which asserts that for every nonempty set A, there exists $B \in A$ such that $A \cap B = \emptyset$. In particular, there does not exists a set such that $A \in A$. As we have argumented above, axiom schema of specification and Russell's paradox implies there does not exists a set of all sets in ZFC. This follows independently by the axiom of regularity.

There are, however, ways of making sense of the *axiom schema of comprehension*. In NBG (von Neumann-Bernays-Gödel) set theory, there is the notion of a *class*, which, in a way, generelizes the idea of sets. *A class is a collection of sets defined by a formula*. Therefore,

$$\{\, x \mid x \text{ is a set} \,\}$$

and

$$\{\, x \mid x \notin x \,\}$$

are classes, but not sets (what we call *proper classes*). Intuitively, proper classes are collections *too big* to be sets. As we have claimed above, every set is a class: any set A is defined by the formula $x \in A$, hence it is a class.

EXERCISE 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. [§1.5]

■ SOLUTION By reflexivity,

$$(\forall a \in S)\ a \in [a]_\sim,$$

hence every element is nonempty and their union is S. Furthermore, suppose $[a]_\sim \cap [b]_\sim \neq \emptyset$ and let e be one of its elements. Then $e \sim a$ and $e \sim b$, and, using symmetry and transitivity, we conclude $a \sim b$. In this case,

$$\begin{aligned} c \in [a]_\sim &\iff c \sim a \\ &\iff c \sim a \text{ and } a \sim b \\ &\iff c \sim b \\ &\iff c \in [b]_\sim \end{aligned}$$

and $[a]_\sim = [b]_\sim$. In other words, they're either disjoint or equal. ■

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

■ SOLUTION We define the relation by

$$(\forall a \in S)(\forall b \in S)\ a \sim b \iff (\exists P \in \mathscr{P})\ a \in P \text{ and } b \in P.$$

Let's prove that it is indeed an equivalence relation:

- Reflexivity: Since $\mathscr{P}$ is a partition on S, there exists $P \in \mathscr{P}$ such that $a \in P$. It follows that $a \sim a$.
- Symmetry: If $a, b \in S$ are such that $a \sim b$, then there exists $P \in \mathscr{P}$ satisfying $a \in P$ and $b \in P$. We conclude that $b \in P$ and $a \in P$, that is, $b \sim a$.
- Transitivity: Given $a, b, c \in S$ with $a \sim b$ and $b \sim c$, there exist $P, Q \in \mathscr{P}$ such that $a, b \in P$ and $b, c \in Q$. Since $\mathscr{P}$ is a partition on S and $b \in P \cap Q$, then $P = Q$. Hence, $a, c \in P$ and $a \sim c$.

Finally, we see that $\mathscr{P}$ is the corresponding partition of the equivalence relation $\sim$ due to its definition: given $a \in S$ and $P \in \mathscr{P}$ with $a \in P$, then $b \in P \iff b \sim a \iff b \in [a]_\sim$ and $P = [a]_\sim$. ■

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

The number of equivalence relations on the set $\{1,\dots,n\}$ is the n-th *Bell number*.

■ SOLUTION As we saw, this question amounts to asking in how many ways we can partition this set. A quick thought shows that these are all the possible partitions:

$$\{\{1,2,3\}\},\quad \{\{1\},\{2,3\}\},\quad \{\{2\},\{3,1\}\},$$
$$\{\{3\},\{1,2\}\},\quad \{\{1\},\{2\},\{3\}\}.$$

Hence, there are exactly 5 equivalence relations on this set. ■

EXERCISE 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? (Hint: Thinking about the second question will help you answer the first one.)

■ SOLUTION Let $S = \mathbb{R}$ and consider the relation

$$a \sim b \iff |a-b| < 1.$$

Then, indeed, $\sim$ is reflexive, since $a - a = 0$, and is symmetric, since $|a-b| = |b-a|$. On the other hand, $0 \sim \frac{1}{2}$ and $\frac{1}{2} \sim 1$, but $0 \nsim 1$, therefore the relation is not transitive.

As we try to construct the partition, we define, as usual,

$$[a]_\sim = \{b \in S \mid b \sim a\}.$$

If follows that each $[a]_\sim$ is non-empty, since the relation is reflexive, and $b \in [a]_\sim \iff a \in [b]_\sim$, since the relation is symmetric. But the intersection of two different sets may be nonempty, as we can see in our example. ■

EXERCISE 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 $\mathbb{R}/\sim$. 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 $b_2 - a_2 \in \mathbb{Z}$. [§II.8.1, II.8.10]

■ SOLUTION We see that $\sim$ satisfies the following:

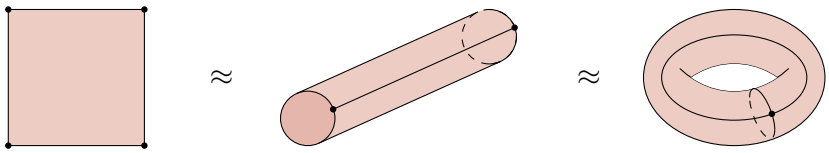
- Reflexivity: If $a \in \mathbb{R}$, then $a - a = 0 \in \mathbb{Z}$ and $a \sim a$.
- Symmetry: Given $a, b \in \mathbb{R}$ with $a \sim b$, we have $b - a \in \mathbb{Z}$. Thus $a - b = -(b-a) \in \mathbb{Z}$ and $b \sim a$.
- Transitivity: If $a, b, c \in \mathbb{R}$ are such that $a \sim b$ and $b \sim c$, then $b - a \in \mathbb{Z}$ and $c - b \in \mathbb{Z}$. So $c - a = (b-a) + (c-b) \in \mathbb{Z}$ and $a \sim c$.

Therefore, $\sim$ is an equivalence relation. Furthermore, observe that each element of $\mathbb{R}/\sim$ is the set of all real numbers with the same fractional part. We can also view $\mathbb{R}/\sim$ as the unitary circle S^1, where each equivalence class corresponds to an angle. This last description is interesting because each element of $\mathbb{R}$ is equivalent to some number in the interval $[0,1]$ and note that $0 \sim 1$. In this sense, we can 'connect' the endpoints of this line segment to form a circle. It will make more sense when considering those sets as groups (see the references indicated above).

Similarly, the relation $\approx$ is an equivalence one:

- Reflexivity: If $(a_1, a_2) \in \mathbb{R} \times \mathbb{R}$, then $a_1 - a_1 = a_2 - a_2 = 0 \in \mathbb{Z}$ and $(a_1, a_2) \approx (a_1, a_2)$.
- Symmetry: Given $(a_1, a_2), (b_1, b_2) \in \mathbb{R} \times \mathbb{R}$ that are equivalent, we have $b_1 - a_1 \in \mathbb{Z}$ and $b_2 - a_2 \in \mathbb{Z}$. Thus $a_1 - b_1 = -(b_1 - a_1) \in \mathbb{Z}$ and $a_2 - b_2 = -(b_2 - a_2) \in \mathbb{Z}$, so $(b_1, b_2) \approx (a_1, a_2)$.
- Transitivity: If $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in \mathbb{R} \times \mathbb{R}$ are such that $(a_1, a_2) \approx (b_1, b_2)$ and $(b_1, b_2) \approx (c_1, c_2)$, then $b_1 - a_1$, $b_2 - a_2$, $c_1 - b_1$, $c_2 - b_2 \in \mathbb{Z}$. Therefore, $c_1 - a_1 = (c_1 - b_1) + (b_1 - a_1) \in \mathbb{Z}$ and $c_2 - a_2 = (c_2 - b_2) + (b_2 - a_2) \in \mathbb{Z}$, so $(a_1, a_2) \approx (c_1, c_2)$.

Every point of $\mathbb{R} \times \mathbb{R}$ is equivalent to a point of the square $[0,1] \times [0,1]$ (given $(a, b) \in \mathbb{R} \times \mathbb{R}$, note that $(a, b) \approx (a', b')$, where a' and b' denote the fractional part of a and b, respectively). Furthermore, we can identify opposite sides of the square, since $(x, 0) \approx (x, 1)$ and $(0, y) \approx (1, y)$ for all $x, y \in \mathbb{R}$. In this manner, $\mathbb{R} \times \mathbb{R}/\approx$ can be imagined as a square whose opposite sides are identified as the same.



Geometrically, one can 'glue' those opposite sides to form a torus in the 3-dimensional space. ∎

2 FUNCTIONS BETWEEN SETS

EXERCISE 2.1 ▷ How many different bijections are there between a set S with n elements and itself? [§II.2.1]

∎ SOLUTION Let $S = \{x_1, \ldots, x_n\}$. In order to have a bijection $f : S \to S$, we'll define this function element by element. Firstly, $f(x_1)$ can be any element of S. That is, we have n options for the image of x_1. Having chosen $f(x_1)$, $f(x_2)$ can be any element of S different from

$f(x_1)$. That is, we have $n-1$ options left. In this way, we see that there are

$$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1 = n!$$

bijections between S and itself. ∎

EXERCISE 2.2 ▷ Prove statement (2) in Proposition 2.1. You may assume that given a family of disjoint nonempty subsets of a set, there is a way to choose one element in each member of the family. [§2.5, V .3.3]

PROPOSITION 2.1 Assume $A \neq \emptyset$, and let $f\colon A \to B$ be a function. 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.

∎ SOLUTION We'll divide the proof in two steps.

($\Longrightarrow$) If $f\colon A \to B$ has a right-inverse, then there exists $g\colon B \to A$ such that $f \circ g = \mathrm{id}_B$, i.e., for each $b \in B$, $f(g(b)) = b$. Therefore, $b \in \operatorname{im} f$, and f is surjective.

($\Longleftarrow$) If f is surjective, then for each $b \in B$, $f^{-1}(b)$ is nonempty. Choose an element $a \in f^{-1}(b)$ and define $g(b) = a$. By definition, $g\colon B \to A$ is a well-defined function such that $f \circ g = \mathrm{id}_B$. Therefore, f has a right-inverse. ∎

Here we use the axiom of choice.

EXERCISE 2.3 Prove that the inverse of a bijection is a bijection and that the composition of two bijection is a bijection.

∎ SOLUTION Let $f : A \to B$ be a bijection. If $b_1, b_2 \in B$ are such that $f^{-1}(b_1) = f^{-1}(b_2)$, then

$$\begin{aligned} f^{-1}(b_1) = f^{-1}(b_2) &\implies f(f^{-1}(b_1)) = f(f^{-1}(b_2)) \\ &\implies \mathrm{id}_B(b_1) = \mathrm{id}_B(b_2) \\ &\implies b_1 = b_2. \end{aligned}$$

Thus, f^{-1} is injective. Now, let $a \in A$ and take $b = f(a)$. Then $f^{-1}(b) = f^{-1}(f(a)) = (f^{-1} \circ f)(a) = \mathrm{id}_A(a) = a$, so f^{-1} is also surjective. We conclude that f^{-1} is a bijection.

For the second part, let $g : B \to C$ be another bijection. Firstly, if $a_1, a_2 \in A$ are such that $(g \circ f)(a_1) = (g \circ f)(a_2)$, then

$$g(f(a_1)) = g(f(a_2)) \implies f(a_1) = f(a_2) \implies a_1 = a_2,$$

since both f and g are injective. Secondly, given $c \in C$, there exists $b \in B$ such that $g(b) = c$, because g is surjective. Again, there exists $a \in A$ such that $f(a) = b$, since f is also surjective, and so we have $(g \circ f)(a) = g(f(a)) = g(b) = c$. Therefore, $g \circ f$ is both injective and surjective, that is, $g \circ f$ is a bijection. ∎

EXERCISE 2.4 ▷ Prove that isomorphism is an equivalence relation (on any set of sets). [§4.1]

■ SOLUTION Two sets A and B are isomorphic if there exists a bijection $f : A \to B$ between them. This relation is reflexive since id_A is a bijection between A and itself. It is symmetric since if $f : A \to B$ is a bijection, so is $f^{-1} : B \to A$. Last but not least, it is transitive since is $f : A \to B$ and $g : B \to C$ are bijections, so is $g \circ f : A \to C$. ■

EXERCISE 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. [§2.6, §4.2]

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

■ SOLUTION A function $f\colon A \to B$ is an *epimorphism* if the following holds:

$$\textit{for all sets } Z \textit{ and all functions } \beta', \beta'' \colon B \to Z$$

$$\beta' \circ f = \beta'' \circ f \implies \beta' = \beta''.$$

The desired analogue is the following.

A function is surjective if and only if it is an epimorphism.

Let us prove this result.

($\implies$) By proposition 2.1, if f is surjective, then it has a right-inverse $g\colon B \to A$. Let Z be any set and $\beta', \beta'' \colon B \to Z$ functions satisfying

$$\beta' \circ f = \beta'' \circ f.$$

Composing on the right by g we get

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

which means $\beta' = \beta''$, since $f \circ g = \mathrm{id}_B$.

($\impliedby$) If f is an epimorphism, then let $b' \in B$ be an arbitrary element and define

$$\beta'(b) = \begin{cases} 1, \text{ if } b = b', \\ 0, \text{ otherwise,} \end{cases}$$

and $\beta'' \equiv 0$. Since $\beta' \neq \beta''$, then $\beta' \circ f \neq \beta'' \circ f$, which means there exists a such that $\beta'(f(a)) \neq \beta''(f(a))$. But this can only happen if $f(a) = b'$, therefore f is surjective. ■

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

■ SOLUTION Recall that a section of a function is a right-inverse. Since π_A is surjective, it admits sections. Let g be defined as follows:

$$\begin{aligned} g : A &\longrightarrow A \times B \\ a &\longmapsto (a, f(a)). \end{aligned}$$

We claim that g is a section of π_A. Indeed, for all $a \in A$, we have $(\pi_A \circ g)(a) = \pi_A(g(a)) = \pi_A((a, f(a))) = a = \mathrm{id}_A(a)$. Thus, $\pi_A \circ g = \mathrm{id}_A$ and g is a right-inverse of π_A. ■

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

■ SOLUTION Let $\varphi_f : A \to \Gamma_f$ be defined as $\varphi_f(a) := (a, f(a))$. This function is clearly injective and it is surjective by the very definition of Γ_f. Thus, A and Γ_f are isomorphic. ■

EXERCISE 2.8 Describe as explicitly as you can all terms in the canonical decomposition (cf. §2.8) 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 $\sim$ be the equivalence relation defined by

$$r \sim r' \iff e^{2\pi i r} = e^{2\pi i r'} \iff e^{2\pi i (r - r')} = 1.$$

Since $e^{2\pi i z} = 1 \iff z \in \mathbb{Z}$, this is the same equivalence relation as the one defined in Exercise 1.6, which means the first function $\mathbb{R} \twoheadrightarrow (\mathbb{R}/\!\sim)$ can be seen as the function *fractional part* $\{\cdot\} : \mathbb{R} \to [0, 1)$ which sends each real number r into the smallest non-negative real number such that $r - \{r\} \in \mathbb{Z}$. Since $(\mathbb{R}/\!\sim) \cong [0, 1)$, we can regard the isomorphism

$$(\mathbb{R}/\!\sim) \underset{\tilde{f}}{\overset{\sim}{\to}} S^1,$$

where S^1 is the unit circle in $\mathbb{C}$ as a function $[0, 1) \to S^1$ where you first stretch the interval so that its length is 2π, then you glue its edges, forming a circle.The final function is simply the injection $S^1 \hookrightarrow \mathbb{C}$ which sends a number to itself. ■

EXERCISE 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 $A \amalg B$ (as described in §1.4) is well-defined *up to isomorphism* (cf. §2.9). [§2.9, 5.7]

■ SOLUTION Since $A' \cong A''$ and $B' \cong B''$, there are bijections $\alpha : A' \to A''$ and $\beta : B' \to B''$. Define $f : A' \cup B' \to A'' \cup B''$ by

$$f(x) = \begin{cases} \alpha(x), \text{ if } x \in A' \\ \beta(x), \text{ if } x \in B'. \end{cases}$$

Since $A' \cap B' = \emptyset$, f is well-defined. We claim that f is a bijection. Let $x, y \in A' \cup B'$ such that $f(x) = f(y)$. Since A'' and B'' are disjoint sets, either $x, y \in A'$ or $x, y \in B'$. In the first case, we have $f(x) = f(y) \implies \alpha(x) = \alpha(y) \implies x = y$, because α is injective. The other case is similar. Therefore, f is injective.

On the other hand, given $z \in A'' \cup B''$, either $z \in A''$ and so there exists $a \in A'$ such that $f(a) = \alpha(a) = z$, or $z \in B''$ and so there exists $b \in B'$ such that $f(b) = \beta(b) = z$, because both α and β are surjective. We proved that f is also surjective and, thus, f is a bijection, establishing an isomorphism between $A' \cup B'$ and $A'' \cup B''$.

Finally, we conclude that the operation $A \amalg B$ is well-defined up to isomorphism, as described in the penultimate paragraph before the exercise section. ■

EXERCISE 2.10 ▷ Show that if A and B are finite sets, then $|B^A| = |B|^{|A|}$. [§2.1, 2.11, §II.4.1]

■ SOLUTION We want to count how many functions from A to B are there. For each $a \in A$, $f(a)$ can be any of the $|B|$ elements of B. Hence we have

$$\underbrace{|B| \cdot |B| \cdot \ldots \cdot |B|}_{|A| \text{ times}} = |B|^{|A|}$$

possible functions. ■

EXERCISE 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 (cf. §1.2) [§1.2, III.2.3]

■ SOLUTION Consider the function $\chi \colon \mathscr{P}(A) \to 2^A$ which assigns for each $B \subseteq A$ a function

$$\chi_B(a) = \begin{cases} 1, \text{ if } a \in B, \\ 0, \text{ otherwise.} \end{cases}$$

Its inverse is the function $\mathbb{1} \colon 2^A \to \mathscr{P}(A)$ which sends each function $f \colon A \to \{0, 1\}$ to the set $\mathbb{1}(f) := f^{-1}(1)$.

In fact, for each $B \subseteq A$, then $\mathbb{1}(\chi_B) = \chi_B^{-1}(1) = B$, and similarly for each $f \in 2^A$,

$$\chi_{\mathbb{1}(f)}(a) = \begin{cases} 1, \text{ if } a \in \mathbb{1}(f), \\ 0, \text{ otherwise} \end{cases}$$

is clearly equal to f, hence $\mathbb{1}$ is the desired bijection. ∎

3 CATEGORIES

EXERCISE 3.1 ▷ Let C be a category. Consider a structure C^{op} with

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

Show how to make this into a category (that is, define composition of morphisms 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. [5.1, §VII.1.1, §IX.1.2, IX.1.10]

∎ SOLUTION Our given category C is endowed with a set-function

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

and we ought to define a new set-function

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

In other words, a set-function

$$\mathrm{Hom}_{\mathsf{C}}(B, A) \times \mathrm{Hom}_{\mathsf{C}}(C, B) \to \mathrm{Hom}_{\mathsf{C}}(C, A).$$

The only sensible choice here is to define $\circ_{\mathsf{C}^{op}}(f, g) := \circ_{\mathsf{C}}(g, f)$. The identity then is the one inherited by C. Composition in C^{op} is associative since

$$\begin{aligned}(h \circ_{\mathsf{C}^{op}} g) \circ_{\mathsf{C}^{op}} f &= f \circ_{\mathsf{C}} (g \circ_{\mathsf{C}} h) \\ &= (f \circ_{\mathsf{C}} g) \circ_{\mathsf{C}} h \\ &= h \circ_{\mathsf{C}^{op}} (g \circ_{\mathsf{C}^{op}} f).\end{aligned}$$

Also, the identity morphisms act as identities with respect to composition since for all $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B) = \mathrm{Hom}_{\mathsf{C}}(B, A)$,

$$\mathrm{id}_B \circ_{\mathsf{C}^{op}} f = f \circ_{\mathsf{C}} \mathrm{id}_B = f.$$

Similarly, $f \circ_{\mathsf{C}^{op}} \mathrm{id}_A = f$. Last but not least,

$$\mathrm{Hom}_{\mathsf{C}^{op}}(A, B) \cap \mathrm{Hom}_{\mathsf{C}^{op}}(C, D) = \mathrm{Hom}_{\mathsf{C}}(B, A) \cap \mathrm{Hom}_{\mathsf{C}}(D, C)$$

is empty unless $A = C$ and $B = D$. ∎

EXERCISE 3.2 If A is a finite set, haw large can be $\mathrm{End}_{\mathsf{Set}}(A)$?

∎ SOLUTION For each $a \in A$, we have $|A|$ options of image (each element of A), therefore $|\mathrm{End}_{\mathsf{Set}}(A)| \leq |A|^{|A|}$. ∎

EXERCISE 3.3 ▷ Formulate precisely what it means to say 1_a is an identity with respect to composition in Example 3.3, and prove this assertion. [§3.2]

■ SOLUTION If $a, b \in S$ are objects and $f \in \mathrm{Hom}(a, b)$ is a morphism, we need to show that

$$f1_a = 1_b f = f;$$

this is what it means to say 1_a and 1_b are identities with respect to composition. Since $f \in \mathrm{Hom}(a, b)$, we have that $\mathrm{Hom}(a, b)$ is nonempty and, therefore, $f = (a, b)$ is the only possible morphism from a to b. Thus, since $1_a = (a, a)$ and $1_b = (b, b)$, it follows that $f1_a = (a, b) = f$ and $1_b f = (a, b) = f$, by the definition of composition in this category. ■

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

■ SOLUTION No, we can't. The relation $<$ is not reflexive and hence our "category" doesn't have identities. ■

EXERCISE 3.5 ▷ Explain in what sense Example 3.4 is an instance of the categories considered in Example 3.3. [§3.2]

■ SOLUTION To explain Example 3.4 in terms of Example 3.3, we let $R = \mathscr{P}(S)$ be the set and the relation in R to be $\subseteq$. Then the objects of the category are exactly the elements of R and $\mathrm{Hom}(A, B)$ is the pair $(A, B) \in R \times R$ if $A \subseteq B$, and $\mathrm{Hom}(A, B) = \emptyset$ otherwise. ■

EXERCISE 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 product of matrices to define composition. Does this category 'feel' familiar? [§VI.2.1, §VIII.1.3]

■ SOLUTION Before defining V, we will first make sense of matrices with 0 rows or 0 columns. The motivation for the following definitions will be explained later. Let $m, n \in \mathbb{N}$ be positive integers. Then:

- There is only one $m \times 0$ matrix, denoted by 0^m: it is the only function from $\{0\}$ to $\mathbb{R}^m$ that sends 0 to $0_{\mathbb{R}^m}$.
- There is only one $0 \times n$ matrix, denoted by 0_n: it is the only function from $\mathbb{R}^n$ to $\{0\}$.
- There is only one 0×0 matrix, denoted by 1_0: it is the only function from $\{0\}$ to $\{0\}$.

Now, we define the multiplication rules for them. If A is a $p \times m$ matrix and B is a $n \times q$ matrix, where $p, q \in \mathbb{N}$ are positive integers, we

set $A \cdot 0^m = 0^p$ and $0_n \cdot B = 0_q$. Also, we set $0_m \cdot 0^m = 1_0$, $0^m \cdot 1_0 = 0^m$, $1_0 \cdot 0_n = 0_n$ and $1_0 \cdot 1_0 = 1_0$.

We are ready to define our category. Since the objects and the morphisms have been defined, we just need to specify how to compose morphisms and check if the conditions for V to be a category are verified.

Let m, n, p be objects of V. If $A \in \mathrm{Hom}_{\mathsf{V}}(m, n)$ and $B \in \mathrm{Hom}_{\mathsf{V}}(n, p)$, then A is a $n \times m$ matrix and B is a $p \times n$ matrix. To multiply two matrices, the number of columns of the first must be the same as the number of rows of the second, so we can take the product $B \cdot A$ (note that $A \cdot B$ is not always defined). Thus, we define the composition of A and B as $BA = B \cdot A$, which is a $p \times m$ matrix, so $BA \in \mathrm{Hom}_{\mathsf{V}}(m, p)$ as required. This composition law is associative, since matrix multiplication is associative (even for the 'zero' matrices). Also, for every $n \in \mathrm{Obj}(\mathsf{V})$, we have the $n \times n$ identity matrix 1_n with ones on the main diagonal and zeros elsewhere (or 1_0, if $n = 0$). From the definition of matrix multiplication, it follows that $A1_n = 1_m A = A$, for every $A \in \mathrm{Hom}_{\mathsf{V}}(n, m)$. Therefore, V is indeed a category.

Note that BA means to first apply A and then B, as we denote for morphisms. Some older authors, such as Herstein and Jacobson, would write AB to express the same idea.

This category represents all finite dimensional real vector spaces and the linear transformations between them. The object $n \in \mathbb{N}$ represents the space $\mathbb{R}^n$, which is isomorphic to every real vector space of dimension n. If $n = 0$, it represents the trivial vector space $\{0\}$, where 0 denotes the zero vector. Furthermore, morphisms encode linear transformations, since matrices are in one-to-one correspondence between, and the composition of morphisms defined here matches exactly with the composition of linear transformations.

This correspondence arises when we fix a basis, which, in this case, may be the canonical one.

That point of view motivated the definition of the 'zero' matrices: 0^m is the only possible transformation from $\{0\}$ to $\mathbb{R}^m$, 0_n is the only possible one from $\mathbb{R}^n$ to $\{0\}$, and 1_0 is the identity on $\{0\}$. ∎

EXERCISE 3.7 ▷ Define carefully objects and morphisms in Example 3.7, and draw the diagram corresponding to composition. [§3.2]

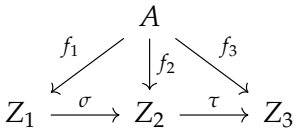
∎ SOLUTION An object of the *coslice* category C^A is a morphism $f \in \mathrm{Hom}_{\mathsf{C}}(A, Z)$ for some object $Z \in \mathrm{Obj}(\mathsf{C})$. Having two objects of C^A,

$$\begin{array}{ccc} A & & A \\ {\scriptstyle f_1}\downarrow & & \downarrow{\scriptstyle f_2} \\ Z_1 & & Z_2\,, \end{array}$$

there's only one sensible way to define a morphism $f_1 \to f_2$: as a commutative diagram

$$\begin{array}{ccc} & A & \\ {\scriptstyle f_1}\swarrow & & \searrow{\scriptstyle f_2} \\ Z_1 & \xrightarrow{\sigma} & Z_2\,. \end{array}$$

As in the slice category C_A, composition correspond to putting two commutative diagrams side-by-side:



and, as before, the diagram obtained by removing the central arrow also commutes. ∎

EXERCISE 3.8 ▷ A *subcategory* C' of a category C consists of a collection of objects of C with sets of 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 composition 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.[4.4, §VI.1.1, §VIII.1.3]

∎ SOLUTION We can define Inf, the category of infinite sets, in the following way:

- $\mathrm{Obj}(\mathsf{Inf})$ = the class of infinite sets;
- for $A, B \in \mathrm{Obj}(\mathsf{Inf})$, $\mathrm{Hom}_{\mathsf{Inf}}(A,B) = B^A$.

Since every infinite set is, in particular, a set, and $\mathrm{Hom}_{\mathsf{Inf}}(A,B) = B^A = \mathrm{Hom}_{\mathsf{Set}}(A,B)$ it follows that Inf can be viewed as a full subcategory of Set. ∎

EXERCISE 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, obtaning 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.) [§2.2, §3.2, 4.5]

∎ SOLUTION We can define the category MSet by setting:

- $\mathrm{Obj}(\mathsf{MSet})$ = the class of all the sets S endowed with an equivalence relation $\sim_S$, which will be denoted by $(S, \sim_S)$;
- for $(S, \sim_S), (T, \sim_T) \in \mathrm{Obj}(\mathsf{MSet})$, let $\mathrm{Hom}((S, \sim_S), (T, \sim_T))$ be the set of functions f from S to T such that $a \sim_S b \implies f(a) \sim_T f(b)$.

We will write S for $(S, \sim_S)$ if the equivalence relation is clear from the context.

The identity 1_S consists of the identity function on S. Composition is defined by composing the corresponding functions, which still preserves equivalent elements, as required. Since all the conditions to be a category are trivially satisfied, we conclude that MSet is a category.

Note that there is a 'copy' of Set inside MSet: it corresponds to the pairs of the form $(S, =_S)$, where $=_S$ denotes the equality, that is,

$$a =_S b \iff a = b.$$

Furthermore, this 'copy' is a full subcategory, since $\mathrm{Hom}(S, T)$ ends up being the set of all functions between S and T if they are endowed with the equality.

Although not so obvious at first sight, this definition of multiset is much more general than the one given in §2.2. The ordinary multisets just have a finite number of repeated elements, whilst there can be infinite multiple instances of elements 'of the same kind' in objects of MSet. Hence, only objects $(S, \sim_S) \in \mathrm{Obj}(\mathsf{MSet})$ with finite equivalence classes determine ordinary multisets: the corresponding one is defined by the function

$$\begin{aligned} m : S/\sim_S &\longrightarrow \mathbb{N}^* \\ P &\longmapsto |P|. \end{aligned}$$

From this point of view, morphisms of multisets are just functions that respect elements 'of the same kind', that is, instances of the same element are mapped onto similar elements. ∎

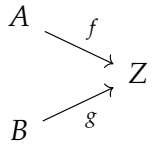
EXERCISE 3.10 Since the objects of a category C are not (necessarily interpreted as) sets, it is not clear how to make sense of a notion of 'subobject' in general. In some situations it *does* make sense to talk about subobjects, and the subobjects of any given object A in C are in one-to-one correspondence 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 This is exactly what we did in Exercise 2.11: a subset B of a given set A is nothing else than the data of a function $\chi_B : A \to \{0, 1\}$ such that $\chi_B(x) = 1$ if $x \in B$ and $\chi_B(x) = 0$ otherwise. Hence, $\{0, 1\}$ (or any two-element set) is a subobject classifier in Set. ∎

EXERCISE 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. [§5.5, 5.12]

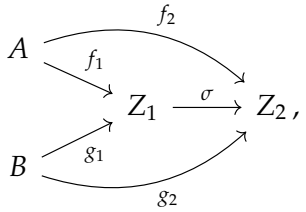
■ SOLUTION We define the category $\mathsf{C}^{A,B}$ similarly as we have defined $\mathsf{C}_{A,B}$:

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



  in C which can be represented by (Z, f, g); and

- morphisms between (Z_1, f_1, g_1) and (Z_2, f_2, g_2) can be represented by the commuting diagram



  viz., they are morphism $\sigma\colon Z_1 \to Z_2$ in C such that $\sigma f_1 = f_2$ *and* $\sigma g_1 = g_2$.

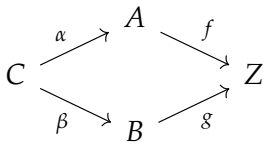
The composition of two morphisms $\sigma\colon (Z_1, f_1, g_1) \to (Z_2, f_2, g_2)$ and $\tau\colon (Z_2, f_2, g_2) \to (Z_3, f_3, g_3)$ is a morphism

$$\tau\sigma\colon (Z_1, f_1, g_1) \to (Z_3, f_3, g_3).$$

In fact, $\tau\sigma\colon Z_1 \to Z_3$ satisfies $\tau\sigma f_1 = \tau f_2 = f_3$ and $\tau\sigma g_1 = \tau g_2 = g_3$. Furthermore, the identity $1_{(Z,f,g)}$ is the morphism $1_Z\colon Z \to Z$. The conditions are trivially satisfied.

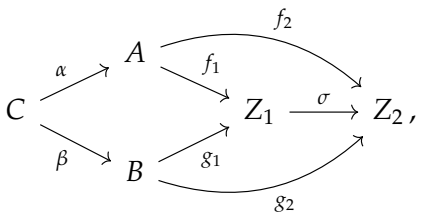
Analogously, fixed two morphisms $\alpha\colon C \to A$ and $\beta\colon C \to B$, we define the category $\mathsf{C}^{\alpha,\beta}$ as follows:

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



  in C which can be represented as (Z, f, g); and

- morphisms between (Z_1, f_1, g_1) and (Z_2, f_2, g_2) corresponds to commutative diagrams



viz., they are morphisms $\sigma\colon Z_1 \to Z_2$ such that $\sigma f_1 = f_2$ and $\sigma g_1 = g_2$.

The composition and identity are the same as in $\mathsf{C}^{A,B}$. In fact, $\mathsf{C}^{\alpha,\beta}$ is a full subcategory of $\mathsf{C}^{A,B}$. ∎

4 MORPHISMS

EXERCISE 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:

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

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.) [§4.1, §II.1.3]

∎ SOLUTION As we hope the reader has already followed the guideline of the exercise, we will begin directly by the general case. If $n = 3$, this is associativity:

$$(f_3 f_2)f_1 = f_3(f_2 f_1).$$

Assuming the result is valid for all compositions of up to $n-1$ morphisms, we decompose a arbitrary composition f in

$$f = AB,$$

where A ends right after we have the same number of right and left parentheses and B is what is left. For example, if $f = ((f_5 f_4)f_3)(f_2 f_1)$, $A = ((f_5 f_4)f_3)$ and $B = (f_2 f_1)$. Notice that A is equal to f if and only if f is already in the canonical choice of placement of the parentheses proposed by the exercise. If this is the case, we are done. If not, we write B in the canonical placement:

$$B = ((\cdots((f_k f_{k-1})f_{k-2})\cdots)f_1).$$

Then, by associativity,

$$\begin{aligned} f &= A((\cdots((f_k f_{k-1})f_{k-2})\cdots)f_1) \\ &= (A((\cdots((f_k f_{k-1})f_{k-2})\cdots)f_2)f_1. \end{aligned}$$

Using the induction hypothesis, we write $A((\cdots((f_k f_{k-1})f_{k-2})\cdots)f_2$ in the canonical placement and the result follows. ∎

A nice curiosity is that Catalan's number C_n is the number of different ways $n+1$ morphisms can be composed so that at every step one is only composing two morphisms.

EXERCISE 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 grupoid (cf. Example 4.6)? [§4.1]

■ SOLUTION Let $\sim$ be the relation and denote the category in Example 3.3 by $\mathsf{C}_\sim$. Since $\mathsf{C}_\sim$ is a grupoid, given $a \sim b$, the morphism $(a,b) \in \mathrm{Hom}_{\mathsf{C}_\sim}(a,b)$ has an inverse $(a,b)^{-1} \in \mathrm{Hom}_{\mathsf{C}_\sim}(b,a)$. This means the set is not empty, and $b \sim a$. Therefore the relation must be *symmetric* (and, in this case, it is an *equivalence relation*).

Reciprocally, let $\sim$ be an equivalence relation in a set S. Then we can define the category $\mathsf{C}_\sim$ as in Example 3.3. Given any elements $a, b \in \mathrm{Obj}(C_\sim) = S$, and an element $(a,b) \in \mathrm{Hom}_{\mathsf{C}_\sim}(a,b)$, then $a \sim b$ and $b \sim a$. We must show, then, that $(b,a) \in \mathrm{Hom}_{\mathsf{C}_\sim}(b,a)$ is the inverse of (a,b). In fact, by the composition rule,

$$(a,b)(b,a) = (a,a) = 1_a \quad \text{and} \quad (b,a)(a,b) = (b,b) = 1_b.$$

Therefore $(b,a) = (a,b)^{-1}$ and the category is a grupoid. ■

EXERCISE 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 explicit example of a category and an epimorphism without a right-inverse.

■ SOLUTION

- Let $g \in \mathrm{Hom}_{\mathsf{C}}(B,A)$ be a right-inverse for f and $Z \in \mathrm{Obj}(\mathsf{C})$ be an arbitrary object. If $\beta', \beta'' \in \mathrm{Hom}_{\mathsf{C}}(B,Z)$ are such that $\beta' \circ f = \beta'' \circ f$, then, by composing by g on the right, we have:

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

  Therefore, f is an epimorphism.

- However, the converse does not hold. For instance, suppose C is the category corresponding to endowing $\mathbb{Z}$ with the relation $\leq$, as in Example 3.3. Then, the morphism $(0,1)$ is an epimorphism (as pointed out in Example 4.10), but it cannot have a right-inverse because it would need to be in $\mathrm{Hom}_{\mathsf{C}}(1,0)$, which is the empty set since $1 \not\leq 0$. ■

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

■ SOLUTION Let $f : A \to B$ and $g : B \to C$ be monomorphisms. We want to prove that $g \circ f$ is also a monomorphism. That is, for all objects Z of C and all morphisms $\alpha', \alpha'' : Z \to A$,

$$g \circ f \circ \alpha' = g \circ f \circ \alpha'' \implies \alpha' = \alpha''.$$

This is a good time to make clear that in general categories morphisms which are both epi- and monomorphisms need not be isomorphisms. Nevertheless, the converse is true.

Since g is a monomorphism, $g \circ f \circ \alpha' = g \circ f \circ \alpha''$ implies $f \circ \alpha' = f \circ \alpha''$. The fact that f is a monomorphism now implies the result.

Since identities are always monomorphisms (and even isomorphisms since they are their own inverses), C_{mono} is really a subcategory of C. The analogous for epimorphisms follows from exactly the same reasoning. However, as identities are monomorphisms, $\mathsf{C}_{nonmono}$ is not a category. ■

EXERCISE 4.5 Give a concrete description of monomorphisms 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 Let $(R, \sim_R)$, $(T, \sim_T)$ and $(S, \sim_S)$ be objects of MSet. If $\sim_S$ is not the equality (trivial equivalence relation), then there exists $s', s'' \in S$ such that $s' \neq s''$, but $s' \sim s''$. In that case, let $\alpha' \colon R \to S$ and $\alpha'' \colon R \to S$ be defined by $\alpha'(r) = s'$, for every $r \in R$, and $\alpha''(r) = s''$, for every $r \in R$. Then $\alpha', \alpha'' \in \mathrm{Hom}((R, \sim_R), (S, \sim_S))$ are different morphisms, but for every $f \in \mathrm{Hom}((S, \sim_S), (T, \sim_T))$, by definition of the morphism, $f \circ \alpha' = f \circ \alpha''$.

In this case, the monomorphism depends on the information of both the morphism (injectivity) and the object (the equivalence relation).

Still, if $\sim_S$ is $=_S$, we *might* have a monomorphism. In fact, if $f \colon S \to T$ is injective, then $f \in \mathrm{Hom}((S, =_S), (T, \sim_T))$ and f is monomorphism, since it is, in particular, a set function. On the other hand, for any $s', s'' \in S$, let α' and α'' be defined as above. Since f is a monomorphism and $\alpha' \neq \alpha''$, it follows that $f \circ \alpha' \neq f \circ \alpha''$, which means $f(s') \neq f(s'')$ if $s' \neq s''$. Therefore the injections are the only monomorphisms.

At the same time, let $T = \{0, 1\}$ and $\sim_T$ be $=_T$. Then, if $s' \in S$, we define

$$\beta'(s) = \begin{cases} 1, \text{ if } s \in [s']_{\sim_S}, \\ 0, \text{ otherwise,} \end{cases}$$

and $\beta'' \equiv 0$. Since $\beta' \neq \beta''$, then $\beta' \circ f \neq \beta'' \circ f$ for any $f \in \mathrm{Hom}((R, \sim_R), (S, \sim_S))$; this means there exists $r \in R$ such that $f(r) \in [s']_{\sim_S}$. Since s' is arbitrary, this means that for any equivalence class $[s']_{\sim_S}$, there exists $r \in R$ such that $f(r) \in [s']_{\sim_S}$. Reciprocally, suppose f satisfies this condition. Then, for any $\beta' \neq \beta''$ in $\mathrm{Hom}((S, \sim_S), (T, \sim_T))$, there exists an equivalence class $[s']_S$ such that $\beta'(s) \neq \beta''(s)$ for any $s \in [s']_{\sim_S}$. In particular, there exists a such that $\beta'(f(a)) \neq \beta''(f(a))$. Therefore f is an epimorphism and we have categorized all monomorphisms and epimorphisms. ∎

5 UNIVERSAL PROPERTIES

EXERCISE 5.1 Prove that a final object is a category C is initial in the opposite category C^{op} (cf. Exercise 3.1).

∎ SOLUTION There's not really much to prove here. An object F of C is final if and only if $\mathrm{Hom}_{\mathsf{C}}(A, F)$ is a singleton for every $A \in \mathrm{Obj}(\mathsf{C})$. But that is, by definition, the same set as $\mathrm{Hom}_{\mathsf{C}^{op}}(F, A)$. The fact that the latter is a singleton is exactly the definition of F being a initial object in C^{op}. (Recall that C and C^{op} have the same objects.) ∎

EXERCISE 5.2 ▷ Prove that $\emptyset$ is the *unique* initial object in Set. [§5.1]

∎ SOLUTION Let A be nonempty, and $S = \{0, 1\}$. Then $f_0, f_1 \colon A \to S$ defined by $f_0(a) = 0$, for all $a \in A$ and $f_1(a) = 1$, for all $a \in A$ are two distinct elements in $\mathrm{Hom}_{\mathsf{Set}}(A, S)$. Therefore A cannot be an initial object in Set. ∎

EXERCISE 5.3 ▷ Prove that final objects are unique up to isomorphism. [§5.1]

∎ SOLUTION The proof is entirely analogous to the one given in Proposition 5.4.

Let C be a category. Recall that for every object A of C there is at least one element in $\mathrm{Hom}_{\mathsf{C}}(A, A)$, namely the identity 1_A. If F is final, then there is a *unique* morphism $F \to F$, which therefore must be the identity 1_F.

Let F_1 and F_2 be both final objects in C. Since F_2 is final, there is a *unique* morphism $f : F_1 \to F_2$ in C; we have to show that f is an isomorphism. Since F_1 is final, there is a unique morphism $g : F_2 \to F_1$ in C. Consider $gf : F_1 \to F_1$; as observed, necessarily $gf = 1_{F_1}$ since F_1 is final. By the same token, $fg = 1_{F_2}$ since F_2 is final. This proves that $f : F_1 \to F_2$ is an isomorphism, as needed. ∎

EXERCISE 5.4 What are the initial and final objects in the category of 'pointed sets' (Example 3.8)? Are they unique?

■ SOLUTION Recall that the category Set^* of pointed sets has pairs (S, s) of sets S and elements $s \in S$ as objects. A morphism $(S, s) \to (T, t)$ corresponds to a set-function $\sigma : S \to T$ such that $\sigma(s) = t$. Since there are no objects of the form (S, s) with $|S| = 0$ (because s should be an element of S) and those objects with $|S| > 1$ are clearly not initial nor final, the objects we seek have $|S| = 1$. We affirm then that objects of the form $(\{s\}, s)$ are the initial and final objects of Set^*.

Surely, there's only one morphism $(\{s\}, s) \to (T, t)$ since s has to be mapped to t. Also, since singletons are final in Set, the only morphism $(T, t) \to (\{s\}, s)$ is the constant function. The result follows. ■

EXERCISE 5.5 ▷ What are the final objects in the categories considered in §5.3? [§5.3]

■ SOLUTION Analogously to the Set category, the final objects will be the singletons. In fact, for each singleton $\{*\}$, let $\psi\colon A \to \{*\}$ be the constant function. Then for each pair (φ, Z), there exists a unique morphism $\varphi \to \psi$, viz. the constant function $\sigma : Z \to \{*\}$, therefore $(\psi, \{*\})$ is a final object.

Reciprocally, if Y has at least 2 elements (y_1 and y_2), let (ψ, Y) be an object of that category. Also, let (φ, Z) be such that $|Z| > |A|$ and $\varphi(z_1) \neq \varphi(z_2)$ if $z_1 \not\sim z_2$ (since $|Z| > |A|$, such φ exists and is not surjective). Then there are two morphism $\sigma_1, \sigma_2\colon (\varphi, Z) \to (\psi, Y)$ defined by:

$$\sigma_i(z) = \psi(a) \text{ if } z = \varphi(a) \quad \text{and} \quad \sigma_i(z) = y_i \text{ if } z \notin \operatorname{im} \varphi.$$

Hence, (ψ, Y) is not a final object. ■

EXERCISE 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? [§VII.5.1]

■ SOLUTION First of all, note that the divisibility relation is reflexive and transitive, so we can define this category as in Example 3.3.

Let $a, b \in \mathbb{Z}^+$. For a moment, suppose that the product $a \times b$ of a and b exists. Thus we know that $a \times b$ divides a and b, and, for all $z \in \mathbb{Z}^+$ such that z divides a and b, we have that z divides $a \times b$. This property is satisfied by the *greatest common divisor* of a and b. Therefore, this category has products.

Now, suppose that the coproduct $a \amalg b$ of a and b exists. Thus we know that a and b divide $a \amalg b$ and, for every $z \in \mathbb{Z}^+$ such that a and b divide z, we have that $a \amalg b$ divides z. This property is satisfied by

the *least common multiple* of a and b. Thereby, this category also has coproducts. ∎

Remark. The divisibility relation is a *partial order* over the set $\mathbb{Z}^+$, that is, it is reflexive, anti-symmetric and transitive. (By an *anti-symmetric* relation $\leq$ we mean that $a \leq b$ and $b \leq a$ implies $a = b$.) It is only a *partial* order because it is not true that a divides b or b divides a for all $a, b \in \mathbb{Z}^+$. Furthermore, $\mathbb{Z}^+$ with the divisibility relation is a *lattice*, as we shall define below.

Let $(L, \leq)$ be a partially ordered set (poset) and let $S \subseteq L$ be an arbitrary subset of L. An element $u \in L$ is an *upper bound* of S if $s \leq u$ for all $s \in S$. Similarly, an element $l \in S$ is a *lower bound* of S if $l \leq s$ for each $s \in S$. An upper bound u of S is said to be a *join* if $u \leq x$ for all upper bound x of S. Analogously, a lower bound l is said to be a *meet* if $x \leq l$ for each lower bound x of S. Finally, $(L, \leq)$ is called a *join-semilattice* if each two-element subset $\{a, b\} \subseteq L$ has a join, and is called a *meet-semilattice* if each two-element subest has a meet, denoted by $a \vee b$ and $a \wedge b$ respectively. A *lattice* is a partially ordered set which is both a join- and a meet-semilattice. Note that $\mathbb{Z}^+$ with the divisibility relation is a lattice where $a \vee b = \operatorname{lcm}(a, b)$ and $a \wedge b = \gcd(a, b)$ for all $a, b \in \mathbb{Z}^+$.

This exercise can be generalized to any lattice. Let $(L, \leq)$ be a partially ordered set and define the corresponding category C as in Example 3.3. Following the same argument given above, C has products if and only if $(L, \leq)$ is a meet-semilattice and it has coproducts if and only if $(L, \leq)$ is a join-semilattice. We deduce that C has both products and coproducts if and only if $(L, \leq)$ is a lattice, and in this case we have $a \times b = a \wedge b$ and $a \coprod b = a \vee b$ for all $a, b \in \operatorname{Obj}(\mathsf{C})$.

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

PROPOSITION 5.4 Let C be a category.

- If I_1, I_2 are both initial objects in C, then $I_1 \cong I_2$.
- If F_1, F_2 are both final objects in C, then $F_1 \cong F_2$.

Further, there isomorphisms are uniquely determined.

∎ SOLUTION Since the disjoint union $A \coprod B$ is the coproduct of A and B in Set (that is, an initial object in $\mathsf{Set}^{A,B}$), it is well-defined up to an isomorphism. ∎

EXERCISE 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.)

PROPOSITION 5.4 Let C be a category.

- If I_1, I_2 are both initial objects in C, then $I_1 \cong I_2$.
- If F_1, F_2 are both final objects in C, then $F_1 \cong F_2$.

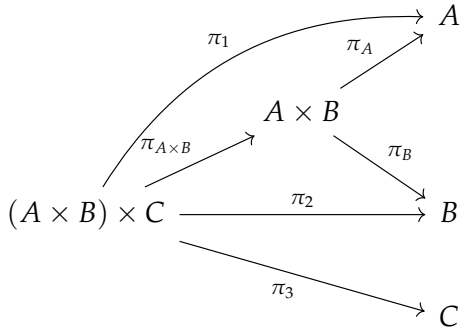
Further, there isomorphisms are uniquely determined.

■ SOLUTION Let's prove that both elements are final object of the same category, the one defined in §5.4. In fact, we already know $A \times B$ is a final element of this category. Let $\pi'_B \colon B \times A \to B$ and $\pi'_A \colon B \times A \to A$ be defined by $\pi'_B((b,a)) = b$ and $\pi'_A((b,a)) = a$. Let (Z, f_A, f_B) be an element in the category. Then $\sigma \colon Z \to B \times A$ defined by $\sigma(z) = (f_B(z), f_A(z))$ is a morphism from (Z, f_A, f_B) to $(B \times A, \pi'_A, \pi'_B)$. Furthermore, this morphism is unique since $\pi'_A(\sigma(z)) = f_A(z)$ and $\pi'_B(\sigma(z)) = f_B(z)$. Using the proposition, we can conclude $A \times B$ and $B \times A$ are isomorphic. ■

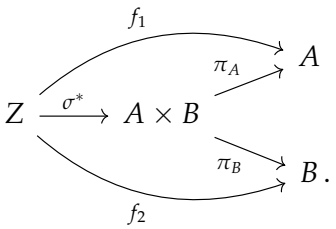
EXERCISE 5.9 Let C be a category with products. Find a reasonable candidate for the universal property that the product $A \times B \times C$ of *three* objects of C ought to satisfy, and prove that both $(A \times B) \times C$ and $A \times (B \times C)$ satisfy this universal property. Deduce that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

■ SOLUTION We define $A \times B \times C$ as a final object in the category $\mathsf{C}_{A,B,C}$, similar to what we did with only two objects. In this case, $\mathsf{C}_{A,B,C}$ is defined analogously as C_A or $\mathsf{C}_{A,B}$, but with three objects. For simplicity, we may denote $S_1 = A$, $S_2 = B$ and $S_3 = C$. Therefore, the product $A \times B \times C$ with morphisms $\{\pi_i : A \times B \times C \to S_i\}_{i \in \{1,2,3\}}$ satisfies the following universal property: for every object Z and morphisms $\{f_i : Z \to S_i\}_{i \in \{1,2,3\}}$ there exists a unique morphism $\sigma : Z \to A \times B \times C$ such that $\pi_i \circ \sigma = f_i$ for all $i \in \{1,2,3\}$.

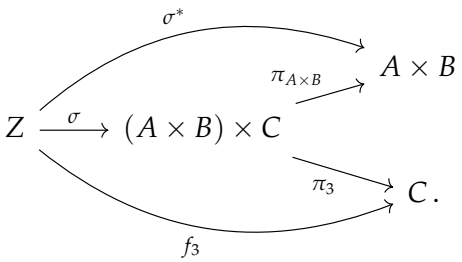
Now, let's prove that $(A \times B) \times C$ satisfies the universal property pointed above. Firstly, we have to define morphisms to A, B and C. By the definition of products in C, there exist morphisms $\pi_A : A \times B \to A$, $\pi_B : A \times B \to B$, $\pi_{A\times B} : (A \times B) \times C \to A \times B$ and $\pi_3 : (A \times B) \times C \to C$ satisfying the universal property for the corresponding products. We will take $\pi_1 = \pi_A \pi_{A\times B}$ and $\pi_2 = \pi_B \pi_{A\times B}$, as in the following diagram:



We claim that $((A \times B) \times C, \pi_1, \pi_2, \pi_3)$ is a final object in $\mathsf{C}_{A,B,C}$. Let $Z \in \mathrm{Obj}(\mathsf{C})$ and $f_i \in \mathrm{Hom}_{\mathsf{C}}(Z, S_i)$, where $i \in \{1,2,3\}$. By the universal property of $A \times B$, there exists a unique $\sigma^* : Z \to A \times B$ such that $f_1 = \pi_A \sigma^*$ and $f_2 = \pi_B \sigma^*$:



Now, by the universal property of $(A \times B) \times C$, there exists a unique $\sigma : Z \to (A \times B) \times C$ such that $\sigma^* = \pi_{A\times B}\sigma$ and $f_3 = \pi_3 \sigma$:



Finally, by associativity, we have

$$f_1 = \pi_A \sigma^* = \pi_A(\pi_{A\times B}\sigma) = (\pi_A \pi_{A\times B})\sigma = \pi_1 \sigma$$

$$f_2 = \pi_B \sigma^* = \pi_B(\pi_{A\times B}\sigma) = (\pi_B \pi_{A\times B})\sigma = \pi_2 \sigma\,,$$

thus we conclude σ is a morphism from (Z, f_1, f_2, f_3) to $((A \times B) \times C, \pi_1, \pi_2, \pi_3)$ in $\mathsf{C}_{A,B,C}$. We just need to show it is unique. Suppose that $\rho : Z \to (A \times B) \times C$ is such that $f_i = \pi_i \rho$ for all $i \in \{1,2,3\}$. Therefore, by the definition of π_1 and π_2, we have that $f_1 = \pi_A(\pi_{A\times B}\rho)$ and $f_2 = \pi_B(\pi_{A\times B}\rho)$. Since σ^* is unique, we must have $\sigma^* = \pi_{A\times B}\rho$. Last but not least, since $\sigma^* = \pi_{A\times B}\rho$ and $f_3 = \pi_3 \rho$, we conclude that $\rho = \sigma$. Therefore, $((A \times B) \times C, \pi_1, \pi_2, \pi_3)$ is indeed a final object in $\mathsf{C}_{A,B,C}$.

In a similar fashion, we can show that $A \times (B \times C)$ (with the appropriate morphisms) is also a final object in $\mathsf{C}_{A,B,C}$. Thus, we deduce that $(A \times B) \times C$ and $A \times (B \times C)$ are necessarily isomorphic by Proposition 5.4. ∎

EXERCISE 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 Let C be a category and I be a set. The product $\prod_{i\in I} A_i$, with morphisms $\{\pi_j : \prod_{i\in I} A_i \to A_j\}_{j\in I}$, of a family $\{A_i\}_{i\in I}$ of objects of C should satisfy the following universal property: for every object Z and morphisms $\{f_i : Z \to A_i\}_{i\in I}$ there exists a unique morphism $\sigma : Z \to \prod_{i\in I} A_i$ such that $\pi_i \circ \sigma = f_i$ for all $i \in I$.

Similarly, the coproduct $\coprod_{i\in I} A_i$, with the morphisms $\{\iota_j : A_j \to \coprod_{i\in I} A_i\}_{j\in I}$, of a family $\{A_i\}_{i\in I}$ of objects of C should satisfy the following universal property: for every object Z and morphisms $\{f_i : A_i \to Z\}_{i\in I}$ there exists a unique morphism $\sigma : \coprod_{i\in I} A_i \to Z$ such that $\sigma \circ \iota_i = f_i$ for all $i \in I$.

In Set, the categorical product is the Cartesian product and the coproduct is the disjoint union. ■

EXERCISE 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 $A/\sim_A$ and $B/\sim_B$.
- Conclude (without further work) that $(A \times B)/\sim \cong (A/\sim_A) \times (B/\sim_B)$.

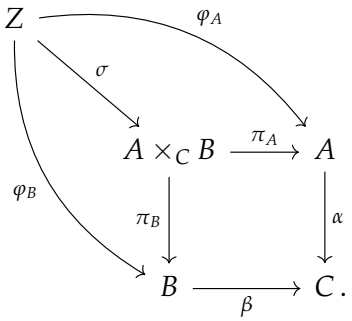
■ SOLUTION Let $\pi_{A/\sim_A} : A \times B \to A/\sim_A$ be defined by $\pi_{A/\sim_A}(a, b) = [a]_{\sim_A}$ and define $\pi_{B/\sim_B}$ in a similar fashion. If $(a_1, b_1) \sim (a_2, b_2)$, then $\pi_{A/\sim_A}(a_1, b_1) = \pi_{A/\sim_A}(a_2, b_2)$ and analogously for $\pi_{B/\sim_B}$. Therefore these functions are in the category defined in §5.3. Using the universal property for quotients, we know that there are unique morphisms $\tilde{\pi}_A : (A \times B)/\sim \to A/\sim_A$ and $\tilde{\pi}_B : (A \times B)/\sim \to B/\sim_B$ in this category. Let's prove that $((A \times B)/\sim, \tilde{\pi}_A, \tilde{\pi}_B)$ is a final object in the category defined in §5.4. In fact, let (Z, f_A, f_B) be an element in such category. Then if $f_A(z) = [a_z]_{\sim_A}$ and $f_B(z) = [b_z]_{\sim_B}$, let $\sigma : Z \to (A \times B)/\sim$ be defined by $\sigma(z) = [(a_z, b_z)]_\sim$. The definition of $\sim$ is such that this function is well-defined. Moreover this

function is unique, since any such morphism must satisfy $\tilde{\pi}_A(\sigma(z)) = f_A(z)$ and $\tilde{\pi}_B(\sigma(z)) = f_B(z)$. Using Proposition 1.5.4, we conclude $(A \times B)/\sim \cong (A/\sim_A) \times (B/\sim_B)$. ∎

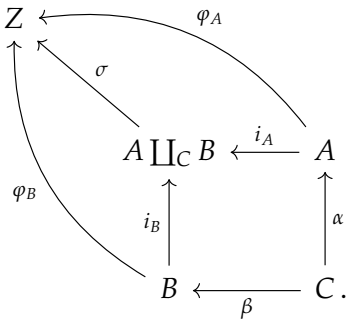
EXERCISE 5.12 ¬ Define the notions of *fibered products* and *fibered coproducts*, as terminal objects of the categories $\mathsf{C}_{\alpha,\beta}$, $\mathsf{C}^{\alpha,\beta}$ considered in Example 3.10 (cf. also Exercise 3.11), by stating carefully the corresponding universal properties.

As it happens, Set has both fibered products and coproducts. Define these objects 'concretely', in terms of naive set theory. [II.3.9, III.6.10, III.6.11]

∎ SOLUTION Let A, B, C be objects in C and $\alpha : A \to C$, $\beta : B \to C$ be two fixed morphisms. We define the corresponding *fibered product* as a final object in the category $\mathsf{C}_{\alpha,\beta}$. Thus, a object $A \times_C B$ with morphisms $\pi_A : A \times_C B \to A$, $\pi_B : A \times_C B \to B$ is a fibered product of α and β if $\alpha\pi_A = \beta\pi_B$ and the following universal property is satisfied: for every object Z and morphisms $\varphi_A : Z \to A$, $\varphi_B : Z \to B$ such that $\alpha\varphi_A = \beta\varphi_B$, there exists a unique morphism $\sigma : Z \to A \times_C B$ making the diagram below commute:



Similarly, if now we set $\alpha : C \to A$ and $\beta : C \to B$, we define the corresponding *fibered coproduct* as a initial object in the category $\mathsf{C}^{\alpha,\beta}$. Therefore, a object $A \coprod_C B$ with morphisms $i_A : A \to A \coprod_C B$, $i_B : B \to A \coprod_C B$ is a fibered coproduct of α and β if $i_A\alpha = i_B\beta$ and the following universal property is satisfied: for every object Z and morphisms $\varphi_A : A \to Z$, $\varphi_B : B \to Z$ such that $\varphi_A\alpha = \varphi_B\beta$, there exists a unique morphism $\sigma : A \coprod_C B \to Z$ making the diagram below commute:



In Set, we can find fibered products as follows. If A, B, C are sets and $\alpha : A \to C$, $\beta \to C$ are two functions, we claim that the set

$$A \times_C B = \bigcup_{x \in C} \alpha^{-1}(x) \times \beta^{-1}(x)$$

with the usual projections π_A and π_B is a fibered product of α and β. Note that we take the product of fibers of α and β over every element of C, which is suggested by the name *fibered product*. It is straightforward that $\alpha\pi_A = \beta\pi_B$ by the definition of $A \times_C B$. Now, if Z is another set together with functions $\varphi_A : Z \to A$, $\varphi_B : Z \to B$ such that $\alpha\varphi_A = \beta\varphi_B$, define $\sigma : Z \to A \times_C B$ by

$$\sigma(z) = (\varphi_A(z), \varphi_B(z))$$

for all $z \in Z$. This function is well-defined since $\alpha\varphi_A = \beta\varphi_B$, so $\varphi_A(z) \in \alpha^{-1}(x)$ and $\varphi_B(z) \in \beta^{-1}(x)$ for some $x \in C$. Furthermore, it follows that $\pi_A\sigma = \varphi_A$ and $\pi_B\sigma = \varphi_B$, so the first diagram above commutes. Finally, this definition of σ is forced by commutativity and so it is unique. Therefore, $A \times_C B$ with π_A and π_B is indeed the desired fibered product.

We can also find fibered coproducts in Set. Let A, B, C be sets and $\alpha : C \to A$, $\beta : C \to B$ be functions. If i_A^* and i_B^* denote the inclusion of A and B in $A \coprod B$, define $\sim$ on the disjoint union as the finest equivalence relation such that

$$(i_A^* \circ \alpha)(x) \sim (i_B^* \circ \beta)(x)$$

for all $x \in C$. By *finest equivalence relation* we mean that, if $\approx$ is an equivalence relation satisfying the property above, then $a \sim b \implies a \approx b$, for all $a, b \in A \coprod B$. This finest relation indeed exists: take the intersection of all the equivalence relations satisfying the property above (here we are using the definition that a relation on a set S is a subset of $S \times S$). Since the intersection of equivalence relations is again an equivalence relation and there is at least one that satisfies this property (which is the relation given by $(A \coprod B) \times (A \coprod B)$), it makes sense to talk about the finest one. Thus, define

$$A \coprod_C B = (A \coprod B)/\sim$$

and, if π is the canonical projection to the quotient, define $i_A = \pi i_A^*$ and $i_B = \pi i_B^*$. We claim that $A \coprod_C B$ with i_A and i_B is a fibered coproduct of α and β. Note that $i_A\alpha = i_B\beta$ by the definition of $\sim$. Now, let Z be another set together with functions $\varphi_A : A \to Z$, $\varphi_B : B \to Z$ such that $\varphi_A\alpha = \varphi_B\beta$. By the universal property of the coproduct, there exists a unique $\varphi : A \coprod B \to Z$ such that $\varphi_A = \varphi i_A^*$ and $\varphi_B = \varphi i_B^*$. Define $\sigma : A \coprod_C B \to Z$ by

$$\sigma([x]_\sim) = \varphi(x)$$

for all $[x]_\sim \in A \coprod_C B$. This definition is forced so that the second diagram above commutes. We just need to show that σ is well-defined. Consider the equivalence relation $\approx$ on $A \coprod B$ given by

$$a \approx b \iff \varphi(a) = \varphi(b).$$

Since $\varphi_A \alpha = \varphi_B \beta$, it follows that

$$\begin{aligned}(\varphi_A \alpha)(x) = (\varphi_B \beta)(x) &\implies ((\varphi i_A^*)\alpha)(x) = ((\varphi i_B^*)\beta)(x) \\ &\implies (\varphi(i_A^* \alpha))(x) = (\varphi(i_B^* \beta))(x) \\ &\implies (i_A^* \alpha)(x) \approx (i_B^* \beta)(x)\end{aligned}$$

for all $x \in C$. By the definition of $\sim$, we conclude that

$$[a]_\sim = [b]_\sim \implies a \sim b \implies a \approx b \implies \varphi(a) = \varphi(b),$$

so σ is well-defined. Therefore, $A \coprod_C B$ with i_A and i_B is indeed the desired fibered coproduct. ∎

II

GROUPS, FIRST ENCOUNTER

1 DEFINITION OF GROUP

EXERCISE 1.1 ▷ Write a careful proof that every group is the group of isomorphisms of a grupoid. In particular, every group is the group of automorphisms of some object in some category. [§2.1]

■ SOLUTION Recall that a grupoid is a category in which every morphism is an isomorphism. Let G be a group. As we saw in the beginning of the chapter, it may be a good idea to consider a category G with a single object $*$ and G as the set $\mathrm{Hom}_{\mathsf{G}}(*,*)$ of morphisms. We shall show that G is in fact a category in which every morphism is an isomorphism.

Notice the difference between G and G.

The identity element of G serves as the identity morphism $1_* \in \mathrm{Hom}_{\mathsf{G}}(*,*)$. The composition and the associativity of morphisms are inherited from those properties in G. We conclude that G is a category. Since G is a group, every morphism has a two-sided inverse and thus is an isomorphism. This makes G a grupoid. ■

EXERCISE 1.2 ▷ Consider the 'set of numbers' listed in §1.1, and decide which are made into groups by conventional operations such as $+$ and $\cdot$. Even if the answer is negative (for example, $(\mathbb{R},\cdot)$ is not a group), see if variations of the definition of these sets lead to groups (for example $(\mathbb{R}^*,\cdot)$ *is* a group; cf. §1.4). [§1.2]

■ SOLUTION In every 'set of numbers' ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$), the operation of addition and multiplication is associative. Also, in every set, 0 is the identity element of addition (since $a+0=0+a=a$ for every $a \in \mathbb{Z}$ or $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$), and analogously for 1 and multiplication. Therefore we'll only verify the inverse property. For every $n \in \mathbb{Z}$, $-n \in \mathbb{Z}$ and $n+(-n)=0$, from which we conclude $\mathbb{Z}$ is a group. If $r=\frac{p}{q} \in \mathbb{Q}$, then $-r=\frac{-p}{q} \in \mathbb{Q}$ and $r+(-r)=0$. Similarly for $\alpha \in \mathbb{R}$ and $z \in \mathbb{C}$. Since $(-1)(-1)=1$, the set $\{+1,-1\}$ is a group with the operation $\cdot$. Analogously, $(\mathbb{Q}^*,\cdot)$, $(\mathbb{R}^*,\cdot)$ and $(\mathbb{C}^*,\cdot)$ are groups; however $(\mathbb{Q},\cdot)$, $(\mathbb{R},\cdot)$ and $(\mathbb{C},\cdot)$ are not groups, since 0 does not have a multiplicative inverse. Furthermore, since $a>0 \implies \frac{1}{a}>0$ and since if $a,b>0$ then $a\cdot b>0$, the structures $(\mathbb{Q}_{>0},\cdot)$ and $(\mathbb{R}_{>0},\cdot)$ are groups. Finally, we can construct even strangers groups: if $\alpha \in \mathbb{C}\backslash\mathbb{Q}$, we define $\mathbb{Q}[\alpha] := \{p+q\alpha \mid p,q \in \mathbb{Q}\}$. Then the structures $(\mathbb{Q}[\alpha],+)$ and $(\mathbb{Q}[\alpha]^*,\cdot)$ are groups. We can do this construction for $\mathbb{Z}$, and they are similarly groups with addition, but not with multiplication, since the multiplicative inverse is not necessarily in the set, this occurs in

The Eisenstein integers can be used to prove *Fermat's Last Theorem* for $n = 3$.

particular for the elements of $\mathbb{Z} \subseteq \mathbb{Z}[\alpha]$. The set $\mathbb{Z}[i]$ is called the *Gaussian integers* and the set $\mathbb{Z}[e^{\frac{2\pi i}{3}}]$ is called the *Eisenstein integers*. ∎

EXERCISE 1.3 Prove that $(gh)^{-1} = h^{-1}g^{-1}$ for all elements g, h of a group G.

∎ SOLUTION By associativity, it follows that

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = geg^{-1} = gg^{-1} = e$$

and

$$(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}eh = h^{-1}h = e$$

for all $g, h \in G$. Since the inverse of gh is unique, we have that $(gh)^{-1} = h^{-1}g^{-1}$ for all $g, h \in G$. ∎

EXERCISE 1.4 Suppose that $g^2 = e$ for all elements g of a group G; prove that G is commutative.

∎ SOLUTION Let a and b be elements of G. All we know is that

$$a^2 = b^2 = (ab)^2 = (ba)^2 = e$$

and we shall deduce that $ab = ba$. We multiply both sides of $abab = (ab)^2 = e$ by a on the left and by b on the right to obtain

$$a^2bab^2 = ab.$$

Since $a^2 = b^2 = e$, this is the desired result. ∎

EXERCISE 1.5 The 'multiplication table' of a group is an array compiling the results of all multiplications $g \bullet h$:

$\bullet$	e	$\cdots$	h	$\cdots$
e	e	$\cdots$	h	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g	g	$\cdots$	$g \bullet h$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

(Here e is the identity elements. Of course the table depends on the order in which the elements are listed in the top row and leftmost column.) Prove that every row and every column of the multiplication table of a group contains all elements of the group exactly once (like Sudoku diagrams!).

∎ SOLUTION We'll prove the result for each row, and it follows analogously for each column. Given a row g and any element h in G, h appears in the row, since $g \bullet (g^{-1} \bullet h) = h$. Moreover, given h_1, h_2 in G, if $g \bullet h_1 = g \bullet h_2$, then $h_1 = h_2$ by the cancellation law, therefore each element appears only once, as we desired to prove. ∎

EXERCISE 1.6 ¬ Prove that there is only *one* possible multiplication table for G if G has exactly 1, 2, or 3 elements. Analyze the possible multiplication tables for groups with exactly 4 elements, and show that there are *two* distinct tables, up to reordering the elements of G. Use these tables to prove that all groups with ≤ 4 elements are commutative.

(You are welcome to analyze groups with 5 elements using the same technique, but you will soon know enough about groups to be able to avoid such brute-force approaches.) [2.19]

■ SOLUTION From Example 1.3, we know that there is only one possible multiplication table if $G = \{e\}$:

$\bullet$	e
e	e

If $|G| = 2$, one of the elements is the identity e. For the second element f, we already have that $f \bullet e = e \bullet f = f$. Since it needs to have an inverse, we must have $f \bullet f = e$, so the multiplication table is:

$\bullet$	e	f
e	e	f
f	f	e

If $|G| = 3$, we may denote it by $G = \{e, f, g\}$, where e is the identity element. Suppose that $f \bullet g = f$ or $f \bullet g = g$. In each case, by the cancellation law we would have $f = e$ or $g = e$, a contradiction. Thus, we must have $f \bullet g = e$ and $f^{-1} = g$, so we also know that $g \bullet f = e$. By Exercise 1.5, we must complete the multiplication table as follows:

$\bullet$	e	f	g
e	e	f	g
f	f	g	e
g	g	e	f

Finally, suppose that $G = \{e, f, g, h\}$, where e is the identity element. Let's find the inverses for each element. We have two cases: either every element is of order two, that is, $f^2 = g^2 = h^2 = e$, or just one of them is of order two and the remaining are inverses for each other. In this last case, possibly after renaming the elements, we have that $f \bullet h = h \bullet f = e$ and $g^2 = e$. In both cases, note that we cannot have $f \bullet g = e = g \bullet g$, $f \bullet g = f = f \bullet e$ or $f \bullet g = g = e \bullet g$ because it would follow from the cancellation law that $f = g$, $g = e$ or $f = e$, a contradiction. Thus, we must have $f \bullet g = h$. Similarly, $g \bullet f = h$ and

$g \bullet h = h \bullet g = f$. By Exercise 1.5, we must fill the multiplication table for the first case as

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	e	h	g
g	g	h	e	f
h	h	g	f	e

and for the second case as

$\bullet$	e	f	g	h
e	e	f	g	h
f	f	g	h	e
g	g	h	e	f
h	h	e	f	g

.

These groups are isomorphic to C_2, C_3, $C_2 \times C_2$ and C_4, respectively.

From these tables, we conclude that all groups with ≤ 4 elements are commutative.

If $|G| = 5$, we could use the same technique to show that there is only one possible multiplication table, up to reordering of the elements of G. As an illustration of the tools we will soon develop, we could simplify this computation. Since $|G|$ is a prime number and the order of each element must divide it, we have that $|g| = 5$ for all $g \in G$ different from the identity element. Therefore, G is cyclic and, for all $g \in G, g \neq e$, it follows that $G = \{e, g, g^2, g^3, g^4\}$ and the multiplication table is:

$\bullet$	e	g	g^2	g^3	g^4
e	e	g	g^2	g^3	g^4
g	g	g^2	g^3	g^4	e
g^2	g^2	g^3	g^4	e	g
g^3	g^3	g^4	e	g	g^2
g^4	g^4	e	g	g^2	g^3

.

In this case, G is isomorphic to C_5. ∎

EXERCISE 1.7 Prove Corollary 1.11.

Corollary 1.11 Let g be an element of finite order, and let $N \in \mathbb{Z}$. Then

$$g^N = e \iff N \text{ is a multiple of } |g|.$$

∎ SOLUTION Obviously, we ought to use Lemma 1.10, which says that if $g^n = e$ for some positive integer n, then $|g|$ is a divisor of n.

Fortunately, the left-to-right implication is exactly it. For the other implication, lets assume that $N = |g|m$ is a multiple of $|g|$. Then,

$$g^N = g^{|g|m} = (g^{|g|})^m = e^m = e,$$

which is our desired result. ∎

EXERCISE 1.8 ¬ Let G be a finite abelian group with exactly one element f of order 2. Prove that $\prod_{g \in G} g = f$. [4.16]

When $G = (\mathbb{Z}/p\mathbb{Z})^*$, this is essentially *Wilson's Theorem*.

∎ SOLUTION Since $g^{|g|-1} \cdot g = e$, for every $g \neq e, f$, g and g^{-1} are different elements of G. Thus we can join the pairs $g \cdot g^{-1}$ in the product $\prod_{g \in G} g$ and we're left with $e \cdot f = f$. ∎

EXERCISE 1.9 Let G be a finite group, of order n, and let m be the number of elements $g \in G$ of order exactly 2. Prove that $n - m$ is odd. Deduce that if n is even, then G necessarily contains elements of order 2.

∎ SOLUTION Note that $n - m$ counts the number of elements of G of order different than 2. Since there is only one element of order 1, which is e, it suffices to show that the number of elements of order greater than 2 is even.

As in the previous exercise, if $g \in G$ has order greater than 2, we see that g and g^{-1} are different elements of G. Thus, recalling that $(g^{-1})^{-1} = g$, we can pair g with g^{-1} for all $g \in G$ such that $|g| > 2$ and so we conclude that the number of elements of order greater than 2 is even.

By *Lagrange's theorem* (which will be proved in section 8), we know that G does not contain elements of order exactly 2 if n is odd.

Finally, if n is even, then m must be odd so that $n - m$ is also odd. Therefore, $m \geq 1$ and G necessarily contains elements of order 2. ∎

EXERCISE 1.10 Suppose the order of g is odd. What can you say about the order of g^2?

∎ SOLUTION If $|g|$ is odd, then 2 and $|g|$ are relatively prime. Thus, by Proposition 1.13,

$$|g^2| = \frac{\text{lcm}(2, |g|)}{2} = \frac{2|g|}{2} = |g|.$$

Hence g and g^2 have the same order. ∎

EXERCISE 1.11 Prove that for all g, h in a group G, $|gh| = |hg|$. (Hint: Prove that $|aga^{-1}| = |g|$ for all a, g in G.)

∎ SOLUTION Let's follow the hint. We'll prove first that $(aga^{-1})^n = e \iff g^n = e$. Observe $(aga^{-1})^n = ag^n a^{-1}$. If $g^n = e$, then $(aga^{-1})^n = aea^{-1} = e$, and if $(aga^{-1})^n = e$, then $g^n = a^{-1}ag^n a^{-1}a = a^{-1}ea = e$. Since $hg = h(gh)h^{-1}$, the result follows. ∎

EXERCISE 1.12 ▷ In the group of invertible 2×2 matrices, consider

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \; h = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}.$$

Verify that $|g| = 4$, $|h| = 3$, and $|gh| = \infty$. [§1.6]

■ SOLUTION An easy calculation shows that

$$g^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \; g^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \; g^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$

and

$$h^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \; h^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 .$$

Therefore, $|g| = 4$ and $|h| = 3$. On the other hand, it follows easily from induction that

$$(gh)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \neq I_2$$

for all integer $n \geq 1$, so $|gh| = \infty$. ■

EXERCISE 1.13 ▷ Give an example showing that $|gh|$ is not necessarily equal to $\operatorname{lcm}(|g|, |h|)$, even if g and h commute. [§1.6, 1.14]

Maybe the reader has encountered them before. They are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

■ SOLUTION As we saw in exercise 1.6, there are exactly 2 groups of order 4, one of them has 1 element of order 0, e, 1 element of order 2, f, and 2 elements of order 4, g and h. Since $gh = e$, the product gh has order 0 even though $\operatorname{lcm}(|g|, |h|) = 4$. This group is also commutative.

The reader may recognize that this group is $\mathbb{Z}/4\mathbb{Z}$, which makes this calculation a little more concrete. The elements of order 4 are $[1]_4$ and $[3]_4$. ■

EXERCISE 1.14 ▷ As a counterpoint to Exercise 1.13, prove that if g and h commute *and* $\gcd(|g|, |h|) = 1$, then $|gh| = |g||h|$. (Hint: Let $N = |gh|$; then $g^N = (h^{-1})^N$; What can you say about this element?) [§1.6, 1.15, §IV.6.15]

■ SOLUTION Following the hint, since this element is a power of g, $|g^N| = \frac{|g|}{\gcd(N,|g|)}$, and since it is also a power of h^{-1} (and $|h^{-1}| = |h|$), $|(h^{-1})^N| = \frac{|h|}{\gcd(N,|h|)}$. It follows that

$$|g| \gcd(N, |h|) = |h| \gcd(N, |g|).$$

Since $\gcd(|g|, |h|) = 1$, then $|g| \mid N$, and similarly for h, from which we conclude $|g||h| \mid N$. Moreover, $(gh)^{|g||h|} = (g^{|g|})^{|h|}(h^{|h|})^{|g|} = e$, implies $N \mid |g||h|$. Therefore $|gh| = |g||h|$. ■

EXERCISE 1.15 ¬ Let G be a commutative group, and let $g \in G$ be an element of maximal *finite* order, that is, such that if $h \in G$ has finite order, then $|h| \leq |g|$. Prove that in fact if h has finite order in G, then $|h|$ *divides* $|g|$. (Hint: Argue by contradiction. If $|h|$ is finite but it does not divide $|g|$, then there is a prime integer p such that $|g| = p^m r$, $|h| = p^n s$, with r and s relatively prime to p and $m < n$. Use Exercise 1.14 to compute the order of $g^{p^m} h^s$.) [§2.1, 4.11, IV.6.15]

■ SOLUTION Following the hint, let's compute the order of $g^{p^m} h^s$. By Proposition 1.13,

$$|g^{p^m}| = \frac{\operatorname{lcm}(p^m, p^m r)}{p^m} = \frac{p^m r}{p^m} = r$$

and

$$|h^s| = \frac{\operatorname{lcm}(s, p^n s)}{s} = \frac{p^n s}{s} = p^n .$$

Since r and p are relatively prime and G is commutative, it follows from Exercise 1.14 that

$$|g^{p^m} h^s| = |g^{p^m}||h^s| = p^n r > p^m r = |g| ,$$

which contradicts that g is of maximal finite order. Therefore, we must have that $|h|$ divides $|g|$. ■

2 EXAMPLES OF GROUPS

EXERCISE 2.1 ¬ One can associate an $n \times n$ matrix M_σ with a permutation $\sigma \in S_n$ by letting the entry at $(i, (i)\sigma)$ be 1 and letting all other entries be 0. For example, the matrix corresponding to the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \in S_3$$

would be

$$M_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} .$$

Prove that, with this notation,

$$M_{\sigma\tau} = M_\sigma M_\tau$$

for all $\sigma, \tau \in S_n$, where the product on the right is the ordinary product of matrices. [IV.4.13]

■ SOLUTION We have to show that the entry at $(i, (i)\sigma\tau)$ of $M_\sigma M_\tau$ is 1 and all other entries are 0. Writing explicitly the matrix multiplication,

$$(M_\sigma M_\tau)_{(i,(i)\sigma\tau)} = \sum_{r=1}^{n} (M_\sigma)_{(i,r)} (M_\tau)_{(r,(i)\sigma\tau)} .$$

The terms $(M_\sigma)_{(i,r)}$ on the RHS are 0 whenever $r \neq (i)\sigma$. Hence,

$$(M_\sigma M_\tau)_{(i,(i)\sigma\tau)} = (M_\sigma)_{(i,(i)\sigma)}(M_\tau)_{((i)\sigma,(i)\sigma\tau)} = 1.$$

For $k \neq i$, we have that

$$(M_\sigma M_\tau)_{(k,(i)\sigma\tau)} = \sum_{r=1}^{n} (M_\sigma)_{(k,r)}(M_\tau)_{(r,(i)\sigma\tau)} = (M_\tau)_{((k)\sigma,(i)\sigma\tau)},$$

which is 0 since $k \neq i$. The result follows. ∎

EXERCISE 2.2 ▷ Prove that if $d \leq n$, then S_n contains elements of order d. [§2.1]

∎ SOLUTION Let σ be the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & d & d+1 & \cdots & n \\ 2 & 3 & \cdots & 1 & d+1 & \cdots & n \end{pmatrix} \in S_n.$$

Then $\sigma^d = e$ and $\sigma^j \neq e$ for every $1 \leq j \leq d-1$, and we have the example we desired. ∎

EXERCISE 2.3 For every positive integer n find an element of order n in $S_{\mathbb{N}}$.

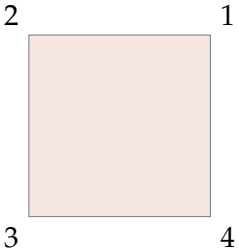
∎ SOLUTION If $n = 1$, just take the identity. If $n \geq 2$, similar to the previous exercise, let $\sigma : \mathbb{N} \to \mathbb{N}$ be the function given by

$$\sigma(x) = \begin{cases} x+1, \text{ if } x \in \{1, \ldots, n-1\}, \\ 1, \text{ if } x = n, \\ x, \text{ otherwise.} \end{cases}$$

It is clear that σ is a bijection, so $\sigma \in S_{\mathbb{N}}$. Furthermore, $\sigma^n = e$ and $\sigma^j \neq e$ for every $1 \leq j \leq n-1$, that is, $|\sigma| = n$. ∎

EXERCISE 2.4 Define a homomorphism $D_8 \to S_4$ by labeling vertices of a square, as we did for a triangle in §2.2. List the 8 permutations in the image of this homomorphism.

∎ SOLUTION Consider the following square.



Now we list the final positions of the vertices after applying each one of the elements of D_8.

D_8	S_4
Identity	$\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix}$
Rotation of 90° counterclockwise	$\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$
Rotation of 180° counterclockwise	$\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix}$
Rotation of 270° counterclockwise	$\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}$
Horizontal reflection	$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$
Vertical reflection	$\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}$
Reflection about 13	$\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}$
Reflection about 24	$\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}$

This homomorphism is clearly not an isomorphism as $|S_4| > |D_8|$. ∎

EXERCISE 2.5 ▷ Describe generators and relations for all dihedral groups D_{2n}. (Hint: Let x be the reflection about a line through the center of a regular n-gon and a vertex, and let y be the counterclockwise rotation by $2\pi/n$. The group D_{2n} will be generated by x and y, subject to three relations. To see that these relations really determine D_{2n}, use them to show that any product $x^{i_1}y^{i_2}x^{i_3}y^{i_4}\cdots$ equals x^iy^j for some i, j with $0 \le i \le 1, 0 \le j < n$.) [8.4, §IV.2.5]

∎ SOLUTION Let x and y be as in the hint. Then $x^2 = e$ and $y^n = e$. Moreover, the *conjugation* of y by x, i.e. xyx^{-1} is equal to $y^{-1} = y^{n-1}$. In fact, rotating the reflected image and the reflecting back is the same as rotating to the other direction, therefore $xy = y^{n-1}x$. Since $x^2 = e$, we have similarly $yx = xy^{n-1}$. Thus, when we have in the product $x^{i_1}y^{i_2}x^{i_3}y^{i_4}\cdots$ two consecutive terms different from 0 i_n, i_{n+1}, (suppose, without loss of generality $i_k \ge i_{k+1}$ then we can change $y^{i_k}x^{i_{k+1}}$ to $x^{i_{k+1}}y^{i_k(n-1)}$ using the last identity, and we can join every x and every y, and use the first two to conclude the final form x^iy^j for some i, j with $0 \le i \le 1, 0 \le j < n$. In particular, $|D_{2n}| = 2n$. ∎

EXERCISE 2.6 ▷ For every positive integer n construct a group containing elements g, h such that $|g| = 2$, $|h| = 2$, and $|gh| = n$. (Hint: For $n > 1$, D_{2n} will do.) [§1.6]

■ SOLUTION If $n = 1$, take any group G with an element x of order two (for example, you may take G as any dihedral group and x as any reflection) and let $g = h = x$. Suppose that $n > 1$. As suggested in the hint, we take $G = D_{2n}$. Let x be the reflection about a line through the center of a regular n-gon and a vertex, and let y be the counterclockwise rotation by $2\pi/n$. Take $g = x$ and $h = xy$. It is clear that $|g| = 2$. By the previous exercise, $xy = y^{-1}x$ so

A similar computation shows that xy^j, $0 \leq j \leq n-1$, are all reflections in D_{2n}.

$$h^2 = (xy)^2 = (xy)(xy) = (xy)(y^{-1}x) = xyy^{-1}x = xex = x^2 = e\,.$$

Thus, $|h| = 2$ too. Finally, $gh = x(xy) = x^2y = ey = y$, which is of order n, as desired. ■

EXERCISE 2.7 ¬ Find all elements of D_{2n} that commute with every other element. (The parity of n plays a role.) [IV.1.2]

As the reader will see in §IV.1.2, the *center* $Z(G)$ of a group G is the subgroup constituted by all the elements that commute with every other element.

■ SOLUTION Firstly, if $n \leq 2$ the order of D_{2n} is less than 4. Since the smallest non-abelian group is S_3, with 6 elements, every element of D_{2n} commute with every other element. In other words, $Z(D_{2n}) = D_{2n}$ for $n \leq 2$.

Now, let $n \geq 3$ and recall (Exercise 2.5) that the group D_{2n} is generated by two elements x, y such that $x^2 = e$, $y^n = e$, and $xyx^{-1} = y^{-1}$. (This means that every element of D_{2n} can be written as x^iy^j for some integers $0 \leq i \leq 1, 0 \leq j < n$.) A quick thought shows that a element $g \in D_{2n}$ is in the center if and only if it commutes with x and y. Thus, $g = x^iy^j \in D_{2n}$ is in $Z(D_{2n})$ iff

$$(x^iy^j)x = x(x^iy^j) \qquad \text{and} \qquad (x^iy^j)y = y(x^iy^j).$$

By the second equation, we have that $x^iy = yx^i$. If $i = 1$, then $y = xyx^{-1} = y^{-1}$, which would imply that the order of y is 2. This contradiction implies that $i = 0$.

By the first equation, $y^j = xy^jx^{-1}$. Since $xy^jx^{-1} = (xyx^{-1})^j = y^{-j}$, we have that $y^{2j} = e$. As the order of y is n, it follows that n divides $2j$. Knowing that $2j < 2n$, we have either $2j = n$ or $j = 0$.

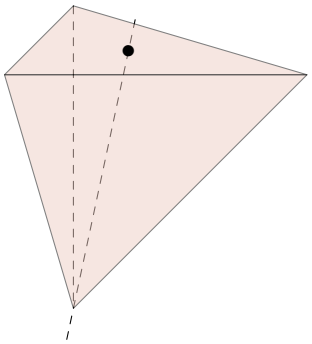
If n is even, the two options are possible and then $Z(D_{2n}) = \{e, y^{n/2}\}$. Otherwise the center is trivial: $Z(D_{2n}) = \{e\}$. ■

EXERCISE 2.8 Find the orders of the groups of symmetries of the five 'platonic solids'.

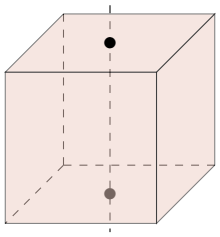
■ SOLUTION Since every symmetry is defined by an orthogonal matrix S, we will calculate these orders using linear algebra in the following way: if G is the desired group, then $\det\colon G \to \{+1, -1\}$ is a nontrivial group homomorphism. Therefore, by the first isomorphism theorem,

we can find the number of rotations R, and in the end multiply the final result by 2. By a theorem from Euler, every rotation in $\mathbb{R}^3$ is a rotation around an axis v, and since the polyhedron is invariant, there are only a finite number of possible axis: its vertices, middle points of its edges, and barycenters of the faces (where we fix the center of the polyhedron at the origin). Since every symmetry induces a permutation of the vertices, we can describe these groups as subgroups of the *symmetric groups*.

- *Tetrahedron.* Observe that the axis passing through the origin and any vertex also passes through the center of the opposite face, therefore we just have to count the axis passing through a vertex and through an edge. In the former, there are four vertex and each one gives two rotation, counting 8. In the latter, there are six edges, but each axis passes through two edges and gives only one rotation, counting 3. Finally, there is also the trivial rotation: the identity, totaling 12 rotation, from where we conclude there are 24 symmetries. Since there are 4 vertices and $|S_4| = 24$, we conclude the symmetry group of the tetrahedron is S_4.

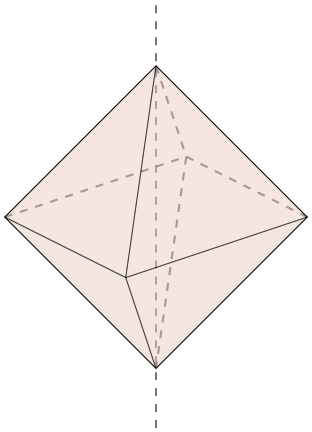


- *Cube.* It has 8 vertices and each axis passing through one, passes through the opposite vertex; further, each axis gives two rotation, counting 8 rotations. Similarly, each vertex passing through the middle point of an edge, passes also through its opposite edge, and each such axis determines only one rotation, giving 6 more rotation. Finally, each axis passing through the center of a face is counted twice and determines three rotations, giving 9 more rotations. Finally, adding up the identity, we have 24 rotations and the desired order is 48. In this case, observe the group of rotations is generated by elements x, y, z such that $x^2 = e$, $y^3 = e$ and $z^4 = e$, and, with further calculations, we conclude its rotation group is S_4 (in fact, each rotation permutes its four diagonals) and therefore its symmetry group if $S_4 \times \{+1, -1\}$.

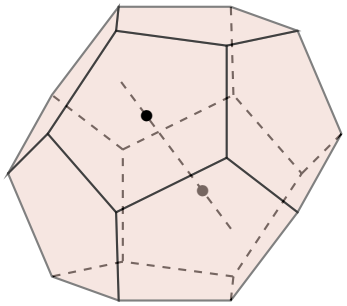


- *Octahedron.* Similarly for the octahedron, each axis is counted twice and each axis through vertex has 3 rotations, each axis through middle point of an edge has 1 rotation and each axis through a face has 2 rotations adding up to 24 with the identity, therefore the order of the symmetry group is 48. Similarly to the cube, its rotation group is S_4 and its symmetry group is $S_4 \times \{+1, -1\}$.

Since the octahedron is *dual* to the cube, it follows immediately that their symmetry groups are isomorphic.

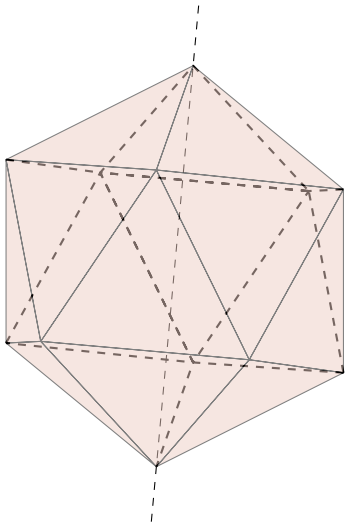


- *Dodecahedron.* Once again, each axis passing through a vertex passes through another vertex and similarly for edges and faces. In the first case, there are 2 rotations, in the second there are 1 rotation and in the third there are 4 rotations, adding up $(20 + 15 + 24 + 1) = 60$ rotations and 120 symmetries. Since now there are rotations such that $x^5 = e$, it might be natural do guess its rotation group is S_5. However this is not really the case, since $|S_5| = 120$. In fact, there are 24 5-order rotations, 20 3-order rotations and 15 2-order rotations, the same as A_5! So we might expect its rotations group is A_5 and its symmetry group is $A_5 \times \{+1, -1\}$.



- *Icosahedron.* Finally, for the dodecahedron, through each vertex passes one axis, counted twice, that has 4 rotations; through each middle point of an edge passes an axis which has 1 rotation; and through each barycenter passes an axis which has 2 rotations, adding up to $(24 + 15 + 20 + 1) = 60$ rotations and 120 symmetries. Similarly to the dodecahedron, its rotation group is A_5 and its symmetry group is $A_5 \times \{+1, -1\}$.

Since the icosahedron and the dodecahedron are dual to each other, it follows immediately their symmetry group are isometric.



■

EXERCISE 2.9 Verify carefully that 'congruence mod n' is an equivalence relation.

■ SOLUTION

- Reflexivity: Note that $n|(a - a) = 0$ because $0 = 0 \cdot n$, for all $a \in \mathbb{Z}$. Thus, $a \equiv a \bmod n$ for all $a \in \mathbb{Z}$.
- Symmetry: Let $a, b \in \mathbb{Z}$ be such that $a \equiv b \bmod n$, that is, there exists $k \in \mathbb{Z}$ such that $b - a = k \cdot n$. Therefore, $a - b = (-k) \cdot n \implies n|(a - b) \implies b \equiv a \bmod n$.
- Transitivity: Let $a, b, c \in \mathbb{Z}$ be such that $a \equiv b \bmod n$ and $b \equiv c \bmod n$. Hence, there are $k, l \in \mathbb{Z}$ such that $b - a = k \cdot n$ and

$c - b = l \cdot n$. Adding these equations, we obtain that $c - a = (b - a) + (c - b) = (k + l) \cdot n \implies n|(c - a) \implies a \equiv c \bmod n$.

We conclude that 'congruence mod n' is an equivalence relation. ∎

EXERCISE 2.10 Prove that $\mathbb{Z}/n\mathbb{Z}$ consists of precisely n elements.

∎ SOLUTION We affirm that the elements of $\mathbb{Z}/n\mathbb{Z}$ are the equivalence classes $[0]_n, [1]_n, \ldots, [n-1]_n$. They are different since $0 \leq a < b < n$ implies $0 < b - a < n$ and then n does not divide $b - a$. Also, every integer a is equivalent to some integer $r \in \{0, 1, \ldots, n-1\}$ modulo n since division with remainder implies that

$$a = qn + r$$

with $0 \leq r < n$. Modulo n we have that $[a]_n = [r]_n$. ∎

EXERCISE 2.11 ▷ Prove that the square of every odd integer is congruent to 1 modulo 8. [§VII.5.1]

∎ SOLUTION Every odd number is of the form $2n + 1$ for some $n \in \mathbb{Z}$. Therefore its square equals $(2n + 1)^2 = 4n(n + 1) + 1$. Since the product of two consecutive numbers is a multiple of 2,

$$4n(n + 1) + 1 \equiv 1 \mod 8,$$

as we desired to prove. ∎

EXERCISE 2.12 Prove that there are no nonzero integers a, b, c such that $a^2 + b^2 = 3c^2$. (Hint: By studying the equation $[a]_4^2 + [b]_4^2 = 3[c]_4^2$ in $\mathbb{Z}/4\mathbb{Z}$, show that a, b, c would all have to be even. Letting $a = 2k$, $b = 2l$, $c = 2m$, you would have $k^2 + l^2 = 3m^2$. What's wrong with that?)

The following method is known as *Method of Infinite Descent* and it is attributed to the famous lawyer and mathematician Pierre de Fermat (1607 - 1665), who often used it to solve Diophantine equations.

∎ SOLUTION Note that this equation has the integer solution $a = 0$, $b = 0$, $c = 0$. Let's prove that it does not have any other integer solution. Suppose that there are integers a, b, c, not all zero, such that $a^2 + b^2 = 3c^2$. We can assume they are all non-negative. Also, note that $c \neq 0$.

Let $\pi : \mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$ be the canonical projection to the quotient. By the definition of $+$ and $\cdot$ in $\mathbb{Z}/4\mathbb{Z}$, we know that $\pi(a + b) = \pi(a) + \pi(b)$ and $\pi(a \cdot b) = \pi(a) \cdot \pi(b)$ for all $a, b \in \mathbb{Z}$ (this means that π is a homomorphism of rings, as we shall see later). Thus, applying π on our equation we obtain $[a]_4^2 + [b]_4^2 = 3[c]_4^2$.

By Exercise 2.11, since 4 divides 8, we know that the square of any odd integer is congruent to 1 mod 4. On the other hand, any even integer is of the form $2n$ for some $n \in \mathbb{Z}$, so its square equals $4n^2$, which is congruent to 0 mod 4. Therefore, we conclude that the square of any integer is congruent to either 0 or 1 mod 4. Thus, we must have

$[a]_4^2 = [b]_4^2 = [c]_4^2 = [0]_4$ because otherwise we would get two distinct numbers of $\{0,1,2,3\}$ congruent to each other mod 4, a contradiction. For this reason, a, b and c are all even and there exist $k, l, m \in \mathbb{Z}$ such that $a = 2k$, $b = 2l$, $c = 2m$. Note that $0 < m < c$. Replacing this in our equation, we get $k^2 + l^2 = 3m^2$. By the same analysis, we get a new solution for which we can apply again this argument, obtaining another solution, and so on. However, an infinite sequence of strictly decreasing positive integers arises (the numbers appearing on the right hand-side of each equation), which is impossible to happen.

This last contradiction is a consequence of the *well-ordering principle*: every non-empty set of positive integers contains a least element.

We conclude that there cannot be an integer solution to the equation besides the trivial one. ∎

EXERCISE 2.13 ▷ Prove that if $\gcd(m,n) = 1$, then there exist integers a and b such that

$$am + bn = 1.$$

(Use Corollary 2.5.) Conversely, prove that if $am + bn = 1$ for some integers a and b, then $\gcd(m,n) = 1$. [2.15, §V.2.1, V.2.4]

Corollary 2.5 The class $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$ if and only if $\gcd(m,n) = 1$.

∎ SOLUTION By Corollary 2.5, the class $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$ and hence there exists an integer a such that $a[m]_n = [1]_n$. This means that $am - 1$ is divisible by n and thus there exists an integer $-b$ such that

$$am - 1 = -bn.$$

Conversely, if $am + bn = 1$, let $d = \gcd(m,n)$. Since $d|m$ and $d|n$, $d|(am + bn) = 1$. Hence $d = 1$. ∎

EXERCISE 2.14 State and prove an analog of Lemma 2.2, showing that the multiplication on $\mathbb{Z}/n\mathbb{Z}$ is a well-defined operation. [§2.3, §III.1.2]

Lemma 2.2 If $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then

$$(a + b) \equiv (a' + b') \mod n.$$

∎ SOLUTION The desired analogue is the following.

If $a \equiv a' \mod n$ and $b \equiv b' \mod n$, then

$$ab \equiv a'b' \mod n.$$

Its proof is also similar to that of Lemma 2.2. By hypothesis, $n \mid a - a'$ and $n \mid b - b'$, therefore

$$n \mid b(a - a') + a'(b - b') = ab - a'b',$$

and $ab \equiv a'b' \mod n$. ∎

EXERCISE 2.15 ¬ Let $n > 0$ be an odd integer.

- Prove that if $\gcd(m, n) = 1$, then $\gcd(2m + n, 2n) = 1$. (Use Exercise 2.13.)
- Prove that if $\gcd(r, 2n) = 1$, then $\gcd(\frac{r-n}{2}, n) = 1$. (Ditto.)
- Conclude that the function $[m]_n \to [2m + n]_{2n}$ is a bijection between $(\mathbb{Z}/n\mathbb{Z})^*$ and $(\mathbb{Z}/2n\mathbb{Z})^*$.

The number $\phi(n)$ of elements of $(\mathbb{Z}/n\mathbb{Z})^*$ is *Euler's ϕ-function*. The reader has just proved that if n is odd, then $\phi(2n) = \phi(n)$. Much more general formulas will be given later on (cf. Exercise V.6.8). [VII.5.11]

■ SOLUTION

- By Exercise 2.13, there are $a, b \in \mathbb{Z}$ such that that $am + bn = 1$. Since n is odd, we can assume that a is even, because if it were not, we could change a for $a + n$, which is even, and b for $b - m$, getting $(a + n)m + (b - n)m = 1$. Thus, there is a' such that $a'(2m) + bn = 1$ and we get that $a'(2m + n) + (b - a')n = 1$. Finally, since $2m + n$ is odd, as before we can replace a' by some $x \in \mathbb{Z}$ and $b - a'$ by $2y$ for some $y \in \mathbb{Z}$. Therefore, it follows that $x(2m + n) + y(2n) = 1$ and, again by Exercise 2.13, we conclude that $\gcd(2m + n, 2n) = 1$.
- Firstly, note that r is odd, so $r - n$ is even an $\frac{r-n}{2}$ is an integer. By Exercise 2.13, there exist $a, b \in \mathbb{Z}$ such that $ar + b(2n) = 1$. Thus,

$$\begin{aligned} ar + (2b)n = 1 &\implies a(r - n) + (2b + a)n = 1 \\ &\implies 2a\left(\frac{r-n}{2}\right) + (2b + a)n = 1 \end{aligned}$$

  and, again by Exercise 2.13, we have that $\gcd(\frac{r-n}{2}, n) = 1$.
- Let $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/2n\mathbb{Z})^*$ and $g : (\mathbb{Z}/2n\mathbb{Z})^* \to (\mathbb{Z}/n\mathbb{Z})^*$ be defined by

$$f([m]_n) = [2m + n]_{2n},\ g([r]_{2n}) = \left[\frac{r-n}{2}\right]_n .$$

  These functions are well-defined by the last two items and because

$$\begin{aligned} m \equiv m' \bmod n &\implies 2m \equiv 2m' \bmod 2n \\ &\implies 2m + n \equiv 2m' + n \bmod 2n \end{aligned}$$

  and

$$\begin{aligned} r \equiv r' \bmod 2n &\implies r - n \equiv r' - n \bmod 2n \\ &\implies \frac{r-n}{2} \equiv \frac{r'-n}{2} \bmod n . \end{aligned}$$

Finally, note that $fg = \mathrm{id}_{(\mathbb{Z}/2n\mathbb{Z})^*}$ and $gf = \mathrm{id}_{(\mathbb{Z}/n\mathbb{Z})^*}$ since

$$(fg)([r]_{2n}) = \left[2\left(\frac{r-n}{2}\right)+n\right]_{2n} = [r]_{2n}$$

and

$$(gf)([m]_n) = \left[\frac{(2m+n)-n}{2}\right]_n = [m]_n\,.$$

Therefore, f and g are bijections. ∎

EXERCISE 2.16 Find the last digit of $1238237^{18238456}$. (Work in $\mathbb{Z}/10\mathbb{Z}$.)

∎ SOLUTION Finding the last digit of a number amounts to finding the remainder of its division by 10. In other words, we want to find

$$1238237^{18238456} \mod 10.$$

Firstly we observe that

$$1238237^{18238456} = (1238230+7)^{18238456} \equiv 7^{18238456} \mod 10.$$

By the same reasoning, modulo 10 we have that

$$7^{18238456} = 49^{9119228} \equiv 9^{9119228} = 81^{4559614} \equiv 1^{4559614} = 1.$$

So the last digit of $1238237^{18238456}$ is 1. ∎

EXERCISE 2.17 Show that if $m \equiv m' \mod n$, then $\gcd(m,n) = 1$ if and only if $\gcd(m',n) = 1$. [§2.3]

∎ SOLUTION By Corollary 2.5,

$$\begin{aligned}\gcd(m,n) = 1 &\iff [m]_n = [m']_n \text{ generates } \mathbb{Z}/n\mathbb{Z}\\ &\iff \gcd(m',n) = 1,\end{aligned}$$

and we're done. ∎

EXERCISE 2.18 For $d \leq n$ define an injective function $\mathbb{Z}/d\mathbb{Z} \to S_n$ preserving the operation, that is, such that the sum of equivalence classes in $\mathbb{Z}/d\mathbb{Z}$ corresponds to the product of the corresponding permutations.

∎ SOLUTION Recall that $\mathbb{Z}/d\mathbb{Z}$ is cyclic and is generated by $[1]_d$, that is, any element of $\mathbb{Z}/d\mathbb{Z}$ is of the form $m \cdot [1]_d$ for some integer m. By Exercise 2.2, there exists a permutation $\sigma \in S_n$ of order d. Define $\varphi : \mathbb{Z}/d\mathbb{Z} \to S_n$ by

$$\varphi(m \cdot [1]_d) = \sigma^m$$

for all $m \cdot [1]_d \in \mathbb{Z}/d\mathbb{Z}$. Since the order of $[1]_d$ and σ are the same, this function is well-defined. It is clear that φ preserves operation. Let's prove that φ is injective. If $\sigma^m = \sigma^{m'}$, then, by Corollary 1.11:

$$\begin{aligned}\sigma^{m-m'} = e_{S_n} \implies d \mid (m-m') &\implies (m-m')\cdot[1]_d = [0]_d\\ &\implies m \cdot [1]_d = m' \cdot [1]_d\,.\end{aligned}$$

Thus, φ is injective. ∎

EXERCISE 2.19 ▷ Both $(\mathbb{Z}/5\mathbb{Z})^*$ and $(\mathbb{Z}/12\mathbb{Z})^*$ consist of 4 elements. Write their multiplication tables, and prove that no reordering of the elements will make them match.

■ SOLUTION Note that $(\mathbb{Z}/5\mathbb{Z})^* = \{[1]_5, [2]_5, [3]_5, [4]_5\}$ and $(\mathbb{Z}/12\mathbb{Z})^* = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$. Their multiplication tables are:

$\cdot$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

and

$\cdot$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[1]_{12}$	$[1]_{12}$	$[5]_{12}$	$[7]_{12}$	$[11]_{12}$
$[5]_{12}$	$[5]_{12}$	$[1]_{12}$	$[11]_{12}$	$[7]_{12}$
$[7]_{12}$	$[7]_{12}$	$[11]_{12}$	$[1]_{12}$	$[5]_{12}$
$[11]_{12}$	$[11]_{12}$	$[7]_{12}$	$[5]_{12}$	$[1]_{12}$

.

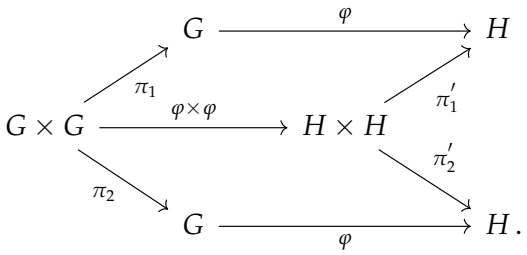
Now, observe that $[2]_5$ has order 4 while no element of $(\mathbb{Z}/12\mathbb{Z})^*$ has order bigger than 2. This implies that they are not isomorphic. ■

3 THE CATEGORY GRP

EXERCISE 3.1 ▷ Let $\varphi : G \to H$ be a morphism in a category C with products. Explain why there is a unique morphism $(\varphi \times \varphi) : G \times G \to H \times H$ compatible in the evident way with the natural projections.

(This morphism is defined explicitly for $\mathsf{C} = \mathsf{Set}$ in §3.1.) [§3.1,3.2]

■ SOLUTION Let π_1 and π_2 be the projection of $G \times G$ in the first and second coordinates, and π_1' and π_2' the projections of $H \times H$, and define $\varphi \times \varphi$ as the morphism which makes the following diagram commute.



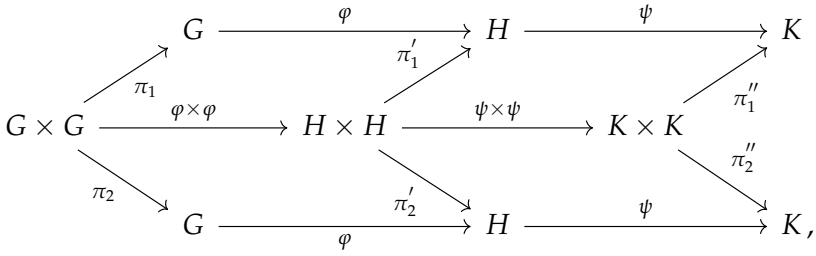
Then the existence and uniqueness follows by the universal property of the product $H \times H$. ■

EXERCISE 3.2 Let $\varphi\colon G \to H, \psi\colon H \to K$ be morphisms in a category with products, and consider morphisms between the products $G \times G, H \times H, K \times K$ as in Exercise 3.1. Prove that

$$(\psi\varphi) \times (\psi\varphi) = (\psi \times \psi)(\varphi \times \varphi).$$

(This part of the commutativity of the diagram displayed in §3.2.)

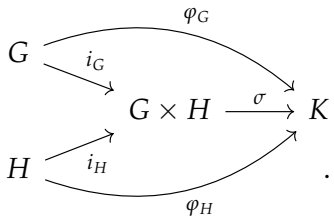
■ SOLUTION Since the following diagram commutes



we conclude $(\psi\varphi) \times (\psi\varphi) = (\psi \times \psi)(\varphi \times \varphi)$ by the uniqueness of $(\psi\varphi) \times (\psi\varphi)$. ■

EXERCISE 3.3 ▷ Show that if G, H are *abelian* groups, then $G \times H$ satisfies the universal property for coproducts in Ab (cf. §I.5.5). [§3.5, 3.6, §III.6.1]

■ SOLUTION Since we are dealing with abelian groups, the abelian notation will be used in this exercise. Let $i_G : G \to G \times H$, $i_H : H \to G \times H$ be the natural injections of G and H into $G \times H$ given by $i_G(g) = (g, 0_H)$ and $i_H(h) = (0_G, h)$ for all $g \in G, h \in H$. It is clear that they are both homomorphisms. Let K be an abelian group and $\varphi_G : G \to K$, $\varphi_H : H \to K$ be homomorphisms. We need to show that there exists a unique homomorphism $\sigma : G \times H \to K$ such that the following diagram commutes:



If a homomorphism σ makes this diagram commute, it is necessarily unique because we have

$$\begin{aligned}\sigma(g,h) &= \sigma((g,0_H) + (0_G,h)) \\ &= \sigma(g,0_H) + \sigma(0_G,h) \\ &= (\sigma i_G)(g) + (\sigma i_H)(h) \\ &= \varphi_G(g) + \varphi_H(h)\end{aligned}$$

for all $(g,h) \in G \times H$. Define the set-function $\sigma : G \times H \to K$ by $\sigma(g,h) = \varphi_G(g) + \varphi_H(h)$, as suggested by the computation above.

Since $\varphi_G(0_G) = \varphi_H(0_H) = 0_K$, the diagram commutes. It remains to show that σ is a homomorphism. Indeed, if (g_1, h_1), $(g_2, h_2) \in G \times H$ then

$$\begin{aligned}\sigma((g_1,h_1)+(g_2,h_2)) &= \sigma(g_1+g_2, h_1+h_2)\\ &= \varphi_G(g_1+g_2)+\varphi_H(h_1+h_2)\\ &= \varphi_G(g_1)+\varphi_G(g_2)+\varphi_H(h_1)+\varphi_H(h_2)\\ &= (\varphi_G(g_1)+\varphi_H(h_1))+(\varphi_G(g_2)+\varphi_H(h_2))\\ &= \sigma(g_1,h_1)+\sigma(g_2,h_2)\end{aligned}$$

since φ_G and φ_H are homomorphisms and K is abelian. Therefore $G \times H$ with i_G and i_H satifies the universal property for coproducts in Ab. ∎

EXERCISE 3.4 Let G, H be groups, and assume that $G \cong H \times G$. Can you conclude that H is trivial? (Hint: No. Can you construct a counterexample?)

∎ SOLUTION It suffices to take H to be any non-trivial group and G to be an infinite product of the H's. ∎

EXERCISE 3.5 Prove that $\mathbb{Q}$ is not the direct product of two nontrivial groups.

∎ SOLUTION Note that, if $r_1, r_2 \in \mathbb{Q}$, then there exists $p, q \in \mathbb{Z}$ such that $pr_1 = qr_2 \neq 0$, and this property is shared by all of its isomorphic group. However, if G and H are nontrivial, $g \neq 0_G \in G$ and $h \neq 0_H \in H$, and $p, q \in \mathbb{Z}$ are such that $p(g, 0_H) = q(0_G, h)$, then they are equal to $(0_G, 0_H)$. Therefore, no product is isomorphic to $\mathbb{Q}$. ∎

EXERCISE 3.6 ▷ Consider the product of the cyclic groups C_2, C_3 (cf. §2.3): $C_2 \times C_3$. By Exercise 3.3, this group is a coproduct of C_2 and C_3 in Ab. Show that it is *not* a coproduct of C_2 and C_3 in Grp, as follows:

- find injective homomorphisms $C_2 \to S_3$, $C_3 \to S_3$;
- arguing by contradiction, assume that $C_2 \times C_3$ is a coproduct of C_2, C_3, and deduce that there would be a group homomorphism $C_2 \times C_3 \to S_3$ with certain properties;
- show that there is no such homomorphism.

[§3.5]

∎ SOLUTION Let $\sigma_x, \sigma_y \in S_3$ be the permutations:

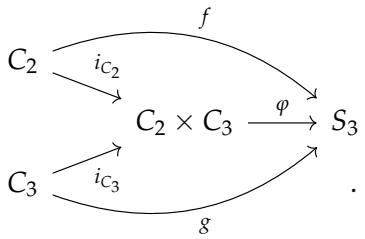
$$\sigma_x = \begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}, \quad \sigma_y = \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}.$$

If x and y are the generators of C_2 and C_3, respectively, define $f : C_2 \to S_3$ and $g : C_3 \to S_3$ by

$$f(x^n) = \sigma_x^n,\ g(y^n) = \sigma_y^n$$

for all $n \in \mathbb{Z}$. Since $|\sigma_x| = 2$ and $|\sigma_y| = 3$, these functions are well-defined. They are clearly injective homomorphisms.

Assume that $C_2 \times C_3$ is a coproduct of C_2 and C_3 in Grp. Then, there exists a unique homomorphism $\varphi : C_2 \times C_3 \to S_3$ such that diagram



commutes, where i_{C_2}, i_{C_3} are the natural injections into the product, as in Exercise 3.3. We can see that

$$\begin{aligned}\varphi(a,b) &= \varphi((a,e_{C_3}) \cdot (e_{C_2},b)) \\ &= \varphi(a,e_{C_3}) \cdot \varphi(e_{C_2},b) \\ &= (\varphi i_{C_2})(a) \cdot (\varphi i_{C_3})(b) \\ &= f(a) \cdot g(b)\end{aligned}$$

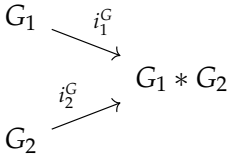
for all $(a,b) \in C_2 \times C_3$. From this result, it can be easily checked that φ is surjective. Since $|C_2 \times C_3| = |S_3| = 6$, it is indeed a bijection and, thus, $C_2 \times C_3$ and S_3 are isomorphic. But this is a contradiction because $C_2 \times C_3$ is abelian and S_3 is not. Therefore, we conclude that $C_2 \times C_3$ with i_{C_2} and i_{C_3} is not a coproduct of C_2 and C_3 in Grp. ∎

EXERCISE 3.7 Show that there is a *surjective* homomorphism $\mathbb{Z} * \mathbb{Z} \to C_2 * C_3$. ($*$ denotes coproduct in Grp; cf. §3.4.)

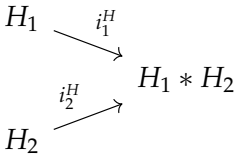
One can think of $\mathbb{Z} * \mathbb{Z}$ as a group with two generators x, y, subject to no relations whatsoever. (We will study a general version of such groups in §5; see Exercise 5.6.)

∎ SOLUTION Actually, something way more general is true: let $\varphi_1 : G_1 \to H_1$ and $\varphi_2 : G_2 \to H_2$ be surjective group homomorphisms. Then there exists a surjective homomorphism $G_1 * G_2 \to H_1 * H_2$.

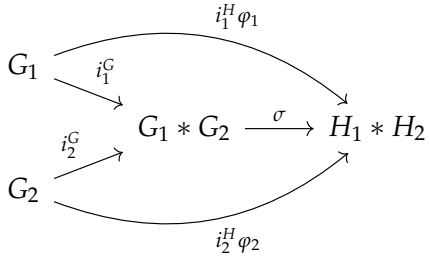
Let



be the canonical injections of $G_1 * G_2$ and



be those of $H_1 * H_2$. Then the universal property of $G_1 * G_2$ implies that there exists a unique morphism $\sigma : G_1 * G_2 \to H_1 * H_2$ such that the diagram



commutes.

Now, I can only imagine two (strange) ways of proving that σ is surjective. The first one is by utilizing the description of $C_2 * C_3$ given in the next exercise (and then we write σ explicitly just as done in this exercise). The next one is by knowing that the coproduct of two epimorphisms is also an epimorphism (in any category) and that, in Grp, epimorphisms are surjective, both results that Aluffi didn't enunciate. ∎

Remark. These characterizations of $\mathbb{Z} * \mathbb{Z}$ and $C_2 * C_3$ become 'obvious' when the reader knows about free products. Just as in the explicit construction of free groups done in §5.3, the elements of $G * H$ are words of the form

$$g_1 h_1 g_2 h_2 \dots g_k h_k.$$

The product in $G * H$ is analogous to the one in free groups. It is constituted by concatenation and reduction of words.

Knowing this we can prove the general result stated in the solution. Denoting by g_n the elements of G_1 and by h_n the elements of G_2 we have that the image of $g_1 h_1 g_2 h_2 \dots g_k h_k$ by σ is simply

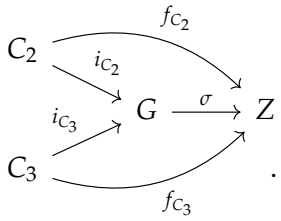
$$\varphi_1(g_1)\varphi_2(h_1)\varphi_1(g_2)\varphi_2(h_2)\dots\varphi_1(g_k)\varphi_2(h_k).$$

This shows that σ is clearly surjective.

EXERCISE 3.8 ▷ Define a group G with two generators x, y, subject (only) to the relations $x^2 = e_G$, $y^3 = e_G$. Prove that G is a coproduct of C_2 and C_3 *in* Grp. (The reader will obtain even more concrete

description for $C_2 * C_3$ in Exercise 9.14; it is called the *modular group*.) [§3.4, 9.14]

■ SOLUTION Let $i_{C_2} : C_2 \to G$ be defined by $i_{C_2}(m) = x^m$ and $i_{C_3} : C_3 \to G$ be defined by $i_{C_3}(m) = y^m$. Then (G, i_{C_2}, i_{C_3}) is a coproduct of C_2 and C_3 in Grp. In fact, let Z be a group and $f_{C_2} : C_2 \to Z$ and $f_{C_3} : C_3 \to Z$ be two homomorphism, and σ a morphism from $C_2 * C_3$ to Z.



Since we have a commuting diagram: $\sigma(x^m) = f_{C_2}(m)$ and $\sigma(y^m) = f_{C_3}(m)$. Since x and y generates G, we can define σ by

$$\sigma(x^{i_1}y^{i_2}x^{i_3}y^{i_4}\cdots) = f_{C_2}(i_1)f_{C_3}(i_2)f_{C_2}(i_3)f_{C_3}(i_4)\cdots$$

and we ensure its existence. On the other hand, this σ is unique since any such morphism must satisfy this identity. ■

EXERCISE 3.9 Show that *fiber* products and coproducts exist in Ab. (Cf. Exercise I.5.12. For coproducts, you may have to wait until you know about *quotients*.)

■ SOLUTION In this exercise, we will use the abelian notation. Let G, H, K be abelian groups and $\alpha : G \to K$, $\beta : H \to K$ be homomorphisms. We will show that the fibered product of α and β is the same one as in Set (see Exercise I.5.12); we just need to introduce an operation. Define

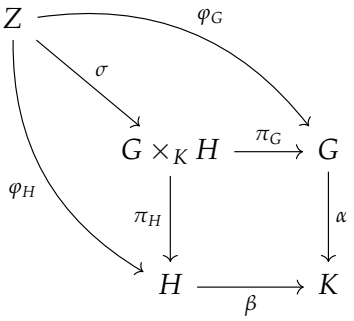
$$G \times_K H = \bigcup_{x \in K} \alpha^{-1}(x) \times \beta^{-1}(x)$$

and consider the usual projections π_G and π_H. We claim that the operation

$$(g_1, h_1) + (g_2, h_2) := (g_1 + g_2, h_1 + h_2)$$

turns $G \times_K H$ into a group. Firstly, note that it is well-defined because α and β are homomorphisms; if $(g_1, h_1), (g_2, h_2) \in G \times_K H$, there are $x, y \in K$ such that $\alpha(g_1) = \beta(h_1) = x$ and $\alpha(g_2) = \beta(h_2) = y$, so $\alpha(g_1 + g_2) = \beta(h_1 + h_2) = x + y \in K$, which implies that $(g_1 + g_2, h_1 + h_2) \in G \times_K H$. It is easy to check that this operation is associative and commutative, $(0_G, 0_H) \in G \times_K H$ is the zero element and $(-g, -h) \in G \times_K H$ is the opposite of $(g, h) \in G \times_K H$. (It is essential to verify that these elements are in $G \times_K H$, which indeed happens because α and β are homomorphisms.) Note that π_G and π_H are homomorphisms and that $\alpha\pi_G = \beta\pi_H$.

Let Z be an abelian group and $\varphi_G : Z \to G$, $\varphi_H : Z \to H$ be homomorphisms such that $\alpha\varphi_G = \beta\varphi_H$. We need to show that there exists a unique $\sigma : Z \to G \times_K H$ such that the diagram



Notice that we did not use that the groups were abelian, so this is also the fibered product in Grp.

commutes. As in Exercise I.5.12, we are forced to define $\sigma(z) = (\varphi_G(z), \varphi_H(z))$ for all $z \in Z$. By doing so, σ is an homomorphism and it is well-defined because $\alpha\varphi_G = \beta\varphi_H$. Therefore, $G \times_K H$ with π_G and π_H is the desired fibered product.

Now, for the fibered coproduct, we set $\alpha : K \to G$ and $\beta : K \to H$ as homomorphisms. As we will see, the fibered coproduct in Ab is similar to the one in Set. Let $i_G^* : G \to G \times H$, $i_H^* : H \to G \times H$ be the natural injections of G and H into $G \times H$ given by $i_G^*(g) = (g, 0_H)$ and $i_H^*(h) = (0_G, h)$ for all $g \in G, h \in H$. Let $N \subseteq G \times H$ be the subgroup generated by the elements of the form

$$(i_G^* \circ \alpha)(x) \cdot ((i_H^* \circ \beta)(x))^{-1}$$

for all $x \in K$. Since $G \times K$ is abelian, we can take the quotient $(G \times K)/N$. Thus, define

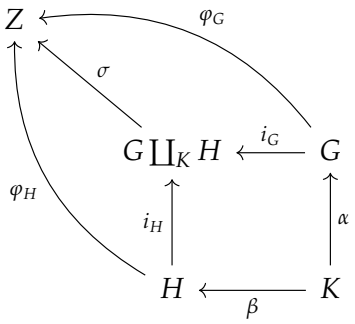
$$G \coprod_K H = (G \times H)/N$$

and, if π is the canonical projection to the quotient, define $i_G = \pi i_G^*$ and $i_H = \pi i_H^*$. Note that $i_G\alpha = i_H\beta$ by the definition of N.

Let Z be another abelian group together with homomorphisms $\varphi_G : G \to Z$, $\varphi_H : H \to Z$ such that $\varphi_G\alpha = \varphi_H\beta$. By Exercise 3.3, there exists a unique $\varphi : G \times H \to Z$ such that $\varphi_G = \varphi i_G^*$ and $\varphi_H = \varphi i_H^*$. Let's show that $N \subseteq \ker \varphi$. Since N is generated by the elements of the form given above, it suffices to show that they are in this kernel. Since $\varphi_G\alpha = \varphi_H\beta$,

$$\begin{aligned}
\varphi((i_G^*\alpha)(x) \cdot ((i_H^*\beta)(x))^{-1}) &= ((\varphi i_G^*)\alpha)(x) \cdot (((\varphi i_H^*)\beta)(x))^{-1} \\
&= (\varphi_G\alpha)(x) \cdot ((\varphi_H\beta)(x))^{-1} \\
&= e_Z
\end{aligned}$$

for all $x \in K$, and it follows that $N \subseteq \ker \varphi$. By Theorem 7.12, there exists a unique $\sigma : G \coprod_K H \to Z$ such that $\varphi = \sigma\pi$. Hence, the diagram



commutes because

$$\sigma i_G = \sigma(\pi i_G^*) = (\sigma\pi) i_G^* = \varphi i_G^* = \varphi_G$$

and, similarly, $\sigma i_H = \varphi_H$. Finally, suppose that there exists another $\rho : G \coprod_K H \to Z$ such that the diagram above commutes. Since $\varphi_G = \rho i_G = (\rho\pi) i_G^*$ and $\varphi_H = \rho i_H = (\rho\pi) i_H^*$, the uniqueness of φ and σ implies that $\varphi = \rho\pi$ and so $\rho = \sigma$. Therefore, σ is the only homomorphism such that the diagram above commutes. We conclude that $G \coprod_K H$ with i_G and i_H is the desired fibered coproduct. ∎

4 GROUP HOMOMORPHISMS

EXERCISE 4.1 ▷ Check that the function π_m^n defined in §4.1 is well-defined and makes the diagram commute. Verify that it is a group homomorphism. Why is the hypothesis $m|n$ necessary? [§4.1]

∎ SOLUTION The function $\pi_m^n := [a]_n \mapsto [a]_m$ is well-defined because $[a]_n \subset [a]_m$; indeed, $x \in [a]_n \implies n|x-a \Rightarrow m|x-a\ (m|n) \Rightarrow x \in [a]_m$. This implies immediately that $x, y \in [a]_n \Rightarrow [x]_n \cap [y]_n \neq \emptyset$ (because a is in that intersection) $\Rightarrow [x]_n = [y]_n \Rightarrow [x]_m \cap [y]_m \neq \emptyset$ (because $[x]_n$ is contained in both) $\Rightarrow [x]_m = [y]_m$.

In that last sequence of steps we used the fact that $m|n$, and the proposition becomes false if $m \nmid n$; in that case $[0]_n = [n]_n$ but we don't have $[0]_m = [n]_m$ because $m \nmid n - 0 = n$, so there is no unique choice for $\pi_m^n([0]_n)$.

Now, clearly $\pi_n \circ \pi_m^n$ takes $a \mapsto [a]_n \mapsto [a]_m$ and so $\pi_n \circ \pi_m^n = \pi_m$. We conclude that the diagram commutes.

We now just have to check that π_m^n is a group homomorphism. Indeed, $\pi_m^n([a]_n + [b]_n) = \pi_m^n([a+b]_n) = [a+b]_m = [a]_m + [b]_m$. ∎

EXERCISE 4.2 Show that the homomorphism $\pi_2^4 \times \pi_2^4 \colon C_4 \to C_2 \times C_2$ is *not* an isomorphism. In fact, is there *any* isomorphism $C_4 \to C_2 \times C_2$?

■ SOLUTION Since we're taking the product of two equal functions, its product is subset of the diagonal $\{(n,n) \mid n \in C_2\}$, and the function is not surjective. The element $1 \in C_4$ has order 4, but there is no element in $C_2 \times C_2$ with order 4, therefore there does not exist such an isomorphism. ■

EXERCISE 4.3 ▷ Prove that a group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ if and only if it contains an element of order n. [§4.3]

■ SOLUTION Let G be such group. The proof will be divided into two steps.

($\Longrightarrow$) Since $[1]_n \in \mathbb{Z}/n\mathbb{Z}$ is of order n and $G \cong \mathbb{Z}/n\mathbb{Z}$, it follows from Proposition 4.8 that G contains an element of order n.

($\Longleftarrow$) Let x be an element of order n in G. Define $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ by

$$\varphi([m]_n) = x^m$$

for all $[m]_n \in \mathbb{Z}/n\mathbb{Z}$. Since $|x| = n$, φ is well-defined (see Corollary 1.11) and is clearly a homomorphism. We claim that φ is injective. Indeed, if $\varphi([m]_n) = \varphi([m']_n)$ then, again by Corollary 1.11,

$$x^m = x^{m'} \implies x^{m-m'} = e_G \implies n|(m-m') \implies [m]_n = [m']_n,$$

as desired. By the Pigeonhole Principle, since $|G| = |\mathbb{Z}/n\mathbb{Z}| = n$, φ is also surjective and, therefore, it is an isomorphism. ■

The Pigeonhole Principle states that, if X, Y are finite sets and $|X| > |Y|$, then any function from X to Y cannot be injective.

EXERCISE 4.4 Prove that no two of the groups $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ are isomorphic to one another. Can you decide whether $(\mathbb{R},+)$, $(\mathbb{C},+)$ are isomorphic to one another? (Cf. Exercise VI.1.1.)

■ SOLUTION Since $\mathbb{R}$ is uncountable, there does not exist a bijection from $\mathbb{Z}$ or $\mathbb{Q}$ to $\mathbb{R}$. Moreover, if $\varphi\colon \mathbb{Q} \to \mathbb{Z}$ is an homomorphism, then, given $r \in \mathbb{Q}$, for each $n \in \mathbb{N}$, we have that $n \mid \phi(r)$, for

$$\varphi(r) = \varphi\underbrace{\left(\frac{r}{n} + \cdots + \frac{r}{n}\right)}_{n \text{ times}} = n\varphi\left(\frac{r}{n}\right).$$

But this implies $\varphi(r) = 0$, and φ is the trivial homomorphism.

■

EXERCISE 4.5 Prove that the groups $(\mathbb{R}\backslash\{0\},\cdot)$ and $(\mathbb{C}\backslash\{0\},\cdot)$ are not isomorphic.

■ SOLUTION The element $i \in \mathbb{C}$ has order 4, but there is no element in $\mathbb{R}\backslash\{0\}$ with order 4. Therefore there cannot be an isomorphism between these two groups. ■

EXERCISE 4.6 We have seen that $(\mathbb{R}, +)$ and $(\mathbb{R}^{>0}, \cdot)$ are isomorphic (Example 4.4). Are the groups $(\mathbb{Q}, +)$ and $(\mathbb{Q}^{>0}, \cdot)$ isomorphic?

■ SOLUTION Suppose that there exists an isomorphism $\varphi : (\mathbb{Q}, +) \to (\mathbb{Q}^{>0}, \cdot)$. Thus, there exists $r \in \mathbb{Q}$ such that $\varphi(r) = 2$, but then

$$\varphi\left(\frac{r}{2}\right)^2 = \varphi\left(2 \cdot \frac{r}{2}\right) = \varphi(r) = 2,$$

which implies that $\sqrt{2}$ is rational, a contradiction. We conclude that $(\mathbb{Q}, +)$ and $(\mathbb{Q}^{>0}, \cdot)$ are not isomorphic. ■

Remark. Even stronger, we can show that the only homomorphism f from $(\mathbb{Q}, +)$ to $(\mathbb{Q}^{>0}, \cdot)$ is the trivial one. Note that, if $f(1) = 1$, we automatically have that $f(r) = f(1)^r = 1$ for all $r \in \mathbb{Q}$. Suppose that $f(1) \neq 1$ and write $f(1) = \frac{a}{b}$ where a and b are positive integers such that $\gcd(a, b) = 1$. Let $k \in \mathbb{N}$ be such that $a, b < 2^k$. We claim that $f(1)$ is not of the form $f(1) = r^n$ for a rational number r, for every $n > k$. In fact, suppose $f(1) = r^n$ and write $r = \frac{c}{d}$ where c and d are positive integers such that $\gcd(c, d) = 1$. This implies that $ad^n = bc^n$ and, by the gcd conditions, we get that $a = c^n$ and $b = d^n$. But then we must have $c = d = 1$ because otherwise we would get $a > 2^k$ or $b > 2^k$. It follows that $a = b = 1$ and $f(1) = 1$, a contradiction. Therefore, $f(1) \neq r^n$ for all $r \in \mathbb{Q}$ and $n > k$. However, $f(1) = f(\frac{1}{k+1})^{k+1}$, which is impossible. Thus we must have $f(1) = 1$ and f is the trivial homomorphism.

We can also prove this result using the *rational root theorem*, which states that, if $x = \frac{p}{q} \in \mathbb{Q}$ is such that

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 = 0$$

for some $a_0, \ldots, a_n \in \mathbb{Z}$ and $\gcd(p, q) = 1$, then p divides a_0 and q divides a_n. Let $f : (\mathbb{Q}, +) \to (\mathbb{Q}^{>0}, \cdot)$ be a homomorphism and write $f(1) = \frac{a}{b}$ where $\gcd(a.b) = 1$. Since $f(1) = f(\frac{1}{n})^n$, the equation $bx^n - a = 0$ has solutions for all $n \in \mathbb{N}$. If $f(1) \neq 1$, all these solutions would be different, by order constraints. However, the rational root theorem implies that there can only be a finite number of such solutions, a contradiction. Therefore, $f(1) = 1$ and f is the trivial homomorphism.

EXERCISE 4.7 Let G be a group. Prove that the function $G \to G$ defined by $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian. Prove that $g \mapsto g^2$ is a homomorphism if and only if G is abelian.

■ SOLUTION The first function is a homomorphism if and only if $g^{-1}h^{-1} = (gh)^{-1}$ for all $g, h \in G$. This means that $g^{-1}h^{-1} = h^{-1}g^{-1}$. It is clear that this equation holds if G is abelian. Conversely, since

every element is the inverse of someone, this equation implies that G is abelian.

For the second function, supposing that it is a homomorphism, we have that $g^2h^2 = ghgh$ for all $g, h \in G$. Multiplying by g^{-1} on the left and by h^{-1} it follows that that G is abelian. The converse is obvious. ∎

EXERCISE 4.8 ¬ Let G be a group, and let $g \in G$. Prove that the functions $\gamma_g \colon G \to G$ defined by $(\forall a \in G) \colon \gamma_g(a) = gag^{-1}$ is an automorphism of G. (The automorphisms γ_g are called 'inner' automorphisms of G.) Prove that the function $G \to \mathrm{Aut}(G)$ defined by $g \mapsto \gamma_g$ is an homomorphism. Prove that the homomorphism is trivial if and only if G is abelian. [6.7, 7.11, IV.1.5]

∎ SOLUTION It is easy to see γ_g is an homomorphism. In fact, for any $a, b \in G$,

$$\begin{aligned}\gamma_g(a)\gamma_g(b) &= (gag^{-1})(gbg^{-1}) \\ &= g(ab)g^{-1} \\ &= \gamma_g(ab),\end{aligned}$$

and its inverse is also easy to find:

$$\begin{aligned}\gamma_{g^{-1}} \circ \gamma_g(a) &= \gamma_{g^{-1}}(gag^{-1}) \\ &= g^{-1}(gag^{-1})g \\ &= a,\end{aligned}$$

and similarly for $\gamma_g \circ \gamma_{g^{-1}}$. Therefore γ_g is an automorphism.

Moreover, this final calculation indicates that $g \to \gamma_g$ *might* be an homomorphism. In fact, given $g, h \in G$, for any $a \in G$

$$\begin{aligned}\gamma_g \circ \gamma_h(a) &= \gamma_g(hah^{-1}) \\ &= g(hah^{-1})g^{-1} \\ &= (gh)a(gh)^{-1} \\ &= \gamma_{gh}(a).\end{aligned}$$

Thus it is an homomorphism.

Finally, this homomorphism is trivial if and only if $(\forall g, a \in G) : gag^{-1} = a$, i.e., $ga = ag$, which means G is abelian. ∎

EXERCISE 4.9 ▷ Prove that if m, n are positive integers such that $\gcd(m, n) = 1$, then $C_{mn} \cong C_m \times C_n$. [§4.3, 4.10, §IV.6.1, V.6.8]

∎ SOLUTION We will prove that $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, which is equivalent to the exercise. By Exercise 4.1, we can define the homomorphism $\varphi : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ by $\varphi = \pi_m^{mn} \times \pi_n^{mn}$. Explicitly,

$$\varphi([x]_{mn}) = ([x]_m, [x]_n)$$

for all $[x]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$. We claim that φ is injective. Indeed, suppose that $\varphi([x]_{mn}) = \varphi([y]_{mn})$ for some $[x]_{mn}, [y]_{mn} \in \mathbb{Z}/mn\mathbb{Z}$. It follows that $x \equiv y \bmod m$ and $x \equiv y \bmod n$, thus, there are $m', n' \in \mathbb{Z}$ such that $y - x = mm' = nn'$. By Exercise 2.13, there are $a, b \in \mathbb{Z}$ such that $am + bn = 1$. Multiplying this equation by $y - x$, we get that

$$\begin{aligned} am(y-x) + bn(y-x) = y - x &\implies amnn' + bnmm' = y - x \\ &\implies (mn)(an' + bm') = y - x \\ &\implies mn|(y-x) \\ &\implies [x]_{mn} = [y]_{mn}, \end{aligned}$$

as desired. Finally, since $|\mathbb{Z}/mn\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}| = mn$, we conclude that φ is also surjective. Therefore, φ is an isomorphism and $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. ∎

Remark. This result is a particular case of the *Chinese remainder theorem*, which states: if $n_1, \ldots, n_k$ are integers such that $\gcd(n_i, n_j) = 1$ when $i \neq j$, then, for any $a_1, \ldots, a_k \in \mathbb{Z}$, there exists an integer x such that

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ &\vdots \\ x &\equiv a_n \bmod n_k \end{aligned}$$

and any two such x are congruent mod $n_1 n_2 \cdots n_k$. For $k = 2$, we proved that x exists when we showed that φ is surjective. The injectivity of φ implies the uniqueness of x mod mn.

This result can be generalized to arbitrary *rings*, which will be presented in chapter III. Let R be a ring and let $I_1, \ldots, I_k$ be two-sided coprime ideals, that is, $I_i + I_j = R$, if $i \neq j$. Then,

$$R/I \cong R/I_1 \times \cdots \times R/I_k$$

where I is the intersection of $I_1, \ldots, I_k$. Moreover, if R is commutative, I equals to the product of these ideals.

EXERCISE 4.10 ▷ Let $p \neq q$ be odd prime integers; show that $(\mathbb{Z}/pq\mathbb{Z})^*$ is not cyclic. (Hint: Use Exercise 4.9 to compute the order N of $(\mathbb{Z}/pq\mathbb{Z})^*$, and show that no element can have order N.) [§4.3]

∎ SOLUTION We first observe that $[x]_{pq} \in \mathbb{Z}/pq\mathbb{Z}$ satisfies $gcd(x, pq) = 1$ if and only if $gcd(x, p) = 1 = gcd(x, q)$ (that happens because $gcd(p, q) = 1$). This means that $[x]_{pq} \in (\mathbb{Z}/pq\mathbb{Z})^* \Leftrightarrow [x]_p \in (\mathbb{Z}/p\mathbb{Z})^*$ and $[x]_q \in (\mathbb{Z}/q\mathbb{Z})^*$, and we conclude, by the remark at the end of the solution to exercise 4.9, that $|\mathbb{Z}/pq\mathbb{Z}| = (p-1)(q-1)$. (Indeed, any two pairs of residues in $(\mathbb{Z}/p\mathbb{Z})^*$ and $(\mathbb{Z}/q\mathbb{Z})^*$ determine uniquely and reversibly a residue in $(\mathbb{Z}/p\mathbb{Z})^*$)

For clarity, we will use $Ord_n(x)$ as a replacement for the order of $[x]_n$ in $(\mathbb{Z}/n\mathbb{Z})^*$. This is to avoid ambiguity when talking about order of the same element in different groups.

Now, we will prove that $Ord_{pq}(x) = lcm(Ord_p(x), Ord_q(x))$. Indeed, if $Ord_p(x), Ord_q(x)|T$, then $[x^T]_p = [1]_p$ and $[x^T]_q = [1]_q$, which implies $[x^T]_{pq} = [1]_{pq}$. In the same fashion, we obtain that if $[x^T]_{pq} = [1]_{pq}$ then $[x^T]_p = [1]_p$ and $[x^T]_q = [1]_q$, by Corollary 1.11, and we conclude $Ord_p(x), Ord_q(x)|T$.

Now, as was pointed below Definition 1.12, $|g| \leq |G|$ and so it is impossible to have $lcm(Ord_p(x), Ord_q(x)) = (p-1)(q-1)$; indeed $lcm(x,y) \leq xy$ and so we would have, for a generating element $[x]_{pq}$, $(p-1)(q-1) = Ord_{pq}(x) = lcm(Ord_p(x), Ord_q(x)) \leq Ord_p(x)Ord_q(x) \leq (p-1)(q-1)$; equality must hold, but both $p-1$ and $q-1$ are even, therefore $lcm(p-1, q-1) \leq (p-1)(q-1)/2$, a contradiction.

We have shown that no element of $(\mathbb{Z}/pq\mathbb{Z})^*$ has the full order of the group, and so we conclude that it is not cyclic, as desired. ∎

Remark. This question admits a natural generalization, that is to ask for which n can the resulting group $(\mathbb{Z}/n\mathbb{Z})^*$ be cyclic. In the next problem (exercise 4.11) we will show that it is indeed cyclic for p prime, and it turns out to be cyclic for $n = p^\alpha$ or $n = 2p^\alpha$, and not cyclic in any other case. While the affirmative answers take a bit more tools to develop, the negative answers are not conceptually harder than the solution above, and so we include them for completeness.

We start with a simple lemma: if $(\mathbb{Z}/ab\mathbb{Z})^*$ is cyclic then so is $(\mathbb{Z}/a\mathbb{Z})^*$. Indeed, the projection pi_a^{ab} sends a generator of $(\mathbb{Z}/ab\mathbb{Z})^*$ into an element whose

EXERCISE 4.11 ▷ In due time we will prove the easy fact that if p is a prime integer, then the equation $x^d = 1$ can have at most d solutions in $\mathbb{Z}/p\mathbb{Z}$. Assume this fact, and prove that the multiplicative group $G = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. (Hint: Let $g \in G$ be an element of maximal order; use Exercise 1.15 to show that $h^{|g|} = 1$ for all $h \in G$. Therefore...) [§4.3, 4.15, 4.16, §IV.6.3]

∎ SOLUTION Let $g \in G$ be as above. Then, by Exercise 1.15, $h^{|g|} = 1$ for every $h \in G$. Since this equation ($x^{|g|} = 1$) has $|G|$ solutions, this implies $|G| \leq |g|$. On the other hand, as was pointed out below Definition 1.12, $|g| \leq |G|$. Therefore $|g| = |G|$, and g generates G. ∎

EXERCISE 4.12 ¬

- Compute the order of $[9]_{31}$ in the group $(\mathbb{Z}/31\mathbb{Z})^*$.

- Does the equation $x^3 - 9 = 0$ have solutions in $\mathbb{Z}/31\mathbb{Z}$? (Hint: Plugging in all 31 elements of $\mathbb{Z}/31\mathbb{Z}$ is too laborious and will not teach you much. Instead, use the result of the first part: if c is a solution of the equation, what can you say about $|c|$?) [VII.5.15]

■ SOLUTION

- We need to compute the powers of 9 mod 31:

$$
\begin{aligned}
&9 \not\equiv 1 \mod 31\\
&9^2 = 81 \equiv 19 \not\equiv 1 \mod 31\\
&9^3 \equiv 19 \cdot 9 = 171 \equiv 16 \not\equiv 1 \mod 31\\
&9^4 \equiv 16 \cdot 9 = 144 \equiv -11 \not\equiv 1 \mod 31\\
&9^5 \equiv (-11) \cdot 9 = -99 \equiv -6 \not\equiv 1 \mod 31\\
&9^6 \equiv (-6) \cdot 9 = -54 \equiv 8 \not\equiv 1 \mod 31\\
&9^7 \equiv 8 \cdot 9 = 72 \equiv 10 \not\equiv 1 \mod 31\\
&9^8 \equiv 10 \cdot 9 = 90 \equiv -3 \not\equiv 1 \mod 31\\
&9^9 \equiv (-3) \cdot 9 = -27 \equiv 4 \not\equiv 1 \mod 31\\
&9^{10} \equiv 4 \cdot 9 = 36 \equiv 5 \not\equiv 1 \mod 31\\
&9^{11} \equiv 5 \cdot 9 = 45 \equiv 14 \not\equiv 1 \mod 31\\
&9^{12} \equiv 14 \cdot 9 = 126 \equiv 2 \not\equiv 1 \mod 31\\
&9^{13} \equiv 2 \cdot 9 = 18 \not\equiv 1 \mod 31\\
&9^{14} \equiv 18 \cdot 9 = 162 \equiv 7 \not\equiv 1 \mod 31\\
&9^{15} \equiv 7 \cdot 9 = 63 \equiv 1 \mod 31.
\end{aligned}
$$

  Therefore, $|[9]_{31}| = 15$.

- Suppose that there exists $c \in \mathbb{Z}/31\mathbb{Z}$ such that $c^3 = [9]_{31}$. Clearly, $c \neq [0]_{31}$ so $c \in (\mathbb{Z}/31\mathbb{Z})^*$. By Proposition 1.13, we must have $\operatorname{lcm}(3, |c|) = |[9]_{31}| \cdot 3 = 3^2 \cdot 5$, which implies that $|c| = 45$ in $(\mathbb{Z}/31\mathbb{Z})^*$. But the order of c must be less or equal than the order of $(\mathbb{Z}/31\mathbb{Z})^*$, which is 30, a contradiction. Therefore, the equation $x^3 - 9 = 0$ cannot have solutions in $\mathbb{Z}/31\mathbb{Z}$. ■

EXERCISE 4.13 ¬ Prove that $\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$. [IV.5.14]

■ SOLUTION Observe that, since $|\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}| = 4$, and, for every automorphism φ, $\varphi(0,0) = (0,0)$, then, enumerating the other three elements, $\mathrm{Aut}_{\mathsf{Grp}}$ can be identified as a subgroup of S_3. Moreover,

the bijections $\varphi\colon \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\psi\colon \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ defined by

$$\begin{aligned}\varphi(a,b) &= (b,a),\\ \psi(0,0) &= (0,0),\\ \psi(1,0) &= (1,1),\\ \psi(0,1) &= (1,0),\\ \psi(1,0) &= (0,1)\end{aligned}$$

are, in fact, homomorphisms and satisfies $\varphi^2 = \mathrm{id}$ and $\psi^3 = \mathrm{id}$. Since these permutations generate S_3, we conclude $\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}) \cong S_3$. ∎

EXERCISE 4.14 ▷ Prove that the order of the group of automorphisms of the cyclic group C_n is the number of positive integers $r \leq n$ that are *relatively prime* to n. (This is called *Euler's ϕ-function*; cf. Exercise 6.14.) [§IV.1.4, IV.1.22, §IV.2.5]

∎ SOLUTION Since 1 generates the group, an automorphism is determined by the image of 1. Since an automorphism φ is, in particular, an isomorphism, the image of 1 is also a generator of C_n, which occurs if and only if $\gcd(\varphi(1), n) = 1$ and we have exactly $\phi(n)$ choices for $\varphi(1)$. ∎

EXERCISE 4.15 ¬ Compute the group of automorphisms of $(\mathbb{Z}, +)$. Prove that if p is prime, then $\mathrm{Aut}_{\mathsf{Grp}}(C_p) \cong C_{p-1}$. (Use Exercise **??**.) [IV.5.12]

∎ SOLUTION As in the previous exercise, since 1 generates $\mathbb{Z}$, any automorphism $\varphi : \mathbb{Z} \to \mathbb{Z}$ is determined by $\varphi(1)$. Since φ is, in particular, an isomorphism, $\varphi(1)$ must also be a generator of $\mathbb{Z}$. Thus, $\varphi(1) = 1$ or $\varphi(1) = -1$, and we have just two automorphisms: one is the identity on $\mathbb{Z}$ and the other one changes the signal of the input integer. It follows that $\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}) \cong C_2$.

Now, let's prove that $\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/((p-1)\mathbb{Z})$ if p is prime. Again, any automorphism of $\mathbb{Z}/p\mathbb{Z}$ is determined by the image of $[1]_p$, which must be a generator of $\mathbb{Z}/p\mathbb{Z}$. Conversely, each generator determines an automorphism of $\mathbb{Z}/p\mathbb{Z}$. Since the generators are the elements of $(\mathbb{Z}/p\mathbb{Z})^*$, these automorphisms are given by

$$\begin{aligned}\varphi_{[n]_p} : \mathbb{Z}/p\mathbb{Z} &\longrightarrow \mathbb{Z}/p\mathbb{Z}\\ [m]_p &\longmapsto m \cdot [n]_p = [m]_p \cdot [n]_p\end{aligned}$$

for all $[n]_p \in (\mathbb{Z}/p\mathbb{Z})^*$. By Exercise **??**, there is a generator x of $(\mathbb{Z}/p\mathbb{Z})^*$. We claim that φ_x generates $\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/p\mathbb{Z})$. Indeed, given $\varphi_y \in \mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/p\mathbb{Z})$, there exists $z \in \mathbb{Z}$ (which we can take positive because $(\mathbb{Z}/p\mathbb{Z})^*$ is finite) such that $y = x^z$ and so

$$\varphi_y(m) = my = mx^z = \varphi_x^z(m)$$

for all $m \in (\mathbb{Z}/p\mathbb{Z})^*$. Thus, $\varphi_y = \varphi_x^z$, as desired. Since the order of $\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/p\mathbb{Z})$ is $p-1$, Exercise 4.3 implies that $\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/((p-1)\mathbb{Z})$. ∎

Similiarly, if $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic, then $\mathrm{Aut}_{\mathsf{Grp}}(C_n) \cong C_{\phi(n)}$, where ϕ denotes Euler's ϕ-function.

EXERCISE 4.16 ¬ Prove *Wilson's theorem: an integer $p > 1$ is prime if and only if*

$$(p-1)! \equiv -1 \mod p.$$

(For one direction, use Exercises 1.8 and **??**. For the other, assume d is a proper divisor of p, and note that d divides $(p-1)!$; therefore....) [IV.4.11]

∎ SOLUTION Let $p > 1$ be a prime number and $G = (\mathbb{Z}/p\mathbb{Z})^*$. By Exercise **??**, G is a cyclic group. Also, we have that $|G| = p-1$. In fact, if $m \in \{1, 2, \ldots, p-1\}$, Exercise 2.13 implies that there exists integers a and b such that

$$am + bp = 1.$$

Modulo p this means that a is the multiplicative inverse of m and so $[m] \in G$. It follows that $G \cong \mathbb{Z}/(p-1)\mathbb{Z}$. If $p = 2$, the result is trivial. Otherwise, this isomorphism makes clear that G has a unique element of order 2. Namely, $[-1]_p$. By Exercise 1.8, it follows that

$$(p-1)! \equiv -1 \mod p.$$

Conversely, if d is a proper divisor of p, we have that $d|(p-1)!$ as it is smaller than p. By our hypothesis, p (and hence d) divides $(p-1)! + 1$. It follows that $d|1$ and then p is prime. ∎

EXERCISE 4.17 For a few small (but not too small) primes p, find a generator of $(\mathbb{Z}/p\mathbb{Z})^*$.

∎ SOLUTION

- $p = 7$: Since $2^3 \equiv 1 \mod 7$, 2 is not a generator of $(\mathbb{Z}/7\mathbb{Z})^*$. On the other hand,

$$\begin{aligned} 3 &\equiv 3 \mod 7 \\ 3^2 &\equiv 2 \mod 7 \\ 3^3 &\equiv 2 \cdot 3 \equiv -1 \mod 7. \end{aligned}$$

  Therefore $3^4 \equiv -3 \mod 7$, $3^5 \equiv -2 \mod 7$ and $3^6 \equiv 1 \mod 7$, and 3 is a generator.

- $p = 13$: Once again, we start trying with the small numbers.

$$\begin{aligned} 2 &\not\equiv 1 \mod 13 \\ 2^2 &\equiv 4 \mod 13 \\ 2^3 &\equiv -5 \mod 13 \\ 2^4 &\equiv 3 \mod 13 \\ 2^5 &\equiv 6 \mod 13 \\ 2^6 &\equiv -1 \mod 13. \end{aligned}$$

  As we have argued above, $2^{n+6} \equiv -2^n \not\equiv 1 \mod 13$, unless $n = 6$, therefore 2 is a generator of $(\mathbb{Z}/13\mathbb{Z})^*$.

- $p = 23$: Since $2^5 \equiv 9 \mod 23$, then $2^{10} \equiv 81 \equiv 12 \mod 23$, $2^{11} \equiv 1 \mod 23$ and 2 is not a generator of $(\mathbb{Z}/23\mathbb{Z})^*$. Similarly, since $2^5 \equiv 3^2 \mod 23$ and $3^3 \equiv 2^2 \mod 23$, and since $5 + 2 + 2 + 2 = 11 = 2 + 3 + 3 + 3$, then $3^{11} \equiv 2^{11} \equiv 1 \mod 23$. On the other hand, $5^2 \equiv 2 \mod 23$, hence $5^{10} \equiv 2^5 \equiv 9 \mod 23$ and $5^{11} \equiv -1 \mod 23$. Analogously as the other two problems, $5^{n+11} \equiv -5^n \not\equiv 1 \mod 23$, and 5 is the desired generator. ∎

As the reader might have noticed, a is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ if and only if $a^{\frac{p-1}{2}} \equiv -1$.

Remark. In general, there are no fast algorithms to find such generators. Furthermore, there is a famous open problem.

Artin's Conjecture (1927). Given an integer a which is neither a perfect square nor -1, then there are infinitely many primes p such that a is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$.

EXERCISE 4.18 Prove the second part of Proposition 4.8.

PROPOSITION 4.8 Let $\varphi : G \to H$ be an isomorphism.

- $(\forall g \in G) : |\varphi(g)| = |g|$;
- G is commutative if and only if H is commutative.

∎ SOLUTION Suppose that G is commutative and take $h_1, h_2 \in H$. Since φ is an isomorphism, there are $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. Thus,

$$h_1 h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2) = \varphi(g_2 g_1) = \varphi(g_2)\varphi(g_1) = h_2 h_1$$

and we conclude that H is commutative. The other implication is similar and it uses φ^{-1}, which is also an isomorphism. ∎

EXERCISE 5.1

■ SOLUTION A ■

EXERCISE 5.2 Since trivial groups T are initial in Grp, one may be led to think that (e, T) should be initial in $\mathscr{F}^A$, for every A: e would be defined by sending every element of A to the (only) element of T; and for any other group G, *there is a unique* homomorphism $T \to G$. Explain why (e, T) is *not* initial in $\mathscr{F}^A$ (unless $A = \emptyset$).

■ SOLUTION If the pair (e, T) is as above and (j, G) is an arbitrary object in $\mathscr{F}^A$, then a morphism from (e, T) to (j, G) is a homomorphism φ such that $\varphi(e(a)) = j(a)$ for every $a \in A$. But $e(a) = e_T$, then $j(a) = \varphi(e_T) = e_G$ for every $a \in A$, which means the morphism does not exists if j is not the constant function $j(a) = e_G$. Therefore (e, T) is not initial in $\mathscr{F}^A$. ■

EXERCISE 5.3 ▷ Use the universal property of free groups to prove that the map $j : A \to F(A)$ is injective, for all sets A. (Hint: It suffices to show that for every two elements a, b of A there is a group G and a set-function $f : A \to G$ such that $f(a) \neq f(b)$. Why? How do you construct f and G?) [§III.6.3]

■ SOLUTION Let a, b be two distinct elements of A. Take G as any non-trivial group and define $f : A \to G$ as the function which sends every element of A to e_G except for b. By the universal property of free groups, there exists a (unique) homomorphism $\varphi : F(A) \to G$ such that $f = \varphi \circ j$. This condition implies that $j(a) \neq j(b)$ since $f(a) \neq f(b)$. Therefore, we conclude that j is injective. ■

EXERCISE 5.4 ▷ In the 'concrete' construction of free groups, one can try to reduce words by performing cancellations in any order; the process of 'elementary reductions' used in the text (that is, from left to right) is only one possibility. Prove that the result of iterating cancellations on a word is independent of the order in which the cancellations are performed. Deduce the associativity of the product in $F(A)$ from this. [§5.3]

■ SOLUTION T ■

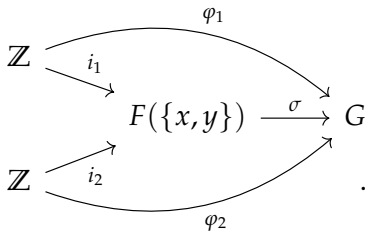
EXERCISE 5.5 Verify explicitly that $H^{\oplus A}$ is a group.

■ SOLUTION Observe first $H^{\oplus A}$ is not empty, since $e\colon A \to H$ defined by $e(a) = e_H$ for every $a \in A$ is the set. For any $\alpha \in H^{\oplus A}$, we can define $E_{\alpha'} = \{a \in A \mid \alpha'(a) \neq e_H\}$ and this set is finite. Hence, if $\alpha'\colon A \to H$ and $\alpha''\colon A \to H$ are in $H^{\oplus A}$, then $E_{\alpha'+\alpha''} \subset E_{\alpha'} \cup E_{\alpha''}$ is a finite set, and $E_{-\alpha'} = E_{\alpha'}$ is also finite. Since e is an identity for the operation and the structure inherited from H^A is associative, $H^{\oplus A}$ is a group. ■

EXERCISE 5.6 ▷ Prove that the group $F(\{x,y\})$ (visualized in Example 5.3) is a coproduct $\mathbb{Z} * \mathbb{Z}$ of $\mathbb{Z}$ by itself in the category Grp. (Hint: With due care, the universal property for one turns into the universal property for the other.) [§3.4, 3.7, 5.7]

■ SOLUTION Recall that $\mathbb{Z}$ satisfy the universal property for the free group over $\{x\}$ and over $\{y\}$. Let j_x and j_y be the inclusions of $\{x\}$ and $\{y\}$ in $\mathbb{Z}$, respectively, so that $j_x(x) = j_y(y) = 1$. Moreover, denote i_x and i_y as the inclusions of $\{x\}$ and $\{y\}$ in $\{x,y\}$, respectively, and j as the inclusion of $\{x,y\}$ in $F(\{x,y\})$. By the universal property of free groups, there are unique homomorphisms $i_1, i_2 : \mathbb{Z} \to F(\{x,y\})$ such that $i_1 j_x = j i_x$ and $i_2 j_y = j i_y$. We claim that $F(\{x,y\})$ with i_1 and i_2 is a coproduct of $\mathbb{Z}$ by itself in Grp.

Let G be another group with homomorphisms $\varphi_1, \varphi_2 : \mathbb{Z} \to G$. They induce functions $\varphi_1 j_x : \{x\} \to G$, $\varphi_2 j_y : \{y\} \to G$ and, since $\{x,y\}$ is a coproduct of $\{x\}$ and $\{y\}$ in Set, there exists a unique function $\varphi : \{x,y\} \to G$ such that $\varphi_1 j_x = \varphi i_x$ and $\varphi_2 j_y = \varphi i_y$. Now, by the universal property of free groups, there exists a unique homomorphism $\sigma : F(\{x,y\}) \to G$ such that $\varphi = \sigma j$. We affirm that the following diagram commutes:



Indeed, we have that

$$\varphi_1 j_x = \varphi i_x = (\sigma j) i_x = \sigma(j i_x) = \sigma i_1 j_x$$

and, since $\mathbb{Z}$ satisfies the universal property of free groups, $\varphi_1 = \sigma i_1$. Similarly, we get that $\varphi_2 = \sigma i_2$ and, thus, the diagram really commutes. Now, we just need to show that σ is the only homomorphism that makes this diagram commute. Suppose $\rho : F(\{x,y\}) \to G$ is another homomorphism that commutes the diagram. Note that

$$\begin{aligned}(\rho j)(x) &= (\rho(j i_x))(x) \\ &= (\rho(i_1 j_x))(x) \\ &= ((\rho i_1)(j_x))(x) \\ &= (\varphi_1 j_x)(x) \\ &= (\varphi i_x)(x) \\ &= \varphi(x)\end{aligned}$$

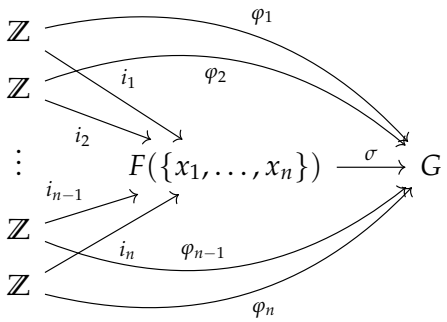
and, similarly, $(\rho j)(y) = \varphi(y)$. Therefore, $\rho j = \varphi$ and, by the uniqueness of σ, we have that $\rho = \sigma$. We conclude that $F(\{x,y\})$ is the desired coproduct. ■

EXERCISE 5.7 ▷ Extend the result of Exercise 5.6 to free groups $F(\{x_1,\dots,x_n\})$ and to free *abelian* groups $F^{ab}(\{x_1,\dots,x_n\})$. [§3.4, §5.4]

■ SOLUTION We proceed in exactly the same way as in the preceding exercise. Let j_{x_k} be the inclusions of $\{x_k\}$ in $\mathbb{Z}$ such that $j_{x_k}(x_k) = 1$ for all $k \in \{1,\dots,n\}$. Also, we denote by i_{x_k} the inclusions of $\{x_k\}$ in $\{x_1,\dots,x_n\}$ and j the inclusion of $\{x_1,\dots,x_n\}$ in $F(\{x_1,\dots,x_n\})$. As before, the universal property of free groups implies the existence of unique morphisms $i_k : \mathbb{Z} \to F(\{x_1,\dots,x_n\})$ such that

$$i_k j_{x_k} = j i_{x_k}$$

for all k. Exactly as before, the diagram

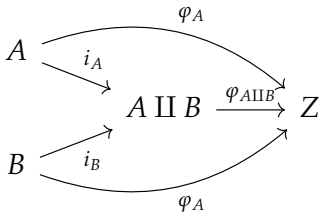


commutes, which implies that $F(\{x_1,\dots,x_n\})$ satisfies the universal property for the coproduct $\mathbb{Z}^{*n}$.

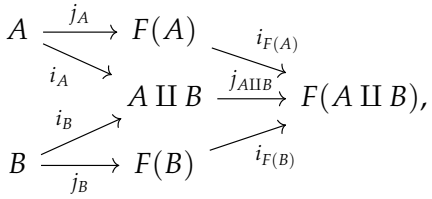
Surely, the same thing holds in Ab. ■

EXERCISE 5.8 Still more generally, prove that $F(A \amalg B) = F(A) * F(B)$ and that $F^{ab}(A \amalg B) = F^{ab}(A) \oplus F^{ab}(B)$ for all sets A, B. (That is, the constructions F and F^{ab} 'preserve coproducts'.)

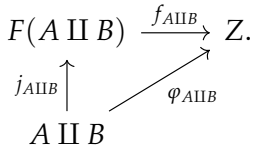
■ SOLUTION Since $F(A), F(B) \subset F(A \amalg B)$, let $i_{F(A)} : F(A) \to F(A \amalg B)$ and $i_{F(B)} : F(B) \to F(A \amalg B)$ be the the natural injection. Then we desire to prove $(F(A \amalg B), i_{F(A)}, i_{F(B)})$ is an initial object in the category defined in §I.5.5. First observe this triple is in this category, since $i_{F(A)}$ and $i_{F(B)}$ are trivially homomorphisms. Further, let $(j_A, F(A))$ and $(j_B, F(B))$ be the free products of A and B respectively. Now, Let (Z, f_A, f_B) be an element in that category. Then f_A and f_B induces set-functions $\varphi_A : A \to Z$ and $\varphi_B : B \to Z$ defined by $\varphi_A = f_A \circ j_A$ and $\varphi_B = f_B \circ j_B$. Since $A \amalg B$ is the coproduct of A and B in Set, there exists a unique function $\varphi_{A\amalg B} : A \amalg B \to Z$ such that the diagram



commutes. Furthermore, if $(j_{A\amalg B}, A \amalg B)$ is the free product of $A \amalg B$, then the following diagram commutes



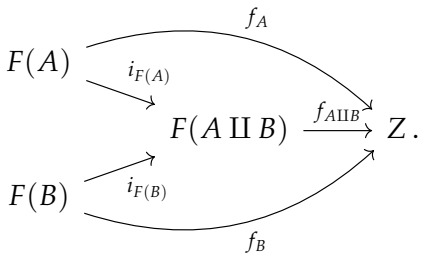
and, by the universal property of free product, there exist a unique morphism $f_{A\amalg B}\colon F(A \amalg B) \to Z$ in the category $\mathscr{F}^{A\amalg B}$ such that



Therefore, using everything above,

$$\begin{aligned} f_{A\amalg B} \circ i_{F(A)} \circ j_A &= f_{A\amalg B} \circ j_{A\amalg B} \circ i_A \\ &= \varphi_{A\amalg B} \circ i_A \\ &= \varphi_A \\ &= f_A \circ j_A. \end{aligned}$$

By the universal property of the free product, this means $f_A = f_{A\amalg B} \circ i_{F(A)}$. Analogously, $f_B = f_{A\amalg B} \circ i_{F(B)}$, which proves the existence of a morphism such that the following diagram commutes



Moreover, any such morphism σ must be equal to $f_{A\amalg B}$. In fact, σ and $f_{A\amalg B}$ induces the same morphisms in A, B, $F(A)$ and $F(B)$, therefore, using the uniqueness of the universal properties, we will find the same function and we conclude $\sigma = f_{A\amalg B}$.

Since everything was done using universal properties, the result follows mutatis mutandis for F^{ab}. ∎

EXERCISE 5.9 Let $G = \mathbb{Z}^{\oplus\mathbb{N}}$. Prove that $G \times G \cong G$.

∎ SOLUTION Recalling that the elements of G are functions from $\mathbb{N}$ to $\mathbb{Z}$, we define

$$\begin{aligned} \varphi : G \times G &\longrightarrow G \\ (f_1, f_2) &\longmapsto f \end{aligned}$$

where

$$f(n) = \begin{cases} f_1\left(\frac{n}{2}\right), & \text{if } n \text{ is even,} \\ f_2\left(\frac{n-1}{2}\right), & \text{if } n \text{ is odd.} \end{cases}$$

In other words, φ combines f_1 and f_2 into only one function f by alternating between those two. For example, $f(0) = f_1(0)$, $f(1) = f_2(0)$, $f(2) = f_1(1)$, $f(3) = f_2(1)$, and so on. Since $f_1(n) \neq 0$ and $f_2(m) \neq 0$ for finitely many $n, m \in \mathbb{N}$, we also have $f(n) \neq 0$ for finitely many $n \in \mathbb{N}$, so φ is well-defined. Also, note that φ is a bijection because it has the inverse

$$\begin{aligned} \varphi^{-1} : G &\longrightarrow G \times G \\ f &\longmapsto (f_1, f_2) \end{aligned}$$

where $f_1(n) = f(2n)$ and $f_2(n) = f(2n+1)$ for all $n \in \mathbb{N}$. Finally, it is easy to check that φ preserves operation, so it is an isomorphism and $G \times G \cong G$.

We can also show this using the last exercise. Since there is a bijection between $\mathbb{N}$ and $\mathbb{N} \amalg \mathbb{N}$ (for example, one can take an analogue of the function above), we have that

$$G = F^{ab}(\mathbb{N}) \cong F^{ab}(\mathbb{N} \amalg \mathbb{N}) \cong F^{ab}(\mathbb{N}) \oplus F^{ab}(\mathbb{N}) = G \oplus G.$$

Since coproducts are the same as products in Ab, we conclude that $G \cong G \times G$. ∎

EXERCISE 5.10

∎ SOLUTION A ∎

6 SUBGROUPS

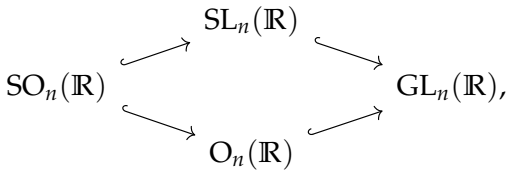
EXERCISE 6.1 ¬ (If you know about matrices.) The group of invertible $n \times n$ matrices with entries in $\mathbb{R}$ is denoted $\mathrm{GL}_n(\mathbb{R})$ (Example 1.5). Similarly, $\mathrm{GL}_n(\mathbb{C})$ denotes the group of $n \times n$ invertible matrices with *complex* entries. Consider the following sets of matrices:

- $\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid \det(M) = 1\}$;
- $\mathrm{SL}_n(\mathbb{C}) = \{M \in \mathrm{GL}_n(\mathbb{C}) \mid \det(M) = 1\}$;
- $\mathrm{O}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid MM^t = M^tM = I_n\}$;
- $\mathrm{SO}_n(\mathbb{R}) = \{M \in \mathrm{O}_n(\mathbb{R}) \mid \det(M) = 1\}$;
- $\mathrm{U}(n) = \{M \in \mathrm{GL}_n(\mathbb{C}) \mid MM^\dagger = M^\dagger M = I_n\}$;
- $\mathrm{SU}(n) = \{M \in \mathrm{U}(n) \mid \det(M) = 1\}$.

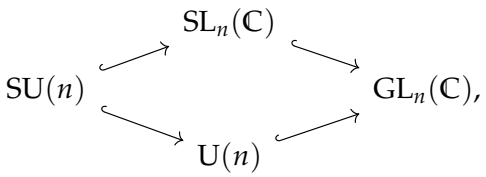
Here I_n stands for the $n \times n$ *identity matrix*, M^t is the *transpose* of M, $M^\dagger$ is the *conjugate transpose* of M, and $\det(M)$ denotes the *determinant* of M. Find all possible inclusions among these sets, and prove that in every case the smaller set is a subgroup of the larger one.

These sets of matrices have compelling geometric interpretations: for example, $\mathrm{SO}_3(\mathbb{R})$ is the group of 'rotations' in $\mathbb{R}^3$. [8.8, 9.1, III.1.4, VI.6.16]

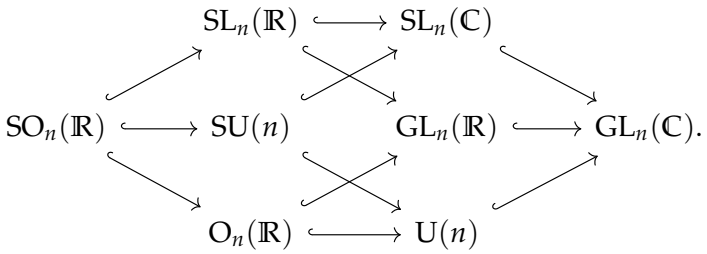
■ SOLUTION In the following diagrams, the hooked arrows denotes the natural injections, therefore $A \hookrightarrow B$ means $A \subseteq B$. The first diagram contains only the real matrices



the second diagram only complex matrices,



and the third diagram contains all of the matrices, using the fact that $\mathbb{R} \subseteq \mathbb{C}$



Let's prove that all of these sets are groups. Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$. Then if $A, B \in \mathrm{SL}_n(\mathbb{K})$, then $\det(A) = \det(B) = 1$ and $\det(AB^{-1}) = \det(A) \cdot \det(B)^{-1} = 1$, therefore $AB^{-1} \in \mathrm{SL}_n(\mathbb{K})$ and it is a subgroup of $\mathrm{GL}_n(\mathbb{K})$. Since the conjugate of a real number is itself, then $M^t = M^\dagger$ for any real matrix M. Let $A, B \in \mathrm{O}_n(\mathbb{R})$ or $\mathrm{U}(n)$, then $B^{-1}(B^{-1})^\dagger = (B^{-1})^\dagger B^{-1} = I_n$,

$$\begin{aligned}(AB^{-1})(AB^{-1})^\dagger &= A(B^{-1}(B^{-1})^\dagger)A^\dagger \\ &= AI_nA^\dagger \\ &= AA^\dagger \\ &= I_n\end{aligned}$$

and similarly for $(AB^{-1})^\dagger(AB^{-1})$. Therefore $\mathrm{O}_n(\mathbb{R})$ and $\mathrm{U}(n)$ are subgroups of $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{C})$ respectively. Finally, since $\mathrm{SO}_n(\mathbb{R}) = \mathrm{O}_n(\mathbb{R}) \cap \mathrm{SL}_n(\mathbb{R})$ and $\mathrm{SU}(n) = \mathrm{U}(n) \cap \mathrm{SL}_n(\mathbb{C})$, the result follows from Lemma 6.3. Clearly, these sets are not empty, since I_n belongs to all of them. ∎

EXERCISE 6.2 ¬ Prove that the set of 2×2 matrices

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$$

with $a, b, d \in \mathbb{C}$ and $ad \neq 0$ is a subgroup of $\mathrm{GL}_2(\mathbb{C})$. More generally, prove that the set of $n \times n$ complex matrices $(a_{ij})_{1 \leq i,j \leq n}$ with $a_{ij} = 0$ for $i > j$ and $a_{11} \cdots a_{nn} \neq 0$ is a subgroup of $\mathrm{GL}_n(\mathbb{C})$. (These matrices are called 'upper triangular', for evident reasons.) [IV.1.20]

∎ SOLUTION We'll prove the more general statement. Let $\mathrm{UT}_n(\mathbb{C})$ be this set and let A and B be matrices of that form, then:

Although they are always called *upper triangular*, this notation is not canonical.

- $AB \in \mathrm{UT}_n(\mathbb{C})$. Let $AB = (c_{ij})_{1 \leq i,j \leq n}$, and $i > j$. By definition of matrix multiplication,

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

  If $i > k$, then $a_{ik} = 0$, and if $k > j$, then $b_{kj} = 0$. Since there is no $i \leq k \leq j$, for $i > j$, then $c_{ij} = 0$.

  Similarly, for $i = j$,

$$c_{ii} = \sum_{k=1}^{\infty} a_{ik} b_{ki}.$$

  If $k \neq i$, then either $k > i$ or $i > k$, and in both cases $a_{ik} b_{ki} = 0$. Therefore $c_{ii} = a_{ii} b_{ii} \neq 0$.

- $B^{-1} \in \mathrm{UT}_n(\mathbb{C})$. Let $B^{-1} = (b_{ij}^{-1})_{1 \leq i,j \leq n}$. Since $B^{-1}B = I_n$, then

$$\sum_{k=1}^{n} b_{ik}^{-1} b_{kj} = \delta_{ij}$$

  if $i \neq j$ (in particular, for $i > j$). Initially, fix $j = 1$. If $i = 1$, then

$$1 = \sum_{k=1}^{n} b_{1k}^{-1} b_{k1} = b_{11}^{-1} b_{11},$$

  implying $b_{11}^{-1} = \frac{1}{b_{11}} \neq 0$. If $i > 1$, then

$$0 = \sum_{k=1}^{n} b_{ik}^{-1} b_{k1} = b_{i1}^{-1} b_{11},$$

  implying $b_{i1}^{-1} = 0$.

The Kronecker delta δ_{ij} is a function defined by $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise.

Now, fix $j = 2$. If $i = 2$, then

$$1 = \sum_{k=1}^{n} b_{2k}^{-1} b_{k2} = b_{22}^{-1} b_{22},$$

for, as we have proved, $b_{21} = 0$, which implies $b^{-1} = \frac{1}{b_{22}} \neq 0$, and if $i > 2$, then

$$0 = \sum_{k=1}^{n} b_{ik}^{-1} b_{k2} = b_{i2}^{-1} b_{22},$$

where once again we used $b_{21} = 0$, implying $b_{i2}^{-1} = 0$.

Continuing in this way, we conclude that $b_{ij}^{-1} = 0$ if $i > j$ and $b_{ii}^{-1} = \frac{1}{b_{ii}} \neq 0$.

Since $I_n \in \mathrm{UT}_n(\mathbb{C})$, this set is nonempty and, thus, a group. ∎

EXERCISE 6.3 ¬ Prove that every matrix in SU(2) may be written in the form

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$ and $a^2 + b^2 + c^2 + d^2 = 1$. (Thus, SU(2) may be realized as a three-dimensional sphere embedded in $\mathbb{R}^4$; in particular, it is *simply connected*.) [8.9, III.2.5]

∎ SOLUTION Let $M \in \mathrm{SU}(2)$ and $x, y, z, w \in \mathbb{C}$ be such that

$$M = \begin{pmatrix} x & y \\ z & w \end{pmatrix}.$$

Since $\det(M) = 1$, we have that

$$M^{-1} = \begin{pmatrix} w & -y \\ -z & x \end{pmatrix},$$

but we also know that $MM^\dagger = M^\dagger M = I_n$, that is, $M^\dagger = M^{-1}$. Thus, $w = \overline{x}$ and $z = -\overline{y}$. If $a, b, c, d \in \mathbb{R}$ are such that $x = a + bi$ and $y = c + di$,

$$M = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

and $\det(\mathrm{M}) = 1$ implies that $x\overline{x} - y(-\overline{y}) = |x|^2 + |y|^2 = a^2 + b^2 + c^2 + d^2 = 1$, as desired. ∎

Remark. The group SU(2) is closely related to the *quaternions*, discovered by the mathematician Willian Hamilton in 1843. To see

this relation, it will come in handy to express quaternions as 2×2 matrices. Let $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ be the following matrices:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},$$
$$\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

The set $\mathbb{H}$ of quaternions are the matrices of the form

$$a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$. Note that the following identities hold:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1},$$
$$\mathbf{ij} = -\mathbf{ji} = \mathbf{k},$$
$$\mathbf{jk} = -\mathbf{kj} = \mathbf{i},$$
$$\mathbf{ki} = -\mathbf{ik} = \mathbf{j}.$$

They imply that $\mathbb{H}$ is closed with respect to addition and multiplication of matrices. Moreover, given a quaternion $X = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, we can define its conjugate by $\overline{X} = a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$. It follows that $X\overline{X} = \overline{X}X = (a^2 + b^2 + c^2 + d^2)\mathbf{1}$ so, if $N(X) = a^2 + b^2 + c^2 + d^2 \neq 0$, X is invertible and $X^{-1} = \overline{X}/N(X)$. The number $N(X)$ is called the norm of X. Since $\overline{XY} = \overline{Y} \cdot \overline{X}$, it is easy to check that the norm is multiplicative, that is, $N(XY) = N(X)N(Y)$, for all $X, Y \in \mathbb{H}$. Therefore, the set of quaternions of norm 1 form a group under multiplication and it follows immediately from this exercise that this group is in fact $\mathrm{SU}(2)$.

Quaternions will be introduced by Aluffi in the initial exercises of chapter III and we will use them in Exercise 8.9.

EXERCISE 6.4 ¬ Let G be a group, and let $g \in G$. Verify that the image of the exponential map $\epsilon_g : \mathbb{Z} \to G$ is a cyclic group (in the sense of Definition 4.7). [§6.3, §7.5]

■ SOLUTION If $|g| = \infty$, all the elements in $\{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$ are distinct. In other words,

$$\mathbb{Z} \to \epsilon_g(\mathbb{Z})$$
$$n \mapsto g^n$$

is injective. Since it is clearly a surjective homomorphism, it follows that $G \cong \mathbb{Z}$.

Otherwise, let $|g| = m$. Similarly as before, this implies that all the elements in $\{e, g, \ldots, g^{m-1}\}$ are distinct. So,

$$\begin{aligned} \mathbb{Z}/m\mathbb{Z} &\to \epsilon_g(\mathbb{Z}) \\ [n]_m &\mapsto g^n \end{aligned}$$

is well-defined (since $|g| = m$) and injective. It is also a surjective homomorphism, so it follows that $G \cong \mathbb{Z}/m\mathbb{Z}$. We conclude that in either case G is cyclic. ∎

EXERCISE 6.5 Let G be a *commutative* group, and let $n > 0$ be an integer. Prove that $\{ g^n \mid g \in G \}$ is a subgroup of G. Prove that this is not necessarily the case if G is not commutative.

∎ SOLUTION Let G be a commutative group and $H = \{ g^n \mid g \in G \}$ and observe that it is trivially non-empty, therefore we just have to prove if $a, b \in H$ then $ab^{-1} \in H$. In fact, $a = g^n$ and $b = h^n$, therefore $ab^{-1} = g^n(h^n)^{-1} = g^n(h^{-1})^n = (gh^{-1})^n$ is an element of H. On the other hand, let $G = S_3$ and let

$$x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ and } y = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Then $x^2 = e$, $y^3 = e$ and $yx = xy^2$. Further, $G = \{e, x, y, y^2, xy, xy^2\}$. But the set $H = \{g^3 \mid g \in G\}$ is not a group. In fact, $e^3 = e$, $x^3 = x$, $y^3 = e$, $(y^2)^3 = e$, $(xy)^3 = x(yx)yxy = x(xy^2)yxy = x^2y^3xy = xy$, and, finally, $(xy^2)^3 = x(y^2x)y^2xy^2 = x(xy)y^2xy^2 = x^2y^3xy^2 = xy^2$. Therefore $H = \{e, x, xy, xy^2\}$, which is not a subgroup of G. ∎

EXERCISE 6.6 Prove that the union of a family of subgroups of a group G is not necessarily a subgroup of G. In fact:

- Let H, H' be subgroups of a group G. Prove that $H \cup H'$ is a subgroup of G only if $H \subseteq H'$ or $H' \subseteq H$.
- On the other hand, let $H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots$ be subgroups of a group G. Prove that $\bigcup_{i \geq 0} H_i$ is a subgroup of G.

∎ SOLUTION To see that the union of a family of subgroups of a group G is not necessarily a subgroup of G, we will take $G = \mathbb{Z}/6\mathbb{Z}$ and the subgroups $H = \{[0]_6, [3]_6\}$ and $H' = \{[0]_6, [2]_6, [4]_6\}$. Note that $[2]_6, [3]_6 \in H \cup H'$, but $[2]_6 + [3]_6 = [5]_6 \notin H \cup H'$ and so $H \cup H'$ is not a subgroup of G. Furthermore:

- Assume that $H \cup H'$ is a subgroup of G and suppose that $H \not\subseteq H'$. Thus, there exists $h \in H$ such that $h \notin H'$. We claim that $H' \subseteq H$. Indeed, let $h' \in H'$ and take $g = hh'$, which is in $H \cup H'$ since it is a subgroup of G. If $g \in H'$ we would have that $h = gh'^{-1} \in H'$ since H' is a subgroup of G. It follows that $g \in H$ and so

$h' = h^{-1}g \in H$ and $H' \subseteq H$. Therefore, if $H \cup H'$ is a subgroup of G then $H \subseteq H'$ or $H' \subseteq H$. Note that the converse is trivially true.

- Since each subgroup is non-empty, $\bigcup_{i\geq 0} H_i$ is also non-empty. Now, if $a, b \in \bigcup_{i\geq 0} H_i$, there are $n, m \in \mathbb{N}$ such that $a \in H_n$ and $b \in H_m$. Assume without loss of generality that $n \leq m$, so $H_n \subseteq H_m$ and both a and b are in H_m. Since its a subgroup of G, $ab^{-1} \in H_m$ and, therefore, $ab^{-1} \in \bigcup_{i\geq 0} H_i$. We conclude that $\bigcup_{i\geq 0} H_i$ is a subgroup of G. ∎

EXERCISE 6.7

∎ SOLUTION A ∎

EXERCISE 6.8 Prove that an *abelian* group G is finitely generated if and only if there is a surjective homomorphism

$$\underbrace{\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}}_{n \text{ times}} \twoheadrightarrow G$$

for some n.

∎ SOLUTION If there is such a surjective homomorphism φ, then G is trivially abelian since $gh = \varphi(z_1 \cdot z_2) = \varphi(z_2 \cdot z_2) = hg$ and it is generated by $g_i = \varphi(e_i)$ for $e_i = (0, \ldots, 1, \ldots, 0)$ (where 1 appears in the i-th position). Therefore, let $g \in G$, then there exists $z = (a_1, \ldots, a_n)$ such that $g = \varphi(z) = \varphi(a_1e_1 + \cdots + a_ne_n) = \varphi(e_1)^{a_1} \cdots \varphi(e_n)^{a_n} = g_1^{a_1} \cdots g_n^{a_n}$. Reciprocally, suppose $g_1, \ldots, g_n$ generates G. Then the function $\psi \colon \mathbb{Z}^n \to G$ defined by $\psi(a_1, \ldots, a_n) = g^{a_1} \cdots g^{a_n}$ is a surjective homomorphism. In fact, since $g_1, \ldots, g_n$ generates G, the function is surjective. Moreover,

$$\begin{aligned}\psi(a_1, \ldots, a_n)\psi(b_1, \ldots, b_n) &= (g_1^{a_1} \cdots g_n^{a_n})(g_1^{b_1} \cdots g_n^{b_n}) \\ &= g^{a_1+b_1} \cdots g^{a_n+b_n} \\ &= \psi(a_1 + b_1, \ldots, a_n + b_n)\end{aligned}$$

and we're done. ∎

EXERCISE 6.9 Prove that every finitely generated subgroup of $\mathbb{Q}$ is cyclic. Prove that $\mathbb{Q}$ is not finitely generated.

∎ SOLUTION Let $G \subseteq \mathbb{Q}$ be the subgroup generated by $r_1, r_2, \ldots, r_n \in \mathbb{Q}$. Let P be the product of the denominators of these generators in their irreducible form. It follows that $H = \{P \cdot g \mid g \in G\}$ is a subset of $\mathbb{Z}$. Moreover, we claim that H a subgroup of $\mathbb{Z}$. Firstly, note that it is non-empty, since $G \neq \emptyset$. Now, if $a, b \in H$, there are $g_1, g_2 \in G$ such that $a = P \cdot g_1$ and $b = P \cdot g_2$. Thus, since $g_1 - g_2 \in G$, $a - b = P \cdot g_1 - P \cdot g_2 = P \cdot (g_1 - g_2) \in H$, and H is indeed a subgroup of

$\mathbb{Z}$. By Proposition 6.9, $H = d\mathbb{Z}$ for some non-negative integer d. We conclude that G is generated by $\frac{d}{p}$ and, by Exercise 6.4, G is cyclic.

To prove that $\mathbb{Q}$ is not finitely generated, it suffices to show that it is not cyclic. If it were generated by some rational number r, which must be non-zero, then $\frac{r}{2}$ would be an integer multiple of r, implying that $\frac{1}{2} \in \mathbb{Z}$, a contradiction. Therefore, $\mathbb{Q}$ is not cyclic. ∎

EXERCISE 6.10 ¬ The set of 2×2 matrices with integer entries and determinant 1 is denoted $\mathrm{SL}_2(\mathbb{Z})$:

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ such that } a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}.$$

Prove that $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

(Hint: This is a little tricky. Let H be the subgroup generated by s and t. Given a matrix $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$, if suffices to show that you can obtain the identity by multiplying m by suitably chosen elements of H. Prove that $\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix}$ are in H, and note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b - qa \\ c & d - qc \end{pmatrix}$$

and

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} = \begin{pmatrix} a - qb & b \\ c - qd & d \end{pmatrix}.$$

Note that if c and d are both nonzero, one of these two operations may be used to decease the absolute value of one of them. Argue that suitable applications of these operations reduce to the case in which $c = 0$ or $d = 0$. Prove directly that $m \in H$ in that case.) [7.5]

∎ SOLUTION Let $U_q = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}$ and $L_q = \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix}$. Since, as can be proven by induction, $t^q = \begin{pmatrix} 1 & q \\ 0 & 1 \end{pmatrix}$, $U_q \in H$ for every integer q. Moreover, since $s^2 = -I_2$ and $s^4 = I_2$, by a straight forward calculation, it follows that $sts^{-1} = L_1$. Since $L_q \cdot L_1 = L_{q+1}$ we conclude by induction that $L_q \in H$ for every positive q. Furthermore, since $L_{-q}L_q = I_2$, then $L_q \in H$ for every integer q. Now, given any matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in

We can define the complex numbers using 2×2 real matrices. In this construction, s represents the imaginary number i.

$\mathrm{SL}_2(\mathbb{Z})$, let initially $A_0 = A$ and suppose without loss of generality $c \geq d$. Then we proceed by the Euclidean Algorithm. Let q_1 be the quotient of the division of c by d. If $A_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = L_{q_1} A_0$, then $c_1 = r_1 \leq d = d_1$. Now we divide d_1 by c_1, and proceed in this way. By Bézout's Theorem, $\gcd(c, d) = 1$, and by the Euclidean Algorithm, there exists n such that the n-th rest is $\gcd(c, d) = 1$ and the $(n+1)$-th remainder is 0, therefore the matrix A_{n+1} is such that $c_{n+1} = 0$ and $d_{n+1} = 1$, or the other way around. If $c_{n+1} = 0$, using the fact that $a_{n+1}d_{n+1} - b_{n+1}c_{n+1} = 1$, we conclude $a_{n+1} = 1$ and

$$A_{n+1} = \begin{pmatrix} 1 & b_{n+1} \\ 0 & 1 \end{pmatrix} \in H.$$

If $d_{n+1} = 0$, using the same identity we conclude $b_{n+1} = -1$ and

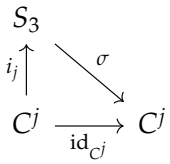
$$A_{n+1} = \begin{pmatrix} a_{n+1} & -1 \\ 1 & 0 \end{pmatrix}.$$

Since $s^3 A_{n+1} = \begin{pmatrix} 1 & 0 \\ -a_{n+1} & 1 \end{pmatrix} \in H$, out initial matrix A belongs to H, as we desired to prove. ∎

EXERCISE 6.11 Since direct sums are coproducts in Ab, the classifications theorem for abelian groups mentioned in the text says that every finitely generated *abelian group* is a coproduct of cyclic groups in Ab. The reader may be tempted to conjecture that every finitely generated *group* is a coproduct *in* Grp. Show that this is not the case by proving that S_3 is not a coproduct of cyclic groups.

∎ SOLUTION Suppose that S_3 satisfies the universal property of a coproduct of cyclic groups. That is, there exist morphisms i_j from some cyclic group (lets denote it by C^j) to S_3. By the universal property, there exists a unique morphism $\sigma : S_3 \to C^j$ such that the diagram

We emphasize that C^j is the j-th element of a family of cyclic groups. It is *not* C_j for some integer j.



commutes. In other words, such that $\mathrm{id}_{C^j} = \sigma i_j$. The fact that id_{C^j} is surjective then implies that so is σ. That is, $|C^j| \leq 6$ for all j.

By Proposition 4.1, for all $g \in S_3$, the order of $\sigma(g)$ divides $|g|$. Since S_3 has elements of order 1, 2, and 3, the order of $\sigma(g)$ can only be one of those 3 numbers. As σ is surjective, it follows that C^j is either equal to the trivial group, C_2 or C_3.

Now, S_3 having a C_3 as a factor in the coproduct implies that there is a injective morphism i and surjective morphism φ such that

$$C_3 \xrightarrow{i} S_3 \xrightarrow{\varphi} C_3$$

is equal to the identity. But there is no surjective morphism $S_3 \to C_3$. In fact, recall that $S_3 = \{e, x, y, xy, y^2, xy^2\}$ is the group generated by x, y such that $x^2 = e$, $y^3 = e$ and $yx = xy^2$. By Proposition 4.1, the order of $\varphi(x)$ divides 2. Since C_3 has no element of order 2, $\varphi(x) = 0$. Similarly, $\varphi(xy) = \varphi(xy^2) = 0$. It follows that $\varphi(y) = \varphi(x \cdot xy) = 0$ and thus φ is not surjective.

Lastly, lets suppose S_3 is a coproduct of n copies of C_2 and m copies of the trivial group. (If n or m are infinite, the argument is analogous.) Then, by the universal property of coproducts, the morphisms $S_3 \to S_3$ are in bijection with families of n morphisms $C_2 \to S_3$ and m morphisms $\{e\} \to S_3$. Since there are 4 possibilities for the former and 1 for the latter, we conclude that there are $4^n \cdot 1^m$ morphisms from S_3 to itself.

Since there are exactly 10 morphisms from S_3 to itself, this shows that our assumption was false and ends the solution. (The reader can verify this by observing that if φ is a morphism from S_3 to itself, Proposition 4.1 implies that $\varphi(x)$ can only be e, x, xy or xy^2. Also, $\varphi(y)$ can only be e, y or y^2. It suffices then to see which of those functions are homomorphisms.) ∎

Remark. As we said in the remark after Exercise 3.7, the elements of the free product $G * H$ are words of the form

$$g_1 h_1 g_2 h_2 \dots g_k h_k.$$

It then follows that the coproduct of two non-trivial groups is infinite. Hence the situation is as bad as it can possibly be: no non-trivial finite group is the coproduct of cyclic groups.

EXERCISE 6.12 Let m, n be positive integers, and consider the subgroup $\langle m, n \rangle$ of $\mathbb{Z}$ they generate. By Proposition 6.9,

$$\langle m, n \rangle = d\mathbb{Z}$$

for some positive integer d. What is d, in relation to m, n?

PROPOSITION 6.9 Let $G \subseteq \mathbb{Z}$ be a subgroup. Then $G = d\mathbb{Z}$ for some $d \geq 0$.

∎ SOLUTION Let $G = \langle m, n \rangle = d\mathbb{Z}$. Since $m, n \in G$, d divides both of them. On the other hand, since $d \in G$, there are $a, b \in \mathbb{Z}$ such that $d = am + bn$. Thus, every common divisor of m and n must divide d and so is less than or equal to d. We conclude that $d = \gcd(m, n)$. ∎

EXERCISE 6.13

■ SOLUTION A ■

EXERCISE 6.14 ▷ If m is a positive integer, denote $\phi(m)$ the number of positive integers $r \leq m$ that are *relatively primes* to m (that is, for which the gcd of r and m is 1); this is called *Euler's ϕ- (or 'totient') function*. For example, $\phi(12) = 4$. In other words, $\phi(m)$ is the order of the group $(\mathbb{Z}/m\mathbb{Z})^*$; cf. Proposition 2.6.

Put together the following observations:

- $\phi(m) =$ the number of generators of C_m,
- every element of C_n generates a subgroup of C_n.
- the discussion following Proposition 6.11 (in particular, every subgroup of C_n is isomorphic to C_m for some $m \mid n$),

to obtain a proof of the following formula

$$\sum_{m>0,\, m|n} \phi(m) = n.$$

(For example, $\phi(1) + \phi(2) + \phi(3) + \phi(4) + \phi(6) + \phi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$.) [4.14, §6.4, 8.15, V.6.8, §VII.5.2]

■ SOLUTION As he says, after Proposition 6.11, there is a bijection between the set of all subgroups of $\mathbb{Z}/n\mathbb{Z}$ and the set of positive divisors of n. Furthermore, observe that for each $m \mid n$, an element $a \in \langle [m]_n \rangle$ is a generator if and only if $\gcd(a, m) = 1$, therefore there are $\phi(m)$ generators. If we count the pairs $(a, \langle [m]_n \rangle)$ for which a generates $\langle [m]_n \rangle$, on the one hand for each $a \in C_n$, there exists one and only one such subgroup; on the other for each positive $m \mid n$, there exists $\phi(m)$ generators, from where we conclude

$$\sum_{m>0,\, m|n} \phi(m) = n,$$

the desired formula. ■

EXERCISE 6.15 ▷ Prove that if a group homomorphism $\varphi : G \to G'$ has a left-inverse, that is, a group homomorphism $\psi : G' \to G$ such that $\psi \circ \varphi = \mathrm{id}_G$, then φ is a monomorphism. [§6.5, 6.16]

■ SOLUTION For all groups Z and all homomorphisms α', α'' from Z to G,

$$\begin{aligned} \varphi \circ \alpha' = \varphi \circ \alpha'' &\implies (\psi \circ \varphi) \circ \alpha'' = (\psi \circ \varphi) \circ \alpha'' \\ &\implies \mathrm{id}_G \circ \alpha' = \mathrm{id}_G \circ \alpha'' \\ &\implies \alpha' = \alpha'', \end{aligned}$$

so φ is a monomorphism. ■

EXERCISE 6.16 ▷ Counterpart to Exercise 6.15: the homomorphism $\varphi : \mathbb{Z}/3\mathbb{Z} \to S_3$ given by

$$\varphi([0]) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \varphi([1]) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \varphi([2]) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

is a monomorphism; show that it has *no* left-inverse in Grp. (Knowing about *normal* subgroups will make this problem particularly easy.) [§6.5]

■ SOLUTION Lets suppose that there exists a morphism $\psi : S_3 \to \mathbb{Z}/3\mathbb{Z}$ such that $\psi \circ \varphi = \mathrm{id}_{\mathbb{Z}/3\mathbb{Z}}$. Using the notation of §2.1, this implies that

$$\psi(e) = [0], \quad \psi(y) = [1], \quad \psi(y^2) = [2].$$

By Proposition 4.1, the order of $\psi(x)$ has to divide 2, the order of x. The same is valid for xy and xy^2, the other elements of order 2. Since $\mathbb{Z}/3\mathbb{Z}$ has no elements of order 2, this implies that $\psi(x) = \psi(xy) = \psi(xy^2) = [0]$. However, ψ is not a homomorphism as $\psi(y) = \psi(x \cdot xy) \neq \psi(x) + \psi(xy)$. ■

Remark. Since $\psi \circ \varphi = \mathrm{id}_{\mathbb{Z}/3\mathbb{Z}}$ and identities are bijective, this implies that ψ is surjective. But then $\ker \psi$ should be a normal subgroup of S_3 with 2 elements, which does not exist.

7 QUOTIENT GROUPS

EXERCISE 7.1

■ SOLUTION A ■

EXERCISE 7.2 Is the *image* of a group homomorphism necessarily a *normal* subgroup of the target?

Trivially, every inclusion is an homomorphism. Since normal groups are scarce, this phenomenon is quite rare.

■ SOLUTION No. Consider, for example the function $\varphi\colon C_2 \to S_3$ defined by $\phi(i) = x^i$. Its image is the set subgroup $\langle x \rangle$, which is not normal, since $yxy^{-1} = xy^2y^{-1} \notin \langle x \rangle$. ■

EXERCISE 7.3 ▷ Verify that the equivalent conditions for normality given in §7.1 are indeed equivalent. [§7.1]

■ SOLUTION Let G be a group and $N \subseteq G$ be a subgroup. We will prove that the following conditions are equivalent:

(1) $gng^{-1} \in N$ for all $g \in G$ and $n \in N$;

(2) $gNg^{-1} = N$ for all $g \in G$;

(3) $gNg^{-1} \subseteq N$ for all $g \in G$;

(4) $gN = Ng$ for all $g \in G$;

(5) $gN \subseteq Ng$ for all $g \in G$.

(1) $\implies$ (2). If $x \in gNg^{-1}$, there exists $n \in N$ such that $x = gng^{-1}$. By condition (1), $x \in N$, so $gNg^{-1} \subseteq N$. On the other hand, if $y \in N$, condition (1) implies that there exists $n' \in N$ such that $g^{-1}y(g^{-1})^{-1} = g^{-1}yg = n'$, that is, $y = gn'g^{-1} \in gNg^{-1}$ and the other inclusion is also true. Thus, $gNg^{-1} = N$ for all $g \in G$.

(2) $\implies$ (3). Trivial.

(3) $\implies$ (4). If $x \in gN$, there exists $n \in N$ such that $x = gn$. By condition (3), $gng^{-1} = n'$ for some $n' \in N$, so $x = gn = n'g \in Ng$ and $gN \subseteq Ng$. On the other hand, if $y \in Ng$, there exists $m \in N$ such that $y = mg$. Condition (3) implies that $g^{-1}m(g^{-1})^{-1} = g^{-1}mg = m'$ for some $m' \in N$, thus, $y = mg = gm' \in gN$ and $Ng \subseteq gN$. Therefore, $gN = Ng$ for all $g \in G$.

(4) $\implies$ (5). Trivial.

(5) $\implies$ (1). If $g \in G$ and $n \in N$, condition (5) implies that there exists $n' \in N$ such that $gn = n'g$. Thus, $gng^{-1} = n' \in N$. ∎

EXERCISE 7.4 Prove that the relation defined in Exercise 5.10 on a free abelian group $F = F^{ab}(A)$ is compatible with the group structure. Determine the quotient $F/\sim$ as a better known group.

∎ SOLUTION Since F is abelian, we only have to verify that $f \sim f'$ implies $f + h \sim f' + h$ for all $h \in F$. This follows immediately from the fact that

$$(f + h) - (f' + h) = f - f'.$$

Now, by Proposition 5.6,

$$\frac{F}{\sim} = \frac{F}{2F} \cong \frac{\mathbb{Z}^{\oplus A}}{2\mathbb{Z}^{\oplus A}},$$

where $2F := \{2f \mid f \in F\}$ and similarly for $2\mathbb{Z}^{\oplus A}$. Finally, I affirm that

$$\frac{\mathbb{Z}^{\oplus A}}{2\mathbb{Z}^{\oplus A}} \cong \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^{\oplus A}.$$

For this, we will need Corollary 8.2, which is famously known as *the first isomorphism theorem*. Let $\varphi : \mathbb{Z}^{\oplus A} \to (\mathbb{Z}/2\mathbb{Z})^{\oplus A}$ be such that

$$\varphi(f)(a) = f(a) \mod 2$$

for all $a \in A$ and $f \in \mathbb{Z}^{\oplus A}$. Clearly φ is a surjective group homomorphism with $2\mathbb{Z}^{\oplus A}$ as kernel. The result follows. ∎

This result simply says that if $\varphi : G \to G'$ is a surjective group homomorphism, then $G' \cong G/\ker\varphi$.

EXERCISE 7.5 ¬ Define an equivalence relation $\sim$ on $\mathrm{SL}_2(\mathbb{Z})$ by letting $A \sim A' \iff A' = \pm A$. Prove that $\sim$ is compatible with the group structure. The quotient $\mathrm{SL}_2(\mathbb{Z})/\sim$ is denoted by $\mathrm{PSL}_2(\mathbb{Z})$ and is called the *modular group*; it would be a serious contender in a contest for 'the most important group in mathematics', due to its role in algebraic geometry and number theory. Prove that $\mathrm{PSL}_2(\mathbb{Z})$ is generated by (the cosets of the) matrices

$$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

(You will not need to work very hard, if you use the result of Exercise 6.10) Note that the first has order 2 in $\mathrm{PSL}_2(\mathbb{Z})$, the second has order 3, and their product has infinite order. [9.14]

■ SOLUTION A ■

EXERCISE 7.6 Let G be a group, and let n be a positive integer. Consider the relation

$$a \sim b \iff (\exists g \in G) ab^{-1} = g^n.$$

- Show that in general $\sim$ is *not* an equivalence relation.
- Prove that $\sim$ is an equivalence relation if G is commutative, and determine the corresponding subgroup of G.

■ SOLUTION

- We will take the same example as in Exercise 6.5. We know that $S_3 = \{e, x, y, y^2, xy, xy^2\}$ where

  $$x = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ and } y = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

  If we fix $n = 3$, as in Exercise 6.5, we have that $H = \{g^3 \mid g \in G\} = \{e, x, xy, xy^2\}$. Note that $x \sim y^2$ and $y^2 \sim xy$ since $x(y^2)^{-1} = xy \in H$ and $y^2(xy)^{-1} = y^2xy = y(yx)y = y(xy^2)y = yx = xy^2 \in H$, but $x \not\sim xy$ because $x(xy)^{-1} = xxy = y \notin H$. Therefore, $\sim$ is not transitive and is not an equivalence relation.

- Suppose G is abelian. This relation is reflexive since $aa^{-1} = e_G = e_G^n$ for all $a \in G$. It is also symmetric: if $a \sim b$, there exists $g \in G$ such that $ab^{-1} = g^n$, thus, $ba^{-1} = (ab^{-1})^{-1} = (g^{-1})^n$ and $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, there are $g, h \in G$ such that $ab^{-1} = g^n$ and $bc^{-1} = h^n$, which implies that $ac^{-1} = (ab^{-1})(bc^{-1}) = g^n h^n = (gh)^n$ and so $a \sim c$, proving that $\sim$ is transitive. Note that transitivity follows from the commutativity of G. It is clear that the corresponding subgroup of G is the one presented in Exercise 6.5: $H = \{g^n \mid g \in G\}$. ■

EXERCISE 7.7 Let G be a group, n a positive integer, and let $H \subseteq G$ be a subgroup generated by all elements of order n in G. Prove that H is normal.

■ SOLUTION Given any element $h \in H$, there exist $a_1, \ldots, a_r$ such that $h = a_1 \cdots a_r$ and $|a_i| = n$. Using the notation from Exercise 4.8, for every $g \in G$,

$$\begin{aligned} g \cdot h \cdot g^{-1} &= \gamma_g(a_1 \cdots a_r) \\ &= \gamma_g(a_1) \cdots \gamma_g(a_r). \end{aligned}$$

Since $|\gamma_g(a_i)| = |a_i| = n$, then ghg^{-1} belongs to H. ■

EXERCISE 7.8 Prove Proposition 7.6. [§7.3]

PROPOSITION 7.6 If H is any subgroup of a group G, the relation $\sim_L$ defined by

$$(\forall a, b \in G) : a \sim_L b \iff a^{-1}b \in H$$

is an equivalence relation satisfying (†).

See the next exercise to remember what is (†), if needed.

■ SOLUTION Let's prove $\sim_L$ is an equivalence relation. Since H is a subgroup of G, $a^{-1} = e_G \in H$ for all $a \in G$ and $\sim_L$ is reflexive. If $a \sim_L b$, then $a^{-1} \in H$ and $b^{-1} = (a^{-1}b)^{-1} \in H$, thus $b \sim_L a$ and the relation is also symmetric. Finally, if $a \sim_L b$ and $b \sim_L c$, then $a^{-1}b, b^{-1}c \in H$ and $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$, so $a \sim_L c$ and $\sim_L$ is transitive. To prove that $\sim_L$ satisfies (†), note that

$$a \sim_L b \implies a^{-1}b = (ga)^{-1}(gb) \in H \implies ga \sim_L gb$$

for all $g \in G$. ■

EXERCISE 7.9 State and prove the 'mirror' statements of Propositions 7.4 and 7.6, leading to the description of relations satisfying (††).

PROPOSITION 7.4 Let $\sim$ be an equivalence relation on a group G, satisfying (†). Then

- the equivalence class of e_G is a subgroup H of G; and
- $a \sim b \iff a^{-1}b \in H \iff aH = bH$.

PROPOSITION 7.6 If H is any subgroup of a group G, the relation $\sim_L$ defined by

$$(\forall a, b \in G) : a \sim_L b \iff a^{-1}b \in H$$

is an equivalence relation satisfying (†).

Let G be a group and $\sim$ an equivalence relation on G. Then, the conditions (†) and (††) are given by

$$(\forall g \in G) : \ a \sim b \implies ga \sim gb \tag{†}$$

$$(\forall g \in G) : \ a \sim b \implies ag \sim bg \tag{††}$$

■ SOLUTION The 'mirror' statement of Proposition 7.4 is:

Let $\sim$ be an equivalence relation on a group G, satisfying (††). Then

- the equivalence class of e_G is a subgroup H of G; and
- $a \sim b \iff ab^{-1} \in H \iff Ha = Hb$.

The proof is very similar to the one given for Proposition 7.4.

Let $H \subseteq G$ be the equivalence class of the identity; $H \neq \emptyset$ as $e_G \in H$. For $a, b \in H$, we have $e_G \sim b$ and hence $b^{-1} \sim e_G$ (applying (††), multiplying on the right by b^{-1}). We also have that $ab^{-1} \sim b^{-1}$ (by (††) again, multiplying $a \sim e_G$ on the right by b^{-1}) and hence

$$ab^{-1} \sim b^{-1} \sim e_G$$

by the transitivity of $\sim$. This shows that $ab^{-1} \in H$ for all $a, b \in H$, proving that H is a subgroup (by Proposition 6.2).

Next, assume $a, b \in G$ and $a \sim b$. Multiplying on the right by b^{-1}, (††) implies $ab^{-1} \sim e_G$, that is, $ab^{-1} \in H$. Since H is closed under the operation, this implies $Hab^{-1} \subseteq H$, hence $Ha \subseteq Hb$; as $\sim$ is symmetric, the same reasoning gives $Hb \subseteq Ha$; and hence $Ha = Hb$. Thus, we have proved

$$a \sim b \implies ab^{-1} \in H \implies Ha = Hb.$$

Finally, assume $Ha = Hb$. Then $a = ae_G \in Hb$, and hence $ab^{-1} \in H$. By definition of H, this means $ab^{-1} \sim e_G$. Multiplying on the right by b shows (by (††) again) that $a \sim b$, completing the proof.

The 'mirror' statement of Proposition 7.6 is:

If H is any subgroup of a group G, the relation $\sim_R$ defined by

$$(\forall a, b \in G) : \ a \sim_R b \iff ab^{-1} \in H$$

is an equivalence relation satisfying (††).

The proof is analogous to the one given in Exercise 7.8. ■

EXERCISE 7.10 ¬ Let G be a group, and $H \subseteq G$ a subgroup. With notation as in Exercise 6.7, show that H is normal in G if and only if $\forall \gamma \in \mathrm{Inn}(G)$, $\gamma(H) \subseteq H$.

Conclude that if H is normal in G, then there is an interesting homomorphism $\mathrm{Inn}(G) \to \mathrm{Aut}(H)$. [8.25]

■ SOLUTION The first part is just the third condition for normality proved in Exercise 7.3.

If H is normal in G, this implies that $\gamma|_H$ is an automorphism of H for all $\gamma \in \mathrm{Inn}(G)$. In other words, $\gamma \mapsto \gamma|_H$ is the desired homomorphism from $\mathrm{Inn}(G)$ to $\mathrm{Aut}(G)$. ■

EXERCISE 7.11 ▷ Let G be a group, and let $[G,G]$ be the subgroup of G generated by all elements of the form $aba^{-1}b^{-1}$. (This is the *commutator* subgroup G; we will return to it in §IV.3.3.) Prove that $[G,G]$ is normal in G. (Hint: With notation as in Exercise 4.8, $g \cdot aba^{-1}b^{-1} \cdot g^{-1} = \gamma_g(aba^{-1}b^{-1})$.) Prove that $G/[G,G]$ is commutative. [7.12, §IV.3.3]

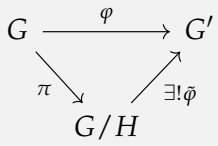
■ SOLUTION With the notation of Exercise 4.8, observe that, given $aba^{-1}b^{-1} \in [G,G]$, and $g \in G$, then

$$\begin{aligned} g \cdot aba^{-1}b^{-1} \cdot g^{-1} &= \gamma_g(aba^{-1}b^{-1}) \\ &= \gamma_g(a)\gamma_g(b)\gamma_g(a)^{-1}\gamma_g(b)^{-1} \in [G,G]. \end{aligned}$$

Furthermore, since $a^{-1}b^{-1}ab \in [G,G]$, then $[ba] = [ba(a^{-1}b^{-1}ab)] = [ab]$ for any $a, b \in G$, and $G/[G,G]$ is commutative. ■

EXERCISE 7.12 ▷ Let $F = F(A)$ be a free group, and let $f : A \to G$ be a set function from the set A to a *commutative* group G. Prove that f induces a unique homomorphism $F/[F,F] \to G$, where $[F,F]$ is the commutator subgroup of F defined in Exercise 7.11. (Use Theorem 7.12.) Conclude that $F/[F,F] \cong F^{ab}(A)$. (Use Proposition I.5.4.) [§6.4, 7.13, VI.1.20]

THEOREM 7.12 Let H be a normal subgroup of a group G. Then for every group homomorphism $\varphi : G \to G'$ such that $H \subseteq \ker \varphi$ there exists a unique group homomorphism $\tilde{\varphi} : G/H \to G'$ so that the diagram



commutes.

PROPOSITION 7.7 Let C be a category.

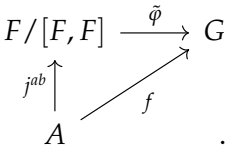
- If I_1, I_2 are both initial objects in C, then $I_1 \cong I_2$.
- If F_1, F_2 are both final objects in C, then $F_1 \cong F_2$.

Further, these isomorphisms are uniquely determined.

■ SOLUTION Let $j : A \to F$ be the inclusion of A in F. By the universal property of free groups, there exists a unique homomorphism $\varphi : F \to G$ such that $f = \varphi j$. Note that, since G is abelian,

$$\begin{aligned}\varphi(aba^{-1}b^{-1}) &= \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1} \\ &= (\varphi(a)\varphi(a)^{-1})(\varphi(b)\varphi(b)^{-1}) = e_G\end{aligned}$$

for all $a, b \in F$, so $[F,F] \subseteq \ker\varphi$. By Exercise 7.11, $[F,F]$ is a normal subgroup of F, so Theorem 7.12 implies that there exists a unique homomorphism $\tilde{\varphi} : F/[F,F] \to G$ such that $\varphi = \tilde{\varphi}\pi$, where $\pi : F \to F/[F,F]$ is the canonical projection to the quotient. Let $j^{ab} = \pi j$. It follows that $f = \varphi j = (\tilde{\varphi}\pi)j = \tilde{\varphi}(\pi j) = \tilde{\varphi} j^{ab}$, so $\tilde{\varphi}$ commutes the diagram



Moreover, it is the unique homomorphism that does this. Indeed, if $\sigma : F/[F,F] \to G$ is such that $f = \sigma j^{ab} = (\sigma\pi)j$, the uniqueness of φ and $\tilde{\varphi}$ implies that $\varphi = \sigma\pi$ and, thus, $\sigma = \tilde{\varphi}$, as desired. Again by Exercise 7.11, $F/[F,F]$ is abelian, so we conclude by Proposition I.5.4 that $F/[F,F] \cong F^{ab}(A)$ because both of them satisfy the universal property for free abelian groups. ■

EXERCISE 7.13 ¬ Let A, B be sets and $F(A), F(B)$ the corresponding free groups. Assume that $F(A) \cong F(B)$. If A is finite, prove that B is also and $A \cong B$. (Use Exercise 7.12 to upgrade Exercise 5.10.) [5.10, VI.1.20]

■ SOLUTION Since $F(A) \cong F(B)$, by Exercise 7.12 we have that

$$F^{ab}(A) \cong \frac{F(A)}{[F(A),F(B)]} \cong \frac{F(B)}{[F(B),F(B)]} \cong F^{ab}(B).$$

Then Exercise 5.10 implies the result. ■

EXERCISE 7.14 Let G be a group. Prove that $\mathrm{Inn}(G)$ is a *normal* subgroup of $\mathrm{Aut}(G)$.

■ SOLUTION A ■

EXERCISE 8.1 If a group H may be realized as a subgroup of two groups G_1 and G_2 and if

$$\frac{G_1}{H} \cong \frac{G_2}{H},$$

does it follows that $G_1 \cong G_2$? Give a proof or a counterexample.

■ SOLUTION Observe that C_3 may be realized as a subgroup of S_3 (as the group $\langle y \rangle$) and as a subgroup of C_6 (as the group $\langle [2]_6 \rangle$). Since $x^2 = e$ and $yx = xy^2$, this subgroup is normal, and since C_6 is commutative, C_3 is normal in C_6. Every pair of subgroups with two elements are isomorphics, therefore

$$\frac{S_3}{C_3} \cong \frac{C_6}{C_3}.$$

However, C_6 and S_3 are not isomorphic. ■

EXERCISE 8.2 ¬ Extend Example 8.6 as follows. Suppose G is a group and $H \subseteq G$ is a *subgroup of index* 2, that is, such that there are precisely two (say, left-) cosets of H in G. Prove that H is normal in G. [9.11, IV.1.16]

■ SOLUTION Let $g \in G$. We want to prove that $gH = Hg$. If $g \in H$, this is obvious so we suppose $g \notin H$. Since there are exactly two left-cosets of H in G, they ought to be H and gH. But the cosets partition G, so we have that $gH = G \setminus H$. Now, we affirm that there are also exactly 2 right-cosets. This then implies that they are H and $Hg = G \setminus H$. The result follows.

We prove something a little bit stronger: if G is any group and H is a subgroup of G, then H has the same number of left- and right-cosets. In fact, the function

$$\varphi : gH \mapsto Hg^{-1}$$

is well-defined and a bijection from $G/\sim_L$ to $G/\sim_R$. If $g_1H = g_2H$, then $g_1^{-1}g_2 \in H$ and so $Hg_1^{-1} = Hg_2^{-1}$, which means that φ is well-defined. It is clearly surjective and it is injective since $Hg_1^{-1} = Hg_2^{-1}$ implies $g_1^{-1}g_2 \in H$ and then $H = g_1^{-1}g_2H$. Multiplying by g_1 on both sides we conclude that φ is injective. ■

EXERCISE 8.3 Prove that every finite group is finitely presented.

■ SOLUTION Let G be a finite group. Considering $A = G$ just as a set, there exists a (unique) homomorphism $\varphi : F(A) \to G$ that takes each letter to its correspondent element of G. Since φ is surjective, Collorary 8.2 implies that $G \cong F(A)/\ker\varphi$. We just need to show that there exist a finite set of words in $\ker\varphi$ such that $\ker\varphi$ is the smallest normal subgroup of $F(A)$ containing it. To do so, we will find the multiplicative table of G inside $\ker\varphi$. Take $\mathscr{R}$ as the set all

words of the form abc^{-1}, where a and b are in A or A' and $c \in A$ is the letter corresponding to $\varphi(ab)$. Note that, if we consider a and b as elements of G, c is their product. For example, if we take C_2 and label its elements by $C_2 = \{e, f\}$, then we have

$$\begin{aligned}\mathscr{R} = \{&eee^{-1}, eff^{-1}, fef^{-1}, ffe^{-1},\\ &e^{-1}ee^{-1}, e^{-1}ff^{-1}, f^{-1}ef^{-1}, f^{-1}fe^{-1},\\ &ee^{-1}e^{-1}, ef^{-1}f^{-1}, fe^{-1}f^{-1}, ff^{-1}e^{-1},\\ &e^{-1}e^{-1}e^{-1}, e^{-1}f^{-1}f^{-1}, f^{-1}e^{-1}f^{-1}, f^{-1}f^{-1}e^{-1}\}.\end{aligned}$$

After reduction, there will be some repeated words, but we know that $|\mathscr{R}| \leq |A \cup A'|^2 = 4|G|^2$, so $\mathscr{R}$ is finite. By construction, $\mathscr{R} \subseteq \ker \varphi$. We claim that $\ker \varphi = \langle \mathscr{R} \rangle$. The inclusion $\langle \mathscr{R} \rangle \subseteq \ker \varphi$ is straightforward. For the other one, take a word $r \in \ker \varphi$. We will prove that $r \in \langle \mathscr{R} \rangle$ by induction on the length of r. If r is the empty word, it is immediate. If r consists of only one letter, we must have $r = e = eee^{-1}$ or $r = e^{-1} = ee^{-1}e^{-1}$ and so $r \in \langle \mathscr{R} \rangle$. Now, suppose that every word with n letters or less that is in $\ker \varphi$ is also in $\langle \mathscr{R} \rangle$, for some $n \geq 1$, and assume that r has $n+1$ letters. If $r = g_1 g_2 \cdots g_{n+1}$ and the product of the corresponding elements of g_1 and g_2 in G corresponds to the letter g, we have that

$$r = g_1 g_2 g_3 \cdots g_{n+1} = (g_1 g_2 g^{-1}) \cdot (g g_3 \cdots g_{n+1}).$$

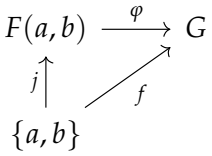
Reduce $g g_3 \cdots g_{n+1}$ to the word s, which has n or less letters. Since $r, g_1 g_2 g^{-1} \in \ker \varphi$, $s \in \ker \varphi$ and, by the inductive hypothesis, $s \in \langle \mathscr{R} \rangle$. Finally, since $g_1 g_2 g^{-1} \in \langle \mathscr{R} \rangle$, we conclude that $r \in \langle \mathscr{R} \rangle$, as desired. Therefore, $\ker \varphi = \langle \mathscr{R} \rangle$ and it follows that G is finitely presented since it admits the presentation $(A|\mathscr{R})$ where both A and $\mathscr{R}$ are finite. ∎

EXERCISE 8.4

∎ SOLUTION A ∎

EXERCISE 8.5 Let a, b be distinct elements of order 2 in a group G, and assume that ab has finite order $n \geq 3$. Prove that the subgroup generated by a and b in G is isomorphic to the dihedral group D_{2n}. (Use the previous exercise.)

∎ SOLUTION Let H be the subgroup generated by a and b, and $\varphi\colon \{a, b\} \to G$ be defined by $f(a) = a$ and $f(b) = b$. By the universal property of free groups, there exists a unique homomorphism φ such that the diagram



commutes. Moreover, since $n > 2$, a and b do not commute, and since $a^2 = b^2 = (ab)^n = e$, the kernel of this homomorphism is the smallest normal subgroup containing a^2, b^2 and $(ab)^n$, from where we conclude, using Corollary 8.2, $H \cong (a, b \mid a^2, b^2, (ab)^n) \cong D_{2n}$. ∎

EXERCISE 8.6 ¬ Let G be a group, and let A be a set of generators for G; assume A is finite. The corresponding *Cayley graph* is a directed graph whose set of vertices is in one-to-one correspondence with G, and two vertices g_1, g_2 are connected by an edge if $g_2 = g_1 a$ for an $a \in A$; this edge may be labeled a and oriented from g_1 to g_2. For example, the graph drawn in Example 5.3 for the free group $F(\{x, y\})$ on two generators x, y is the corresponding Cayley graph (with the convention that horizontal edges are labeled x and point to the right and vertical edges are labeled y and point up).

Prove that if a Cayley graph of a group is a tree, then the group is free. Conversely, prove that free groups admit Cayley graphs that are trees. [§5.3, 9.15]

∎ SOLUTION A tree is a graph in which any two vertices are connected by *exactly one* path. In this case, there cannot be repeated vertices on the path and, therefore, there are not repeated edges either. With this definition, let's prove each implication separately:

Other definition states that a tree is a connected acyclic graph, that is, there is a path between any two vertices and there is no cycles (loops). Note that these two definitions are equivalent.

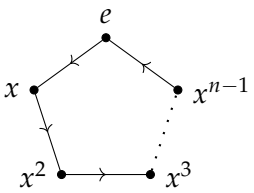
($\Longrightarrow$) Let G be a group with a set of generators A and whose Cayley graph is a tree. We claim that $G \cong F(A)$. Note that each path in this graph induces a reduced word in $F(A)$ corresponding to the juxtaposition of the labels of the edges (or the inverse of the label, if the edge is traversed in the opposite orientation). Conversely, each reduced word also induces a path in the graph as long as we fix a starting point. Thus, define $\varphi : G \to F(A)$ by letting $\varphi(g)$ be the word induced by the path from e_G to g, for all $g \in G$. Since the graph is a tree, φ is well-defined. This function is a bijection, since it has the inverse $\psi : F(A) \to G$ where $\psi(r)$ is the end of the path induced by r starting from e_G. We just need to prove that φ preserves operation. Let $a, b \in G$ be arbitrary. By the definition of the Cayley graph, if we traverse the path induced by $\varphi(b)$ but starting from a, we end at ab. Thus, concatenating the paths induced by $\varphi(a)$ and $\varphi(b)$ (but starting from a), we get a *walk* (as called in graph theory) from e_G to ab that may not be a path, but it can be reduced to one as follows. Let r be the first repeated edge on the walk. It exists because otherwise the graph would contain a cycle. Furthermore, since the graph is a tree, it must repeat in the reverse orientation just after it appears for the first time. We may remove these edges and the correspondent vertex from the walk. After repeating this process sometimes, we will end with a path from e_G to ab, that corresponds to the word $\varphi(ab)$. But this matches exactly to how to reduce the word $\varphi(a)\varphi(b)$, as defined in Section 5. Therefore, it follows that $\varphi(ab) = \varphi(a)\varphi(b)$. We conclude that φ is an isomorphism and, thus, G is a free group.

($\Longleftarrow$) Let $G = F(A)$ be a free group, where A is a set. To construct the Cayley graph of G, we will use the corresponding letters for A in $F(A)$, which we may also denote by A for simplicity. This is the generalization of the graph presented in Example 5.3. If we label the edges as in the example, note that going through an edge labeled x corresponds to attach this letter at the end of the word, and going on the other direction corresponds to attach x^{-1}. Since every reduced word has a unique representation when written with letters of A and A', moving through an edge only attaches a new letter or removes the final one. Now, take two distinct words $r, s \in F(A)$ and let's prove that there is only one path between them on the graph. Let t be the largest word in common between r and s, starting from the first letter (t can be the empty word). To get from r to s without repeating vertices on the graph, we must remove the final letters of r one by one until we get to t. There is only one way to do that: multiply by the inverse of each final letter. If we did something else, the word would increase and we would eventually have to come back to a previous word, which is not allowed. After getting to t, we must attach the remaining letters of s one by one. Again, there is only one way to do that without repeating vertices. This process shows that there exists a unique path between r and s on the graph and, therefore, we conclude that this graph is indeed a tree. ∎

If we fix the empty word as the starting point of the tree, t is called the *lowest common ancestor* of r and s. The path described here corresponds to come back from r to t and then go to s.

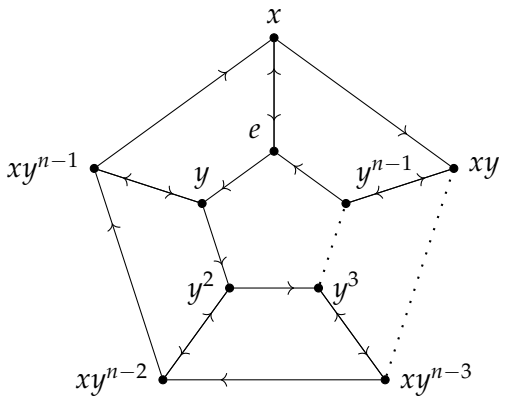
Here we present the Cayley graphs of some groups:

- C_n with set of generators $A = \{x\}$, where $|x| = n$.



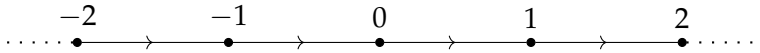
  This is a cycle of length n.

- D_{2n} with set of generators $A = \{x, y\}$, where $x^2 = e$, $y^n = e$ and $yx = xy^{-1}$.



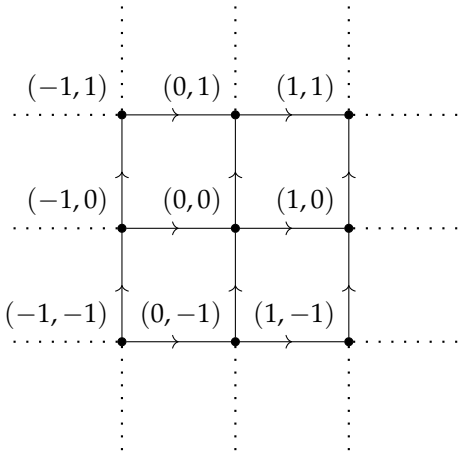
The edges at the inner and outer cycles represent multiplication by y, while the edges connecting these cycles represent multiplication by x.

- $\mathbb{Z}$ with set of generators $A = \{1\}$.



This is an infinite path. Note that it is a tree and that $\mathbb{Z} \cong F(\{1\})$.

- $\mathbb{Z} \times \mathbb{Z}$ with set of generators $A = \{(1,0),(0,1)\}$.



This is an infinite grid. Horizontal edges represent addition by $(1,0)$ and vertical edges represent addition by $(0,1)$.

- If G is a finite group and we take $A = G$ as the set of generators, the correspondent Cayley graph is the complete graph on $|G|$ vertices.

EXERCISE 8.7 ▷ Let $(A|\mathscr{R})$, resp., $(A'|\mathscr{R}')$, be a presentation for a group G, resp., G' (cf. §8.2); we may assume that A, A' are disjoint. Prove that the group $G * G'$ presented by

$$(A \cup A'|\mathscr{R} \cup \mathscr{R}')$$

satisfies the universal property for the *coproduct* of G and G' in Grp. (Use the universal properties of both free groups and quotients to construct natural homomorphisms $G \to G * G'$, $G' \to G * G'$.) [§3.4, §8.2, 9.14]

■ SOLUTION By Exercise 5.8, $F(A \cup A')$ is the coproduct $F(A) * F(A')$ in Grp. Thus, there exist natural morphisms

$$i : F(A) \to F(A \cup A') \qquad \text{and} \qquad i' : F(A') \to F(A \cup A').$$

Also, composing with the projection $\pi^* : F(A \cup A') \to G * G'$ we get morphisms

$$\pi^* i : F(A) \to G * G' \qquad \text{and} \qquad \pi^* i' : F(A') \to G * G'.$$

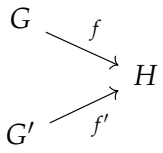
As Aluffi does in §8.2, we denote by R the smallest normal subgroup of $F(A)$ containing $\mathscr{R}$ and similarly for R'.

Now, since $R \subseteq \ker \pi^* i$ and $R' \subseteq \ker \pi^* i'$, the universal property of quotients gives us morphisms

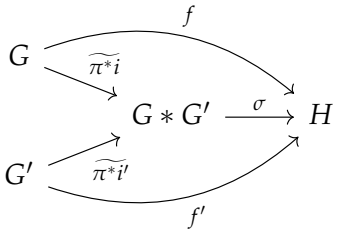
$$\widetilde{\pi^* i} : G \to G * G' \qquad \text{and} \qquad \widetilde{\pi^* i'} : G' \to G * G'$$

such that $\pi^* i = \widetilde{\pi^* i}\pi$ and $\pi^* i' = \widetilde{\pi^* i'}\pi'$, where $\pi : F(A) \to G$ and $\pi' : F(A') \to G'$ are the natural projections.

We ought to show that these morphisms work as the natural injections of the coproduct $G * G'$. In other words, we have to show that if H is any group and we have morphisms



then there exists a unique morphism $\sigma : G * G' \to H$ such that the diagram



commutes. By composing with the projections π and π', we get morphisms

$$\pi f : F(A) \to H \qquad \text{and} \qquad \pi' f' : F(A') \to G'.$$

Thus, by the universal property of coproducts, we get a unique morphism

$$\sigma^* : F(A \cup A') \to H$$

such that $\sigma^* i = f\pi$ and $\sigma^* i' = f'\pi'$. Similarly as before, we have that $R \cup R' \subseteq \ker \sigma^*$ and then the universal property of quotients induces a unique morphism

$$\sigma : G * G' \to H$$

such that $\sigma^* = \sigma\pi^*$. Utilising all the commuting diagrams we have, it follows that

$$\sigma\widetilde{\pi^* i}\pi = f\pi \qquad \text{and} \qquad \sigma\widetilde{\pi^* i'}\pi' = f'\pi'.$$

Since the projections to the quotients are epimorphisms, the result follows. ∎

EXERCISE 8.8 ¬ (If you know about matrices (cf. Exercise 6.1).) 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. [VI.3.3]

■ SOLUTION A ■

EXERCISE 8.9 ¬ (Ditto.) Prove that $\mathrm{SO}_3(\mathbb{R}) \cong \mathrm{SU}(2)/\{\pm I_2\}$, where I_2 is the identity matrix. (Hint: It so happens that every matrix $\mathrm{SO}_3(\mathbb{R})$ can be written in the form

$$\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

where $a, b, c, d \in \mathbb{R}$ and $a^2+b^2+c^2+d^2 = 1$. Proving this fact is not hard, but at this stage you will probably find it computationally demanding. Feel free to assume this, and use Exercise 6.3 to construct a surjective homomorphism $\mathrm{SU}(2) \to \mathrm{SO}_3(\mathbb{R})$; compute the kernel of this homomorphism.)

If you know a little topology, you can now conclude that the fundamental group of $\mathrm{SO}_3(\mathbb{R})$ is C_2. [9.1, VI.1.3]

■ SOLUTION To simplify the computation a little bit, we will use the quaternions, which were introduced in the Remark after Exercise 6.3. By this exercise, we know that the matrices of $\mathrm{SU}(2)$ correspond to the quaternions of norm 1 (unit quaternions). We can also naturally identify the vectors of $\mathbb{R}^3$ with the so called pure quaternions, that is, quaternions with real part $a = 0$. A famous result is that every rotation in the 3-dimensional space is of the form

$$X \longmapsto ZXZ^{-1},$$

for some unit quaternion Z and for all pure quaternions X. Thus, we can define the surjective function $\varphi : \mathrm{SU}(2) \to \mathrm{SO}_3(\mathbb{R})$ that takes the unit quaternion Z and sends it to the matrix M_Z corresponding to the rotation given above. Note that, given two unit quaternions Y, Z, we have that $M_{YZ} = M_Y M_Z$. Indeed, this product of matrices corresponds to the composition of the rotations, so the resulting rotation is

$$X \longmapsto ZXZ^{-1} \longmapsto Y(ZXZ^{-1})Y^{-1} = (YZ)X(YZ)^{-1},$$

which corresponds to M_{YZ}, as desired. Therefore, φ is a surjective homomorphism.

In matrix form, let's show that φ sends

$$\begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix}$$

to

$$\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(ac+bd) \\ 2(ad+bc) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(ab+cd) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

for all $a, b, c, d \in \mathbb{R}$ such that $a^2 + b^2 + c^2 + d^2 = 1$. Let $Z = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ be a unit quaternion. If $X = a'\mathbf{1} + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$, it follows that the coordinates of ZX and $XZ^{-1} = X\overline{Z}$ are given by

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix} \begin{pmatrix} a' \\ b' \\ c' \\ d' \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \begin{pmatrix} a' \\ b' \\ c' \\ d' \end{pmatrix},$$

respectively. Thus, the matrix that represents the map $X \mapsto ZXZ^{-1}$ is given by the product of these two 4×4 matrices and so it is:

$$\begin{pmatrix} N(Z) & 0 & 0 & 0 \\ 0 & a^2 + b^2 - c^2 - d^2 & 2(bc - ad) & 2(ac + bd) \\ 0 & 2(ad + bc) & a^2 - b^2 + c^2 - d^2 & 2(cd - ab) \\ 0 & 2(bd - ac) & 2(ab + cd) & a^2 - b^2 - c^2 + d^2 \end{pmatrix}.$$

Since we are dealing only with pure quaternions, we conclude that

$$M_Z = \begin{pmatrix} a^2 + b^2 - c^2 - d^2 & 2(bc - ad) & 2(ac + bd) \\ 2(ad + bc) & a^2 - b^2 + c^2 - d^2 & 2(cd - ab) \\ 2(bd - ac) & 2(ab + cd) & a^2 - b^2 - c^2 + d^2 \end{pmatrix},$$

as desired.

Finally, let's show that $\mathrm{SO}_3(\mathbb{R}) \cong \mathrm{SU}(2)/\{\pm I_2\}$. To do so, we will compute $\ker \varphi$. Let $a, b, c, d \in \mathbb{R}$ be such that $a^2 + b^2 + c^2 + d^2 = 1$ and the corresponding matrix M_Z equals to the identity. This implies that

$$a^2 + b^2 - c^2 - d^2 = a^2 - b^2 + c^2 - d^2 = a^2 - b^2 - c^2 + d^2 = 1$$

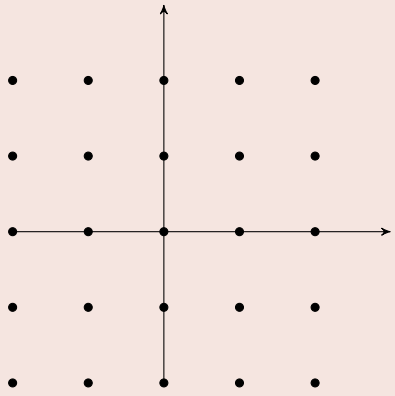
To find $\ker \varphi$, we could have found who are the unit quaternions in $Z(\mathbb{H})$, the center of $\mathbb{H}$. Since $Z(\mathbb{H}) = \mathbb{R}$, they are ± 1, which correspond to $\pm I_2$ in $\mathrm{SU}(2)$.

and, since $a^2 + b^2 + c^2 + d^2 = 1$,

$$c^2 + d^2 = b^2 + d^2 = b^2 + c^2 = 0,$$

so $b = c = d = 0$ and $a = \pm 1$. It follows that, if $M \in \ker \varphi$, then $M = \pm I_2$. Since I_2 and $-I_2$ are clearly in this kernel, we have that $\ker \varphi = \{\pm I_2\}$. Since φ is surjective, we conclude from Corollary 8.2 that $\mathrm{SO}_3(\mathbb{R}) \cong \mathrm{SU}(2)/\{\pm I_2\}$. ∎

EXERCISE 8.10 View $\mathbb{Z} \times \mathbb{Z}$ as a subgroup of $\mathbb{R} \times \mathbb{R}$:



Describe the quotient

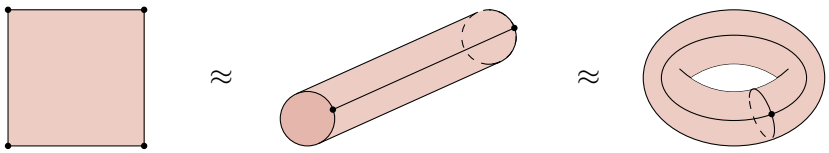
$$\frac{\mathbb{R} \times \mathbb{R}}{\mathbb{Z} \times \mathbb{Z}}$$

in terms analogous to those used in Example 8.7. (Can you 'draw a picture' of this group? Cf. Exercise I.1.6.)

■ SOLUTION Since S^1 has a group structure, one can naturally give $S^1 \times S^1$ a group structure. Each one represents a rotation in one plane. If we consider the transformation which maps (r, s) to the rotation by $2\pi r$ radians in the first plane and $2\pi s$ in the second, then the kernel of this transformation is $\mathbb{Z} \times \mathbb{Z}$, and we conclude

$$\frac{\mathbb{R} \times \mathbb{R}}{\mathbb{Z} \times \mathbb{Z}} \cong S^1 \times S^1 \left(\cong \frac{\mathbb{R}}{\mathbb{Z}} \times \frac{\mathbb{R}}{\mathbb{Z}} \right).$$

The group $\mathbb{T}^2 = S^1 \times S^1$ is called the *torus* (more generally, $\mathbb{T}^n = \underbrace{S^1 \times \cdots \times S^1}_{n \text{ times}}$ is the n-dimensional torus). It is possible to draw $\mathbb{T}^2$, as we have done in Exercise I.1.6,



We start with the square $[0, 1] \times [0, 1]$, and we "glue" its sides. ■

EXERCISE 8.11 (Notation as in Proposition 8.10.) Prove 'by hand' (that is, without invoking universal properties) that N is normal in G if and only if N/H is normal in G/H.

PROPOSITION 8.10 Let H be a normal subgroup of a group G, and let N be a subgroup of G containing H. Then N/H is normal in G/H if and only if N is normal in G, and in this case

$$\frac{G/H}{N/H} \cong \frac{G}{N}.$$

■ SOLUTION Suppose N is normal in G. We want to prove that, for all $g \in G$ and $n \in N$,

$$(gH)(nH)(gH)^{-1} \in N/H.$$

But this element is $gng^{-1}H$, which is in N/H by the normality of N.

Conversely, if N/H is normal in G/H,

$$(gH)(nH)(gH)^{-1} \in N/H,$$

for all $g \in G$ and $n \in N$. But this means precisely that $gng^{-1} \in N$. The result follows. ■

EXERCISE 8.12 (Notation as in Proposition 8.11.) Prove 'by hand' (that is, by using Proposition 6.2) that HK is a subgroup of G if H is normal.

PROPOSITION 8.2 A *nonempty* subset H of a group G is a subgroup if and only if

$$(\forall a, b \in H) : \ ab^{-1} \in H.$$

PROPOSITION 8.11 Let H, K be subgroups of a group G, and assume that H is normal in G. Then

- HK is a subgroup of G, and H is normal in HK;
- $H \cap K$ is normal in K, and

$$\frac{HK}{H} \cong \frac{K}{H \cap K}.$$

■ SOLUTION Firstly, note that $HK \neq \emptyset$ because it contains both H and K, which are nonempty. Now, let $a, b \in HK$ be arbitrary. There are $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $a = h_1k_1$ and $b = h_2k_2$. Since H is normal in G, there exists $h_3 \in H$ such that $h_3 = (k_1k_2^{-1})h_2^{-1}(k_1k_2^{-1})^{-1}$, that is, $k_1k_2^{-1}h_2^{-1} = h_3k_1k_2^{-1}$. Thus,

$$\begin{aligned} ab^{-1} &= (h_1k_1)(h_2k_2)^{-1} \\ &= h_1(k_1k_2^{-1}h_2^{-1}) \\ &= h_1(h_3k_1k_2^{-1}) \\ &= (h_1h_3)(k_1k_2^{-1}) \in HK \end{aligned}$$

and, by Proposition 6.2, HK is a subgroup of G. ■

EXERCISE 8.13

■ SOLUTION A ■

EXERCISE 8.14 Generalize the result of Exercise 8.13: if G is a group of order n and k is an integer relatively prime to n, then the function $g \mapsto g^k$ is surjective.

■ SOLUTION Let $a, b \in \mathbb{Z}$ such that $ak + bn = 1$. Given $g \in G$, since $g^n = e$, then $g = g^{ak+bn} = (g^a)^k \cdot (g^n)^b = (g^a)^k$ and g is in the image of the function. ■

EXERCISE 8.15 Let a, n be positive integers, with $a > 1$. Prove that n divides $\phi(a^n - 1)$, where ϕ is Euler's ϕ-function; see Exercise 6.14. (Hint: Example 8.15.)

■ SOLUTION Let $G = (\mathbb{Z}/(a^n - 1)\mathbb{Z})^*$. Since $(a^{n-1})a + (-1)(a^n - 1) = 1$, Exercise 2.13 implies that $\gcd(a, a^n - 1) = 1$, so $a \in G$. It is clear that $|a| = n$, thus, by Example 8.15, n divides $|G| = \phi(a^n - 1)$. ■

EXERCISE 8.16 Generalize Fermat's little theorem to congruences modulo arbitrary (that is, possibly nonprime) integers. Note that it is *not* true that $a^n \equiv a \mod n$ for all a and n: for example, 2^4 is not congruent to 2 modulo 4. *What* is true? (This generalization is known as *Euler's theorem*.)

■ SOLUTION Euler's theorem says that if n is a positive integer and a is relatively prime to n, then

$$a^{\phi(n)} \equiv 1 \mod n,$$

where ϕ is Euler's ϕ-function.

To prove this, let $G = (\mathbb{Z}/n\mathbb{Z})^*$. Since $\gcd(a, n) = 1$, $a \in G$. Let d be the order of a in G. By Lagrange's theorem (Example 8.15), $\phi(n) = dk$, where k is a positive integer. Then,

$$a^{\phi(n)} = (a^d)^k \equiv 1^k \equiv 1 \mod n.$$

This is the desired result. ■

EXERCISE 8.17 ▷ Assume G is a finite abelian group, and let p be a prime divisor of $|G|$. Prove that there exists and element in G of order p. (Hint: Let g be any element of G, and consider the subgroup $\langle g \rangle$; use the fact the fact that this group is cyclic to show that there is an element $h \in \langle g \rangle$ of *prime* order q. If $q = p$, you are done; otherwise, use the quotient $G/\langle h \rangle$ and induction.) [§8.5, 8.18, 8.20, §IV.2.1]

■ SOLUTION A ■

EXERCISE 8.18 Let G be an abelian group of order $2n$, where n is odd. Prove that G has *exactly one* element of order 2. (It has at least one, for example by Exercise 8.17. Use Lagrange's theorem to establish that it cannot have more than one.) Does the same conclusion hold if G is not necessarily commutative?

■ SOLUTION By Exercise 8.17, there exists an element $g \in G$ of order 2 because 2 is prime and it divides $|G| = 2n$. Let $H = \langle g \rangle = \{e_G, g\}$ be the subgroup generated by g. Since G is abelian, H is normal in G and we can take the quotient G/H. By Lagrange's theorem,

$$\left|\frac{G}{H}\right| = [G : H] = \frac{|G|}{|H|} = \frac{2n}{2} = n.$$

Suppose that there exists another element $g' \in G$ of order 2. Since $g' \notin H$ and $(g')^2 = e_G$, $g'H \neq e_G H$ and $(g'H)^2 = e_G H$, that is, $g'H$ is of order 2 in G/H. But Lagrange's theorem implies that 2 divides $|G/H| = n$, a contradiction since n is odd. Therefore, G has exactly one element of order 2.

Note that the hypothesis that G is commutative is necessary. For example, S_3 is of order $6 = 2 \cdot 3$ and it has three elements of order 2:

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

■

EXERCISE 8.19 Let G be a finite group, and let d be a proper divisor of $|G|$. Is it necessarily true that there exists an element of G with order d? Give a proof or a counterexample.

■ SOLUTION This is false even for commutative groups. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then $|G| = 4$, but there is no element of order 4. In fact, since $2a = 0$ for any $a \in \mathbb{Z}/2\mathbb{Z}$, then $2(a, b) = 0$ for any $(a, b) \in \mathbb{Z}/2\mathbb{Z}$. More generally, this happens for any product $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, for which $\gcd(n, m) > 1$. ■

EXERCISE 8.20 ▷ Assume G is a finite abelian group, and let d be a divisor of $|G|$. Prove that there exists a *subgroup* $H \subseteq G$ of order d. (Hint: induction; use Exercise 8.17.) [§IV.2.2]

■ SOLUTION We'll induct on the order of G. If $|G| = 1$, the result is trivial. Now, lets suppose that the theorem is true for all groups with order $< |G|$ and let p be a prime factor of d. By Exercise 8.17, there exists an element x of order p in G. The induction hypothesis implies that $G/\langle x \rangle$ has a subgroup of order d/p. Proposition 8.9 implies that this subgroup is of the form $H/\langle x \rangle$ for some subgroup H of G. This is the desired subgroup as it has order d. ■

EXERCISE 8.21 ▷ Let H, K be subgroups of a group G. Construct a bijection between the set of cosets hK with $h \in H$ and the set of left-cosets of $H \cap K$ in H. If H and K are finite, prove that

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

[§8.5]

■ SOLUTION A helpful observation here is that $h(H \cap K) = H \cap (hK)$ for all $h \in H$, so we can connect the cosets of $H \cap K$ in H and the cosets hK with $h \in H$ by intersection with H, as we will do soon. Before that, let's prove this equality. If $x \in h(H \cap K)$, there exists $y \in H \cap K$ such that $x = hy$. In particular, since $y \in H$ and $y \in K$, $x \in H$ and $x \in hK$, so $x \in H \cap (hK)$ and $h(H \cap K) \subseteq H \cap (hK)$. On the other hand, if $x' \in H \cap (hK)$, there exists $k \in K$ such that $x' = hk$. Therefore, $k = h^{-1}x' \in H$ so $k \in H \cap K$ and $x' \in h(H \cap K)$, proving the other inclusion.

More generally, a similar argument shows that $g(H \cap K) = (gH) \cap (gK)$, for all $g \in G$.

Let $X = \{hK | h \in H\}$. Define $f : X \to H/(H \cap K)$ by

$$f(hK) = h(H \cap K) = H \cap (hK)$$

for all $hK \in X$. Since distinct cosets of X are disjoint, it follows that f is injective. Furthermore, given $h(H \cap K) \in H/(H \cap K)$, it is immediate that $f(hK) = h(H \cap K)$, so f is also surjective. We conclude that f is a bijection between X and $H/(H \cap K)$.

Note that $HK = \bigcup_{h \in H} hK$. Therefore, if H and K are finite, we have that $|HK| = |X| \cdot |K|$ since the cosets are disjoint and $|hK| = |K|$ for all $h \in K$ by Lemma 8.13. By the bijection above and by Lagrange's theorem, it follows that

$$|HK| = |X| \cdot |K| = \left| \frac{H}{H \cap K} \right| \cdot |K| = \frac{|H| \cdot |K|}{|H \cap K|},$$

as desired. ■

EXERCISE 8.22

■ SOLUTION A ■

EXERCISE 8.23 ▷ Consider the subgroup

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

of S_3. Show that the cokernel of the inclusion $H \hookrightarrow S_3$ is trivial, although $H \hookrightarrow S_3$ is not surjective. [§8.6]

■ SOLUTION As we have seen in Exercise 7.2, H is not a normal group, and, even more, if N is a normal group containing H, then $y \in H$. Since x and y generates S_3, $N = S_3$ and the cokernel is trivial. ■

EXERCISE 8.24 ▷ Show that epimorphisms in Grp do not necessarily have right-inverses. [§I.4.2]

■ SOLUTION We will construct an epimorphism that does not have a right-inverse. Let $G = \mathbb{Z}/4\mathbb{Z}$ and $H = \{[0]_4, [2]_4\}$. Since G is commutative, H is a normal subgroup and we can take $\pi : G \to G/H$ as the canonical projection. It is an epimorphism in Set because it is surjective and, therefore, it is an epimorphism in Grp. However, π does not have a right-inverse. Indeed, if φ were a right-inverse for π, $\varphi([1]_4 H)$ would need to be $[1]_4$ or $[3]_4$, because $\pi^{-1}([1]_4 H) = \{[1]_4, [3]_4\}$. But then we get that $[0]_4 = \varphi([0]_4 H) = \varphi([2]_4 H) = 2\varphi([1]_4 H) = [2]_4$, a contradiction. ■

EXERCISE 8.25 Let H be a commutative normal subgroup of G. Construct an interesting homomorphism from G/H to $\mathrm{Aut}(H)$. (Cf. Exercise 7.10.)

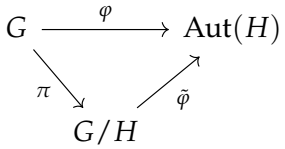
■ SOLUTION Recall from Exercise 4.8 that the map

$$\begin{aligned} G &\to \mathrm{Aut}(G) \\ g &\mapsto \gamma_g, \end{aligned}$$

where $\gamma_g(a) = gag^{-1}$ for all $a \in G$, is a homomorphism. By restricting domains, we obtain a morphism

$$\varphi : G \to \mathrm{Aut}(H).$$

Observe that if $h \in H$, then $\varphi(h) = \gamma_h|_H = \mathrm{id}_H$, since H is commutative. Then the universal property of quotients (Theorem 7.12) implies that φ factors through the quotient. In other words, it exists a unique homomorphism $\tilde{\varphi} : G/H \to \mathrm{Aut}(H)$ so that the diagram



commutes. That is, the function defined by $gH \mapsto \gamma_g|_H$ is well-defined and a homomorphism. ■

9 GROUP ACTIONS

EXERCISE 9.1 (Once more, if you are already familiar with a little linear algebra...) The matrix groups listed in Exercise 6.1 all come with evident actions on a vector space: If M is an $n \times n$ matrix with (say) real entries, multiplication to the right by a column n-vector $\mathbf{v}$ returns a column n-vector $M\mathbf{v}$, and this defines a left action on $\mathbb{R}^n$ viewed as the space of column n-vectors.

- Prove that, through this action, matrices $M \in \mathrm{O}_n(\mathbb{R})$ preserve lengths and angles in $\mathbb{R}^n$.
- Find an interesting action of $\mathrm{SU}(2)$ on $\mathbb{R}^3$. (Hint: Exercise 8.9.)

■ SOLUTION

- Observe that the inner product of two vectors $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$ is given by

$$\langle \mathbf{v}, \mathbf{w} \rangle = \mathbf{v}^t \cdot \mathbf{w},$$

where $\cdot$ is the matrix product. Therefore, if $M \in \mathrm{O}_n(\mathbb{R})$,

$$\begin{aligned} \langle M\mathbf{v}, M\mathbf{w} \rangle &= (M\mathbf{v})^{\mathbf{t}} \cdot M\mathbf{w} \\ &= \mathbf{v}^t \cdot (M^t \cdot M) \cdot \mathbf{w} \\ &= \mathbf{v}^t \cdot \mathbf{w} \\ &= \langle \mathbf{v}, \mathbf{w} \rangle. \end{aligned}$$

If $\mathbf{v} = \mathbf{w}$, this proves M preserves lengths. Moreover, if θ is the angle between $\mathbf{v}$ and $\mathbf{w}$, then $\cos\theta = \frac{\langle \mathbf{v}, \mathbf{w} \rangle}{\|\mathbf{v}\|\|\mathbf{w}\|}$, and this also proves M preserves angles.

- As we have seen in Exercise 6.3, every quaternion $q = a + bi + cj + dk \in \mathbb{H}$ may be represented by a matrix

$$q = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}.$$

If we let $z = a + bi$ and $w = c + di$, then $q = z + wj$ and it may be seen as $q = \begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$. Moreover, its norm $|q|$ is the determinant of the matrix. Therefore $\mathrm{SU}(2)$ is isomorphic (actually, it is *diffeomorphic*) to the unit quaternions. Given a unitary $q \in \mathbb{H}$, since every real number commutes with any quaternion, they are fixed by the inner automorphism γ_q. Since this is a orthogonal $\mathbb{R}$-linear transformation, for $\gamma_q(t) = |qtq^{-1}| = |q||t||q^{-1}| = |t|$, this transformation preserves the space orthogonal to $\mathbb{R}$, which we usually denote by $\operatorname{im}\mathbb{H}$ and is isomorphic to $\mathbb{R}^3$.

Hence, for every $M \in \mathrm{SU}(2)$, there corresponds a unique quaternion q defined above, and to each quaternion q there corresponds an orthogonal transformation γ_q. Similarly to the complex case, every quaternion may be written as $q = \cos\theta + u\sin\theta$, where u is a unitary quaternion in $\operatorname{im}\mathbb{H}$. Since u commutes with q, then $\gamma_q(u) = u$, and we can restrict γ_q to the plane in $\operatorname{im}\mathbb{H}$ orthogonal to u. In this case, if $v \cdot u = 0$, let $w = u \times v$. Then $uv = w$, $vw = u$, $wu = v$, and the product is antisymmetric. Therefore, by direct calculation, $\gamma_q(v) = v\cos 2\theta - w\sin 2\theta$ and $\gamma_q(w) = x\cos 2\theta + v\sin 2\theta$, and γ_q is a rotation in $\mathbb{R}^3$ around

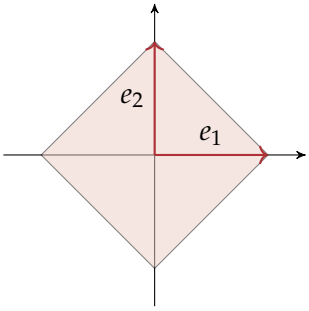
the axis u by the angle 2θ. Furthermore, observe that a rotation around the axis u through the angle 2θ is the same as a rotation around $-u$ through -2θ. Thus, as we saw in Exercise 8.9, the kernel of this transformation is $\{I_2, -I_2\}$. ∎

EXERCISE 9.2 The effect of the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

on the plane is to respectively flip the plane about the y-axis and to rotate it 90° clockwise about the origin. With this in mind, construct an action of D_8 on $\mathbb{R}^2$.

∎ SOLUTION Let e_1, e_2 be the canonical basis of $\mathbb{R}^2$ and consider the square constituted by e_1, e_2, $-e_1$, and $-e_2$.



We'll let D_8 act on this square and see what happens the the vectors e_1 and e_2.

D_8	e_1	e_2
Identity	e_1	e_2
Rotation of 90° counterclockwise	e_2	$-e_1$
Rotation of 180° counterclockwise	$-e_1$	$-e_2$
Rotation of 270° counterclockwise	$-e_2$	e_1
Horizontal reflection	e_1	$-e_2$
Vertical reflection	$-e_1$	e_2
Reflection about the line $y = x$	e_2	e_1
Reflection about the line $y = -x$	$-e_2$	$-e_1$

Since linear transformations are determined by their effects on the basis vectors, this table determines an action of D_8 on $\mathbb{R}^2$. ∎

EXERCISE 9.3 If $G = (G, \cdot)$ is a group, we can define an 'opposite' group $G^\circ = (G, \bullet)$ supported on the same set G, by prescribing

$$(\forall g, h \in G) : \; g \bullet h := h \cdot g.$$

- Verify that G° is indeed a group.
- Show that the 'identity': $G^\circ \to G$, $g \mapsto g$ is an isomorphism if and only if G is commutative.
- Show that $G^\circ \cong G$ (even if G is not commutative!).
- Show that giving a *right*-action of G on a set A is the same as giving a homomorphism $G^\circ \to S_A$, that is, a *left*-action of G° on A.
- Show that the notions of left- and right-actions coincide 'on the nose' for *commutative* groups. (That is, if $(g, a) \mapsto ag$ defines a right-action of a commutative group G on a set A, then setting $ga = ag$ defines a left-action).
- For any group G, explain how to turn a right-action of G into a left-action of G. (Note that the simple 'flip' $ga = ag$ does *not* work in general if G is not commutative.)

■ SOLUTION

- Since G is a group, the set G is nonempty. The operation in G° is associative because $\cdot$ is associative:

$$(g \bullet h) \bullet k = k \cdot (h \cdot g) = (k \cdot h) \cdot g = g \bullet (h \bullet k),$$

for all $g, h, k \in G$. Furthermore, e_G is also the identity of G° since $e_G \bullet g = g \cdot e_G = g$ and $g \bullet e_G = e_G \cdot g = g$ for all $g \in G$. Finally, given $g \in G$, its inverse g^{-1} in G is also its inverse in G° because $g \bullet g^{-1} = g^{-1} \cdot g = e_G$ and $g^{-1} \bullet g = g \cdot g^{-1} = e_G$. Therefore, G° is indeed a group.

- Let $\varphi : G^\circ \to G$ be defined by $\varphi(g) = g$ for all $g \in G$. This function is clearly a bijection, so it suffices to show that φ is an homomorphism if and only if G is commutative. Indeed,

$$\varphi(g \bullet h) = \varphi(g) \cdot \varphi(h) \iff g \bullet h = g \cdot h \iff h \cdot g = g \cdot h$$

and the desired equivalency follows.

- We can find another isomorphism between G and G° that works in any case. Define $\varphi : G^\circ \to G$ by $\varphi(g) = g^{-1}$ for all $g \in G$. Note that it does not matter where this inverse is computed because they coincide on G and G°. It is clear that φ is a bijection. Furthermore,

$$\varphi(g \bullet h) = (g \bullet h)^{-1} = (h \cdot g)^{-1} = g^{-1} \cdot h^{-1} = \varphi(g) \cdot \varphi(h)$$

for all $g, h \in G$, so φ is also a homomorphism. Therefore, $G^\circ \cong G$.

- The remark made after Theorem 9.5 tells us that a right-action of a group G on a set A is a set-function $\rho : G \times A \to A$ such that $\rho(e_G, a) = a$ for all $a \in A$ and

$$(\forall g, h \in G), (\forall a \in A) : \ \rho(g \cdot h, a) = \rho(h, \rho(g, a)).$$

  If we denote $\rho(g, a) = ag$, this last relation means that $a(gh) = (ag)h$ for all $g, h \in G$ and $a \in A$. Note that this definition is slightly different to the one given for left-actions on a set.

  A right-action ρ of G on A defines $\sigma : G^\circ \to \mathrm{Hom}_{\mathsf{Set}}(A, A)$ in a natural way if we set $\sigma(g)(a) = \rho(g, a)$ for all $g \in G$ and $a \in A$. It preserves operation because

$$\begin{aligned} \sigma(g \bullet h)(a) &= \rho(g \bullet h, a) \\ &= \rho(h \cdot g, a) \\ &= \rho(g, \rho(h, a)) \\ &= \sigma(g)(\sigma(h)(a)) \\ &= (\sigma(g) \circ \sigma(h))(a) \end{aligned}$$

  for all $a \in A$, so $\sigma(g \bullet h) = \sigma(g) \circ \sigma(h)$ for all $g, h \in G$. Furthermore, since $\sigma(e_G)(a) = \rho(e_G, a) = a$, $\sigma(e_G) = \mathrm{id}_A$ and each $\sigma(g)$ has inverse $\sigma(g^{-1})$. Therefore, the image of σ is in S_A and we can restrict the codomain of σ to S_A, obtaining the desired homomorphism, which is a left-action of G° on A.

- If $\rho : G \times A \to A$ is a right-action of an abelian group G on a set A it follows that ρ is also a left-action of G on A because $\rho(e_G, a) = a$ for all $a \in A$ and

$$\rho(gh, a) = \rho(hg, a) = \rho(g, \rho(h, a))$$

  for all $g, h \in G$ and $a \in A$. Using the leaner notation, we see that

$$a(gh) = (ag)h \iff (gh)a = h(ga) \iff (hg)a = h(ga)$$

  for all $g, h \in G$ and $a \in A$, so setting $ga = ag$ turns the right-action into a left-action.

- As we did in the third item, we can use the idea of taking the inverse of an element of G. Therefore, given a right-action $(g, a) \mapsto ag$ of G on A, we can turn it into a left-action by setting $ga = ag^{-1}$. Indeed, it follows that $e_G a = ae_G^{-1} = ae_G = a$ for all $a \in A$ and

$$(gh)a = a(gh)^{-1} = a(h^{-1}g^{-1}) = (ah^{-1})g^{-1} = g(ha)$$

  for all $g, h \in G$ and $a \in A$. ∎

EXERCISE 9.4

■ SOLUTION A ■

EXERCISE 9.5 Prove that the action by left-multiplication of a group on itself is free.

■ SOLUTION Fixed $g \in G$, by the cancellation law, given any $a \in G$, $ga = a$ implies $g = e_G$. Therefore the left-multiplication is free, as is the right-multiplication, for analogous reasons. ■

EXERCISE 9.6 Let O be an orbit of an action of a group G on a set. Prove that the induced action of G on O is transitive.

■ SOLUTION Let G act on a set A and let $a \in A$. We can restrict this action to $O = O_G(a)$. Indeed, given $x \in O$, there exists $g \in G$ such that $x = ga$ and so

$$g'x = g'(ga) = (g'g)a \in O$$

for all $g' \in G$. Let's prove that this induced action is transitive. Take $x, y \in O$. There are $g_1, g_2 \in G$ such that $x = g_1 a$ and $y = g_2 a$. Thus, if $g = g_2 g_1^{-1}$, it follows that

$$y = g_2 a = (g_2 g_1^{-1} g_1)a = (g_2 g_1^{-1})(g_1 a) = gx.$$

Therefore, the action of G on O is transitive. ■

EXERCISE 9.7 Prove that stabilizers are indeed subgroups.

■ SOLUTION Let $g, h \in \mathrm{Stab}_G(a)$. In other words, $ga = a$ and $ha = a$. By acting on the left by h^{-1} we have that $a = h^{-1}a$. Thus, $(gh^{-1})a = g(h^{-1}a) = ga = a$ which means that $gh^{-1} \in \mathrm{Stab}_G(a)$. The result follows. ■

EXERCISE 9.8

■ SOLUTION A ■

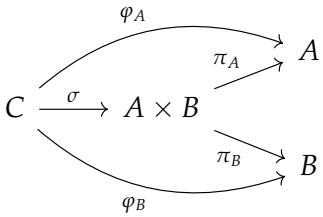
EXERCISE 9.9 Prove that G-Set has product and coproducts and that every finite object of G-Set is a coproduct of objects of the type $G/H = \{\text{left-cosets of } H\}$, where H is a subgroup of G and G acts on G/H by left-multiplication.

■ SOLUTION Products and coproducts in G-Set are very similar to those in Set, as we shall describe.

Let (ρ_A, A) and (ρ_B, B) be two objects. Take $(\rho_{A\times B}, A \times B)$, where $A \times B$ is the usual product in Set (that is, the Cartesian product) and $\rho_{A\times B} : G \times (A \times B) \to A \times B$ is the action given by

$$\rho_{A\times B}(g, (a, b)) = (\rho_A(g, a), \rho_B(g, b))$$

for all $g \in G$ and $(a, b) \in A \times B$. In the usual shorthand notation, this means that $g(a, b) = (ga, gb)$ for all $g \in G$ and $(a, b) \in A \times B$. Note that this is indeed an action and that the projections π_A and π_B are equivariant. We claim that $(\rho_{A\times B}, A \times B)$ with π_A and π_B is the product of (ρ_A, A) and (ρ_B, B) in G-Set. Let (ρ_C, C) be an object and $\varphi_A : C \to A$, $\varphi_B : C \to B$ be equivariant functions. We need to show that there is a unique equivariant function $\sigma : C \to A \times B$ such that the diagram



commutes. We are forced to define σ by

$$\sigma(c) = (\varphi_A(c), \varphi_B(c))$$

for all $c \in C$. Finally, σ is equivariant since φ_A and φ_B are equivariant:

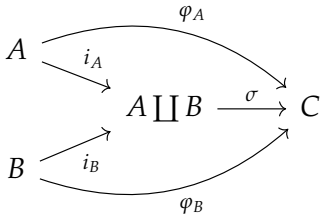
$$\begin{aligned} \sigma(gc) &= (\varphi_A(gc), \varphi_B(gc)) \\ &= (g\varphi_A(c), g\varphi_B(c)) \\ &= g(\varphi_A(c), \varphi_B(c)) \\ &= g\sigma(c) \end{aligned}$$

for all $g \in G$ and $c \in C$.

For the coproduct, take $(\rho_{A\coprod B}, A \coprod B)$, where $A \coprod B$ is the usual coproduct in Set (that is, the disjoint union) and $\rho_{A\coprod B} : G \times (A \coprod B) \to A \coprod B$ is the action given by

$$\rho_{A\coprod B}(g, x) = \begin{cases} i_A(\rho_A(g, a)), \text{ if } x = i_A(a) \text{ for some } a \in A \\ i_B(\rho_B(g, b)), \text{ if } x = i_B(b) \text{ for some } b \in B \end{cases}$$

for all $g \in G$ and $x \in A \coprod B$. In the usual shorthand notation, this means that $gi_A(a) = i_A(ga)$ and $gi_B(b) = i_B(gb)$ for all $g \in G$, $a \in A$ and $b \in B$. Note that this is indeed an action and that the inclusions i_A and i_B are equivariant. We claim that $(\rho_{A\coprod B}, A \coprod B)$ with i_A and i_B is the coproduct of (ρ_A, A) and (ρ_B, B) in G-Set. Let (ρ_C, C) be an object and $\varphi_A : A \to C$, $\varphi_B : B \to C$ be equivariant functions. We need to show that there is a unique equivariant function $\sigma : A \coprod B \to C$ such that the diagram



commutes. We are forced to define σ by

$$\sigma(c) = \begin{cases} \varphi_A(a), \text{ if } c = i_A(a) \text{ for some } a \in A \\ \varphi_B(b), \text{ if } c = i_B(b) \text{ for some } b \in B \end{cases}$$

for all $c \in C$. Finally, note that σ is equivariant since φ_A and φ_B are equivariant. Indeed, given $c \in A \coprod B$, we have that $c = i_A(a)$ for some $a \in A$ or $c = i_B(b)$ for some $b \in B$. In the first case,

$$\sigma(gc) = \sigma(gi_A(a)) = \sigma(i_A(ga)) = \varphi_A(ga) = g\varphi_A(a) = g\sigma(c)$$

for all $g \in G$, and the second case is analogous.

Let G act on a finite set X and let $\mathcal{O}$ be the set of orbits of this action. Firstly, note that $\mathcal{O}$ is a partition on X. Indeed, its is immediate that every element is in some set of $\mathcal{O}$ (just take its orbit). Moreover, if $c \in O_G(a) \cap O_G(b)$, there are $g_1, g_2 \in G$ such that $c = g_1 a = g_2 b$, so $a = g_1^{-1}c$, $b = g_2^{-1}c$ and it follows that $O_G(c) = O_G(a) = O_G(b)$. Thus, different orbits need to be disjoint, as desired. Denote by ρ_O the induced action of G on an orbit $O \in \mathcal{O}$. If ρ is the action of G on X, we claim that

$$(\rho, X) \cong \coprod_{O \in \mathcal{O}} (\rho_O, O).$$

where the coprodct on the right is the one similar to the defined above for just two objects. Indeed, there is a natural bijection $\varphi : X \to \coprod_{O \in \mathcal{O}} O$ which sends an element to a copy of itself in its orbit, since $\mathcal{O}$ is a partition on X. By the definition of the action of the coproduct given above, it is easy to check that φ is equivariant, so Exercise 9.8 implies the desired isomorphism. Finally, Exercise 9.6 tells us the each ρ_O is transitive, so it follows from Proposition 9.9 and the observation above that (ρ, X) is a coproduct of objects of the type $G/H = \{\text{left-cosets of } H\}$, where H is a subgroup of G and G acts on G/H by left-multiplication. ∎

EXERCISE 9.10 Let H be any subgroup of a group G. Prove that there is a bijection between the set G/H of *left*-cosets of H and the set $H\backslash G$ of *right*-cosets of H in G. (Hint: G acts on the right on the set of right-cosets; use Exercise 9.3 and Proposition 9.9.)

∎ SOLUTION Consider the left-action defined by $\rho(g, Ha) = H(ga)$. Clearly, $\rho(e_G, Ha) = Ha$ and $\rho(g_1 \cdot g_2, Ha) = \rho(g_1, \rho(g_2, a))$. Furthermore, this action is transitive, since left multiplication is surjective. For any $a \in G$, $H(ga) = Ha$ if and only if $g \in H$, hence $\text{Stab}_G(a) = H$, from where we conclude G/H is isomorphic to $H\backslash G$. ∎

EXERCISE 9.11 ¬ Let G be a finite group, and let H be a subgroup of index p, where p is the *smallest prime dividing* $|G|$. Prove that H is normal in G, as follows:

- Interpret the action of G on G/H by left-multiplication as a homomorphism $\sigma : G \to S_p$.
- Then $G/\ker\sigma$ is (isomorphic to) a subgroup of S_p. What does this say about the index of $\ker\sigma$ in G?
- Show that $\ker\sigma \subset H$.
- Conclude that $H = \ker\sigma$, by index considerations.

Thus H is a kernel, proving that it is normal. (This exercise generalizes the result of Exercise 8.2.) [9.12]

■ SOLUTION A ■

EXERCISE 9.12 ¬ Generalize the result of Exercise 9.11, as follows. Let G be a group, and let $H \subseteq G$ be a subgroup of index n. Prove that H contains a subgroup K that is normal in G and such that $[G : K]$ divides the gcd of $|G|$ and $n!$. (In particular, $[G : K] \leq n!$.) [IV.2.23]

■ SOLUTION As in the previous exercise, the action of G on G/H by left-multiplication can be interpreted as a homomorphism $\sigma : G \to S_{G/H}$. By Theorem 8.1, $G/\ker\sigma$ is isomorphic to $\operatorname{im}\sigma$, which is a subgroup of $S_{G/H}$. Let $K = \ker\sigma$, which is a normal subgroup of G. Since $|G/H| = [G : H] = n$, it follows that $|S_{G/H}| = n!$ and so, by Lagrange's theorem, $[G : K]$ divides $n!$. Since K is a subgroup of G, Lagrange's theorem also implies that $[G : K]$ divides $|G|$ and, thus, $[G : K]$ divides the gcd of $|G|$ and $n!$. It remains to show that $K \subseteq H$. Let $k \in K$ be an arbitrary element. Since $K = \ker\sigma$, $\sigma(k)$ is the identity on G/H. This means that $(kg)H = gH$ for all $g \in G$. In particular, if we take $g = e_G$, we have that $kH = (ke_G)H = e_GH = H$, so $k \in H$. Thus, $K \subseteq H$, as desired. ■

EXERCISE 9.13

■ SOLUTION A ■

EXERCISE 9.14

■ SOLUTION T ■

EXERCISE 9.15 ¬ Prove that every (finitely generated) group G acts freely on any corresponding Cayley graph. (Cf. Exercise 8.6. Actions on a directed graph are defined as actions on the set of vertices preserving incidence: if the vertices v_1, v_2 are connected by an edge, then so must be gv_1, gv_2 for every $g \in G$.) In particular, conclude that every free group acts freely on a tree. [9.16]

■ SOLUTION Take the Cayley graph of G corresponding to a set of generators A. If V denotes the set of vertices of this graph, there

is a bijection between G and V which sends each element of G to its correspondent vertex on the graph. Thus, for simplicity, we will operate with vertices as if they were elements of G. In this sense, we can define a natural action $\rho : G \times V \to V$ by left multiplication. Moreover, ρ preserves incidence and orientation: if there is an edge from $v_1 \in V$ to $v_2 \in V$, there exists $a \in A$ such that $v_2 = v_1 a$ and so $gv_2 = g(v_1 a) = (gv_1)a$, that is, there is an edge from gv_1 to gv_2 for all $g \in G$. Therefore, G acts on its Cayley graph. To show that this action is free, note that, if $gv = v$ for some $v \in V$, $g \in G$, we must have $g = e_G$ by the cancellation law, so e_G is the only element fixing any element of V.

In particular, since a free group admits a Cayley graph that is a tree (this is Exercise 8.6), we conclude that every free group acts freely on a tree. ∎

EXERCISE 9.16 ▷ The converse of the last statement in Exercise 9.15 is also true: only free groups can act freely on a tree. Assuming this, prove that every subgroup of a free group (on a finite set) is free. [§6.4]

∎ SOLUTION Let F be a free group on a finite set and let $H \subseteq F$ be a subgroup. By the preceding exercise, F acts freely on a tree (its Cayley graph, *cf.* Exercise 8.6). The restriction of this action to H surely preserves the fact that it is free. That is, H also acts freely on a tree. We conclude that H is free. ∎

EXERCISE 9.17

∎ SOLUTION A ∎

EXERCISE 9.18 Show how to construct a *groupoid* carrying the information of the action of a group G on a set A. (Hint: A will be the set of objects of the grupoid. What will be the morphisms?)

∎ SOLUTION Let's define the category C as follows:

- $\mathrm{Obj}(\mathsf{C}) = A$;
- for $a, b \in A$, $\mathrm{Hom}_{\mathsf{C}}(a, b) = \{(g, a) \in G \times A \mid b = ga\}$.

The objects of C are the elements of A and the morphisms are essentially elements of G representing the action. The reason for taking ordered pairs is to guarantee that $\mathrm{Hom}_{\mathsf{C}}(a, b)$ and $\mathrm{Hom}_{\mathsf{C}}(c, d)$ are disjoint unless $a = c$ and $b = d$. We define the composition of $(g, a) \in \mathrm{Hom}_{\mathsf{C}}(a, b)$ and $(h, b) \in \mathrm{Hom}_{\mathsf{C}}(b, c)$ as $(h, b)(g, a) := (h \cdot g, a) \in \mathrm{Hom}_{\mathsf{C}}(a, c)$, that is, we simply multiply h and g. Note that we really have that $(h \cdot g, a) \in \mathrm{Hom}_{\mathsf{C}}(a, c)$ because $(h \cdot g)a = h(ga) = hb = c$. Since G is a group, this composition is associative. Furthermore, the identity morphisms are $1_a = (e_G, a) \in \mathrm{Hom}_{\mathsf{C}}(a, a)$ for all $a \in A$, which are identities with respect to composition since e_G

is the identity element of G. Therefore, C is indeed a category. To prove that it is also a grupoid, note that $(g^{-1}, b) \in \mathrm{Hom}(b, a)$ is a two-sided inverse for $(g, a) \in \mathrm{Hom}_{\mathsf{C}}(a, b)$ since $g^{-1}b = g^{-1}(ga) = (g^{-1}g)a = a$, $(g^{-1}, b)(g, a) = (e_G, a) = 1_a$ and $(g, a)(g^{-1}, b) = (e_G, b) = 1_b$.

This grupoid carries the information of the action in the sense that we can compute ga by simply looking at the morphisms that depart from a, for all $g \in G$ and $a \in A$. The identities and the composition of morphisms in C correspond to the properties given by and $e_G a = a$ $(gh)a = g(ha)$ for all $g, h \in G$ and $a \in A$. ∎

10 GROUP OBJECTS IN CATEGORIES

EXERCISE 10.1 Define all the unnamed maps appearing in the diagrams in the definition of group object, and prove that they are indeed isomorphisms when so indicated. (For the projection $1 \times G \to G$, what is left to prove is that the composition

$$1 \times G \to G \to 1 \times G$$

is the identity, as mentioned in the text.)

∎ SOLUTION T ∎

EXERCISE 10.2 ▷ Show that *groups*, as defined in §1.2, are 'group objects in the category of sets'. [§10.1]

∎ SOLUTION All we need to do is to prove that a couple of diagrams commute. Firstly, the commutativity of

$$\begin{array}{ccccc} (G \times G) \times G & \xrightarrow{m \times \mathrm{id}_G} & G \times G & \xrightarrow{m} & G \\ \cong \downarrow & & & & \| \\ G \times (G \times G) & \xrightarrow{\mathrm{id}_G \times m} & G \times G & \xrightarrow{m} & G \end{array}$$

asserts the associativity of the binary operation in G. The commutativity of

$$\begin{array}{ccc} 1 \times G & \xrightarrow{e \times \mathrm{id}_G} & G \times G \\ & \searrow^{\cong} & \downarrow m \\ & & G \end{array} \qquad \begin{array}{ccc} G \times 1 & \xrightarrow{\mathrm{id}_G \times e} & G \times G \\ & \searrow^{\cong} & \downarrow m \\ & & G \end{array}$$

follows from the existence of a two-sided identity. Lastly, the commutativity of

$$\begin{array}{ccccc} G & \xrightarrow{\Delta} & G \times G & \xrightarrow{\mathrm{id}_G \times \iota} & G \times G \\ \downarrow & & & & \downarrow m \\ 1 & & \xrightarrow{\quad e \quad} & & G \end{array} \qquad \begin{array}{ccccc} G & \xrightarrow{\Delta} & G \times G & \xrightarrow{\iota \times \mathrm{id}_G} & G \times G \\ \downarrow & & & & \downarrow m \\ 1 & & \xrightarrow{\quad e \quad} & & G \end{array}$$

means exactly that there exists two-sided inverses. ∎

EXERCISE 10.3 Let $(G, \cdot)$ be a group, and suppose $\circ : G \times G \to G$ is a group homomorphism (w.r.t. $\cdot$) such that $(G, \circ)$ is *also* a group. Prove that $\circ$ and $\cdot$ coincide. (Hint: First prove that the identity with respect to the two operations must be the same.)

∎ SOLUTION To avoid confusion, we will denote the homomorphism $\circ$ by f, that is $f(g,h) = \circ(g,h) = g \circ h$ for all $g, h \in G$. Let e_1 and e_2 be the identities with respect to $\cdot$ and $\circ$, respectively. Since f is a homomorphism with respect to $\cdot$, it follows that

$$\begin{aligned} e_2 &= e_2 \circ e_2 \\ &= f(e_2, e_2) \\ &= f(e_2 \cdot e_1, e_1 \cdot e_2) \\ &= f((e_2, e_1) \cdot (e_1, e_2)) \\ &= f(e_2, e_1) \cdot f(e_1, e_2) \\ &= (e_2 \circ e_1) \cdot (e_1 \circ e_2) \\ &= e_1 \cdot e_1 = e_1, \end{aligned}$$

so these two identities are the same and we will denote it simply by e. With a similar computation, we have that

$$\begin{aligned} g \circ h &= f(g,h) \\ &= f(g \cdot e, e \cdot h) \\ &= f((g,e) \cdot (e,h)) \\ &= f(g,e) \cdot f(e,h) \\ &= (g \circ e) \cdot (e \circ h) \\ &= g \cdot h \end{aligned}$$

for all $g, h \in G$. Therefore, $\circ$ and $\cdot$ coincide. ∎

EXERCISE 10.4 Prove that every *abelian* group has exactly one structure of group object *in the category* Ab.

∎ SOLUTION A ∎

EXERCISE 10.5 By the previous exercise, a group object in Ab is nothing other than an abelian group. What is a group object in group?

∎ SOLUTION T ∎

III

RINGS AND MODULES

1 DEFINITION OF RING

EXERCISE 1.1 ▷ Prove that if $0 = 1$ in a ring R, then R is a zero-ring. [§1.2]

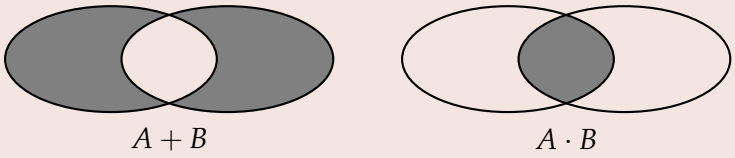
■ SOLUTION Observe that, for every $r \in R$,

$$r = 1 \cdot r = 0 \cdot r = 0.$$

Hence $R = \{0\}$ is a zero-ring. ■

EXERCISE 1.2 ¬ Let S be a set, and define operations on the power set $\mathscr{P}(S)$ of S by setting $\forall A, B \in \mathscr{P}(S)$

$$A + B := (A \cup B) \setminus (A \cap B), \qquad A \cdot B := A \cap B :$$



$A + B$ $\qquad$ $A \cdot B$

(where the solid grey indicates the set included in the operation). Prove that $(\mathscr{P}(S), +, \cdot)$ is a commutative ring. [2.3, 3.15]

This addition operation is usually called *symmetric difference*.

■ SOLUTION Since $\mathscr{P}(S)$ has two 'distinguished' elements, $\varnothing$ and S, we can surely guess that they might be the identities. We quickly verify that

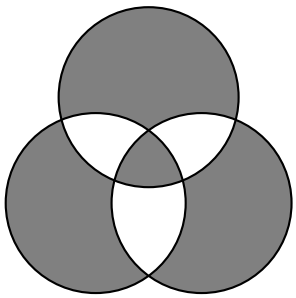
$$A + \varnothing = (A \cup \varnothing) \setminus (A \cap \varnothing) = A \setminus \varnothing = A$$

and that

$$A \cdot S = A \cap S = A,$$

since $A \subseteq S$. Similarly, $\varnothing + A = A$ and $S \cdot A = A$. This means that $\varnothing$ is the additive identity and S is the multiplicative identity.

The addition is associative since both $(A + B) + C$ and $A + (B + C)$ are the set indicated in the following diagram.

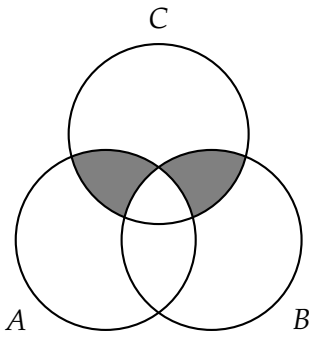


$A + B + C$

Also, clearly $\cdot$ is associative and both operations are commutative. The additive inverse of a element is simply itself as

$$A + A = (A \cup A) \setminus (A \cap A) = A \setminus A = \varnothing.$$

Lastly, we have distributivity since



represents both $(A + B) \cdot C$ and $(A \cdot C) + (B \cdot C)$. ∎

EXERCISE 1.3 ¬ Let R be a ring, and let S be any set. Explain how to endow the set R^S of set-functions $S \to R$ of two operations $+, \cdot$ so as to make R^S into a ring, such that R^S is just a copy of R if S is a singleton. [2.3]

∎ SOLUTION Similarly to what has been done at the very end of section 4 of chapter II, if $f, g : S \to R$ are two functions of R^S, we can set their sum as the function given by

$$(f + g)(s) \coloneqq f(s) + g(s)$$

and their product as the function defined by

$$(f \cdot g)(s) \coloneqq f(s) \cdot g(s),$$

for all $s \in S$. These operations naturally 'inherits' the associative and distributive properties of $+, \cdot$ in R and note that the sum is also

commutative. Furthermore, the function that sends every element of S to 0_R is the zero element and the one that sends every element to 1_R is the multiplicative identity. Finally, it is clear that the opposite of a function $f : S \to R$ is the function given by

$$(-f)(s) = -f(s)$$

for all $s \in S$. Therefore, R^S is a ring.

Notice that, if S is the singleton $\{*\}$, R^S is just a copy of R in the sense that the function

$$\begin{aligned} \varphi : R^S &\to R \\ f &\mapsto f(*) \end{aligned}$$

is a bijection, it preserves both operations and $\varphi(1_{R^S}) = 1_R$. As we will see in future sections, φ is a *ring isomorphism*. ∎

EXERCISE 1.4 ▷ The set of $n \times n$ matrices with entries in a ring R is denoted $\mathcal{M}_n(R)$. Prove that componentwise addition and matrix multiplication make $\mathcal{M}_n(R)$ into a ring, for any ring R. The notation $\mathfrak{gl}_n(R)$ is also commonly used, especially for $R = \mathbb{R}$ of $\mathbb{C}$ (although this indicates one is considering them as *Lie algebras*) in parallel with the analogous notation for the corresponding groups of units; cf. Exercise II.6.1. In fact, the parallel continues with the definition of the following sets of matrices:

- $\mathfrak{sl}_n(\mathbb{R}) = \{M \in \mathfrak{gl}_n(\mathbb{R}) \mid \operatorname{tr}(M) = 0\}$;
- $\mathfrak{sl}_n(\mathbb{C}) = \{M \in \mathfrak{gl}_n(\mathbb{C}) \mid \operatorname{tr}(M) = 0\}$;
- $\mathfrak{so}(\mathbb{R}) = \{M \in \mathfrak{sl}_n(\mathbb{R}) \mid M + M^t = 0\}$;
- $\mathfrak{su}(n) = \{M \in \mathfrak{sl}_n(\mathbb{C}) \mid M + M^\dagger = 0\}$.

Here $\operatorname{tr}(M)$ is the *trace* of M, that is, the sum of its diagonal entries. The other notation matches the notation user in Exercise II.6.1. Can we make rings of these sets by endowing them with ordinary addition and multiplication of matrices? (These sets are all Lie algebras; cf. Exercise VI.1.4.) [§1.2, 2.4, 5.9, VI.1.2, VI.1.4]

∎ SOLUTION Since $(R, +, 0_R)$ is a commutative group, then $(\mathcal{M}_n(R), +, 0_n)$ where 0_n is the matrix whose entries are all 0_R. ∎

EXERCISE 1.5 Let R be a ring. In a, b are zero-divisors in R, is $a + b$ necessarily a zero-divisor?

∎ SOLUTION No. Consider, for example, $R = \mathbb{Z}/6\mathbb{Z}$. Then 2 and 3 are zero-divisors, but $5 = 2 + 3$ is not a zero-divisor. ∎

EXERCISE 1.6 ¬ An element a of a ring R is *nilpotent* if $a^n = 0$ for some n.

- Prove that if a and b are nilpotent in R and $ab = ba$, then $a + b$ is also nilpotent.
- Is the hypothesis $ab = ba$ in the previous statement necessary for its conclusion to hold?

[3.12]

■ SOLUTION

- Lets say that $a^n = 0$ and $b^m = 0$. Since a and b commute, the binomial theorem is valid. That is,

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

If $k < n$, then $n + m - k > m$ so that $b^{n+m-k} = 0$. Else, $a^k = 0$. In other words, every term in the sum above is zero.

- Yes, the hypothesis is necessary. For a counter-example, take

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}.$$

Then $(a+b)^2$ is the identity matrix, which shows that $a + b$ is *not* nilpotent. ■

EXERCISE 1.7 Prove that $[m]$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$ if and only if m is divisible by all prime factors of n.

■ SOLUTION ($\Longrightarrow$) If $[m]_n$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$, there exists $k \in \mathbb{N}$ such that $[m]_n^k = [m^k]_n = [0]_n$ and so n divides m^k. Thus, if p is a prime factor of n, p divides m^k and, since it is a prime number, p divides m.

($\Longleftarrow$) Suppose that m is divisible by all prime factors of n and let $k \in \mathbb{N}$ be the largest exponent appearing in the prime factorization of n. It is clear that n divides m^k and so $[m]_n^k = [m^k]_n = [0]_n$. Therefore, m is nilpotent in $\mathbb{Z}/n\mathbb{Z}$. ■

EXERCISE 1.8 Prove that $x = \pm 1$ are the only solutions to the equation $x^2 = 1$ in an integral domain. Find a ring in which the equation $x^2 = 1$ has momre than 2 solutions.

■ SOLUTION If $x^2 = 1$, then $x^2 - 1 = 0$ and $(x+1)(x-1) = 0$. Since we are in an integral domain, $x + 1 = 0$ or $x - 1 = 0$, which is the desired conclusion. On the other hand, if $R = \mathbb{Z}/8\mathbb{Z}$, then $[1]_8^2 = [3]_8^2 = [5]_8^2 = [7]_8^2 = 1$. ■

EXERCISE 1.9 ▷ Prove Proposition 1.12. [§1.2]

PROPOSITION 1.12 In a Ring R:

- u is a left- (resp., right-) unit if and only if left- (resp., right-) multiplication by u is a *surjective* function $R \to R$;
- if u is a left- (resp., right-) unit, then right- (resp., left-) multiplication by u is injective; that is, u is not a right- (resp., left-) zero-divisor;
- the inverse of a two-sided unit is unique;
- two-sided units form a group under multiplication.

■ SOLUTION The book has already proved the first two claims for u right-unit. Suppose u left-unit, and $v \in R$ satisfies $u \cdot v = 1_R$. If $\lambda_u \colon R \to R$ is defined by $\lambda_u(r) = u \cdot r$, then, for every $r \in R$,

$$\lambda_u(vr) = u(vr) = (uv)r = 1_R \cdot r = r,$$

and left-multiplication by u is surjective. Reciprocally, if the function is surjectire, there exists a $v \in R$ such that $u \cdot v = \lambda_u(v) = 1_R$, and u is a left-unit.

Analogously, let u be a left-unit and $v \in R$ be such that $u \cdot v = 1$. If $\rho_u(r) = r \cdot u$, then

$$(\rho_v \circ \rho_u)(r) = \rho_v(\rho_u(r)) = \rho_v(r \cdot u) = (ru)v = r(uv) = r \cdot 1_R = r.$$

Hence ρ_u is injective. ■

EXERCISE 1.10 Let R be a ring. Prove that if $a \in R$ is a right-unit and has two or more left-inverses, then a is *not* a left-zero-divisor and *is* a right-zero-divisor.

■ SOLUTION Our hypothesis says that there are two elements $b_1, b_2 \in R$ such that $b_1 a = b_2 a = 1$. This implies that

$$(b_1 - b_2)a = b_1 a - b_2 a = 1 - 1 = 0,$$

which says precisely that a is a right-zero-divisor. Now, lets suppose that a is a left-zero-divisor. In other words, lets suppose that there is a non-zero element $c \in R$ such that $ac = 0$. Multiplying by c on the right on $b_1 a = 1$, we get that

$$0 = b_1 ac = c,$$

which is absurd. The result follows. ■

EXERCISE 1.11 ▷ Construct a field with 4 elements: as mentioned in the text, the underlying abelian group will have to be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$; $(0,0)$ will be the zero element, and $(1,1)$ will be the multiplicative identity. The question is what $(0,1)\cdot(0,1)$, $(0,1)\cdot(1,0)$, $(1,0)\cdot(1,0)$ must be, in order to get a *field*. [§1.2, §V.5.1]

■ SOLUTION By Proposition 1.12, two-sided units of a ring R form a group under multiplication, so $F \setminus \{0_F\}$ with $\cdot_F$ is a group for all fields F. Therefore, we have to define multiplication in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ so that $\{(1,1),(0,1),(1,0)\}$ be a group with identity $(1,1)$ under this operation. But all groups of order 3 are isomorphic to C_3 (see Exercise II.1.6) and, thus, the multiplication table for $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ must be the one below.

Since $(1,1)$, $(1,0)$ and $(0,1)$ are indistinguishable with respect to their addition properties in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, we could have taken the identity as $(1,0)$ or $(0,1)$ and we would have gotten isomorphic fields to this one.

$\cdot$	$(0,0)$	$(1,1)$	$(0,1)$	$(1,0)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(1,1)$	$(0,0)$	$(1,1)$	$(0,1)$	$(1,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(1,0)$	$(0,0)$	$(1,0)$	$(1,1)$	$(0,1)$

Since this multiplication is commutative, it only remains to show that the distributive properties hold in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which can be done with some few computations. Therefore, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with this multiplication becomes a field. ■

Remark. The field we constructed above is called (for obvious reasons) a *finite field*. They are very important and appear in a number of areas of mathematics and computer science such as number theory, algebraic geometry, Galois theory, finite geometry, cryptography and coding theory. We will find them again in future chapters. Here are some properties of the finite fields:

- There exists a finite field of order n if and only if n is a power of a prime number. Furthermore, all finite fields of the same order are isomorphic to each other and so they are all unambiguously denoted by $\mathbb{F}_n$, $\mathbf{F}_n$ or $\mathrm{GF}(n)$ (here the letters GF stand for "Galois field").
- As for all fields, the nonzero elements of a finite field form a group under multiplication. This group is always cyclic. For example, we pointed above that this group is isomorphic to C_3 if we consider the field as $\mathbb{F}_4$.
- A finite field of order p^k is of characteristic p, so there is a 'copy' of $\mathbb{Z}/p\mathbb{Z}$ inside it. Some properties follow from this observation. For example, $(x+y)^p = x^p + y^p$ for all $x, y \in \mathbb{F}_{p^k}$. We can also generalize Fermat's little theorem:

$x^{p^k} = x$ for all $x \in \mathbb{F}_{p^k}$. With this, we can conclude that $x^{p^k} - x$ factors in $\mathbb{F}_{p^k}$ as

$$x^{p^k} - x = \prod_{a \in \mathbb{F}_{p^k}} (x - a).$$

Moreover, $\mathbb{F}$ is the *splitting field* of $x^{p^k} - x$ over $\mathbb{Z}/p\mathbb{Z}$.

- For all prime numbers p and positive integers n, we can find an irreducible polynomial $f(x)$ in $\mathbb{Z}/p\mathbb{Z}$ of degree n. Therefore, it follows that

$$\mathbb{F}_{p^n} \cong \frac{\mathbb{Z}/p\mathbb{Z}}{(f(x))}$$

and so we can explicitly construct all finite fields. For example, the finite field $\mathbb{F}_4$ of this exercise is isomorphic to $(\mathbb{Z}/2\mathbb{Z})/(x^2 + x + 1)$. This observation makes it easier to calculate multiplication tables as we did above.

EXERCISE 1.12 ◁ Just as complex numbers may be view as combinations $a + bi$, where $a, b \in \mathbb{R}$ and i satisfies the relation $i^2 = -1$ (and commutes with $\mathbb{R}$), we may construct a ring $\mathbb{H}$ by considering linear combinations $a + bi + cj + dk$ where $a, b, c, d \in \mathbb{R}$ and i, j, k commutes with $\mathbb{R}$ and satisfies the relations:

$$i^2 = j^2 = k^2 = -1 \quad ij = -hi = k \quad jk = -kj = i \quad ki = -ik = j.$$

■ SOLUTION T ■

EXERCISE 1.13

■ SOLUTION A ■

EXERCISE 1.14 ▷ Let R be a ring, and let $f(x), g(x) \in R[x]$ be nonzero polynomials. Prove that

$$\deg(f(x) + g(x)) \leq \max(\deg(f(x)), \deg(g(x))).$$

Assuming that R is an integral domain, prove that

$$\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x)).$$

[§1.3]

■ SOLUTION Let $f(x) = \sum_{i \geq 0} a_i x^i$ and $g(x) = \sum_{i \geq 0} b_i x^i$. If d is the greatest index such that $a_i \neq 0$ and e is the greatest index such that $b_i \neq 0$, it is clear that every coefficient $c_i = a_i + b_i$ in

$$f(x) + g(x) = \sum_{i \geq 0} c_i x^i = \sum_{i \geq 0} (a_i + b_i) x^i$$

is zero if $i > d + e$. This means that

$$\deg(f(x) + g(x)) \leq \max(\deg(f(x)), \deg(g(x))).$$

Now let R be an integral domain. As we know, the k-th coefficient of $f(x) \cdot g(x)$ is

$$\sum_{i+j=k} a_i b_j x^{i+j}.$$

Clearly if $k > d + e$ this sum has no non-zero terms. However, since the $(d + e)$-th coefficient is $a_d b_e$ and R is an integral domain, $a_d b_e \neq 0$. This means that the degree of $f(x) \cdot g(x)$ is exactly $d + e$. ∎

EXERCISE 1.15 ▷ Prove that $R[x]$ is an integral domain if and only if R is an integral domain.

∎ SOLUTION If $R[x]$ is an integral domain, it is clear that R is too since the polynomials of degree 0 form a 'copy' of R inside $R[x]$. Now, suppose that R is an integral domain. It is clear that $R[x]$ is commutative since R is commutative. Moreover, $R[x]$ does not have nonzero zero-divisors. Indeed, let $f = \sum_{i \geq 0} a_i x^i$ and $g = \sum_{i \geq 0} b_i x^i$ be two nonzero polynomials in $R[x]$. If r and s are the largest integers such that $a_r \neq 0$ and $b_s \neq 0$, the coefficient of x^{r+s} in $f(x) \cdot g(x)$ is

$$\sum_{i+j=r+s} a_i b_j = \left(\sum_{\substack{i+j=r+s \\ i>r}} a_i b_j \right) + a_r b_s + \left(\sum_{\substack{i+j=r+s \\ j>s}} a_i b_j \right) = a_r b_s \neq 0$$

and so $f(x) \cdot g(x)$ is a nonzero polynomial, as desired. Note that $a_r b_s \neq 0$ because both a_r and b_s are nonzero and R is an integral domain. Therefore, we conclude that $R[x]$ is also an integral domain. ∎

EXERCISE 1.16 Let R be a ring, and consider the ring of power series $R[[x]]$ (cf. §1.3).

(i) Prove that a poer series $a_0 + a_1 x + a_2 x^2 + \cdots$ is a unit in $R[[x]]$ if and only if a_0 is a unit in R. What is the inverse of $1 - x$?

(ii) Prove that $R[[x]]$ is an integral domain if and only if R is.

∎ SOLUTION T ∎

EXERCISE 1.17

∎ SOLUTION A ∎

EXERCISE 2.1 ▷ Prove that if there is a homomorphism from a zero-ring to a ring R, then R is a zero-ring. [§2.1]

■ SOLUTION Let $\varphi : \{*\} \to R$ be a homomorphism. Since homomorphisms take identities to identities,

$$0 = \varphi(*) = 1.$$

As $a \cdot 1 = a$ for all $a \in R$, we conclude that $a = a \cdot 1 = a \cdot 0 = 0$ for all $a \in R$. In other words, R is the trivial ring. ■

EXERCISE 2.2

■ SOLUTION T ■

EXERCISE 2.3 Let S be a set, and consider the power set ring $\mathscr{P}(S)$ (Exercise 1.2) and the ring $(\mathbb{Z}/2\mathbb{Z})^S$ you constructed in Exercise 1.3. Prove that these two rings are isomorphic. (Cf. Exercise I.2.11.)

■ SOLUTION By Exercise I.2.11, the function $\chi : \mathscr{P}(S) \to (\mathbb{Z}/2\mathbb{Z})^S$ which assigns for each $A \subseteq S$ a function

$$\chi_A(x) = \begin{cases} [1]_2, & \text{if } x \in A \\ [0]_2, & \text{otherwise.} \end{cases}$$

is a bijection. We claim that χ is also a ring homomorphism. Firstly, recall that $S = 1_{\mathscr{P}(S)}$ and notice that χ_S is the function that sends every element of S to $[1]_2$, which is the multiplicative identity of $(\mathbb{Z}/2\mathbb{Z})^S$. Now, let $A, B \subseteq S$ be two arbitrary subsets. Note that $(\chi_A + \chi_B)(x)$ equals to $[1]_2$ if and only if x belongs to A or B but not to both of them, that is, if and only if $x \in (A \cup B) \smallsetminus (A \cap B) = A + B$. Thus, it follows that $\chi_{A+B} = \chi_A + \chi_B$. Moreover, $(\chi_A \cdot \chi_B)(x) = [1]_2$ if and only if $\chi_A(x) = \chi_B(x) = [1]_2$, that is, if and only if $x \in A \cap B = A \cdot B$. Hence, $\chi_{A \cdot B} = \chi_A \cdot \chi_B$. It follows that χ is also a ring homomorphism and so we conclude that $\mathscr{P}(S)$ and $(\mathbb{Z}/2\mathbb{Z})^S$ are isomorphic. ■

EXERCISE 2.4

■ SOLUTION A ■

EXERCISE 2.5 ¬ The *norm* of a quaternion $w = a + bi + cj + dk$, with $a, b, c, d \in \mathbb{R}$, is the real number $N(w) = a^2 + b^2 + c^2 + d^2$.

Prove that the function from the multiplicative group $\mathbb{H}^*$ of nonzero quaternions to the multiplicative group $\mathbb{R}^+$ of positive real numbers, defined by assigning to each nonzero quaternion its norm, is a homomorphism. Prove that the kernel of this homomorphism is isomorphic to $\mathrm{SU}(2)$ (cf. Exercise II.6.3). [4.10, IV.4.17, V.6.19]

■ SOLUTION *A priori*, in order to prove that this function is a homomorphism, one could simply observe that

$$N(w_1 w_2) = N(w_1)N(w_2)$$

by expanding both sides explicitly. However, I think it is more interesting to understand a couple important facts about quaternions and then proving this result more elegantly. We begin by defining the conjugate $\overline{w}$ of a quaternion $w = a + bi + cj + dk$ by

$$\overline{w} = a - bi - cj - dk.$$

As we saw in Exercise , $N(w) = w\overline{w}$. Now, while conjugation is not a multiplicative operation, it is *anti-multiplicative*, in the sense that $\overline{w_1 w_2} = \overline{w_2}\,\overline{w_1}$. (This can be quickly verified by an explicit calculation.) This implies that

$$N(w_1 w_2) = (w_1 w_2)(\overline{w_1 w_2}) = w_1\, w_2\, \overline{w_2}\,\overline{w_1} = N(w_1)N(w_2).$$

Now, to compute the kernel of this homomorphism, we will represent a quaternion $w = a + bi + cj + dk$ as a complex matrix

$$\begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix},$$

just like in the previous exercise. Notice that the norm of w is given by the determinant of the corresponding matrix. (This gives another proof that the norm is multiplicative.) Just for now, we shall denote by W the matrix associated with the quaternion w.

Observe that we have

$$WW^\dagger = W^\dagger W = N(w)I,$$

where I is the identity matrix. If $w \in \ker N$, this shows that W is unitary. The fact that $N(w) = \det W$ then implies that $W \in \mathrm{SU}(2)$. The reverse inclusion was done in Exercise II.6.3. ■

EXERCISE 2.6

■ SOLUTION T ■

EXERCISE 2.7 ▷ Let $R = \mathbb{Z}/2\mathbb{Z}$, and let $f(x) = x^2 - x$; note $f(x) \neq 0$. What is the polynomial function $R \to R$ determined by $f(x)$? [§2.2, §V.4.2, §V.5.1]

■ SOLUTION The polynomial function determined by $f(x)$ takes r and sends it to $f(r) = r^2 - r$ for all $r \in \mathbb{Z}/2\mathbb{Z}$. But note that $f([0]_2) = f([1]_2) = [0]_2$, so this polynomial function is the same as the one determined by $g(x) = 0$, even though $f(x) \neq 0$. ■

EXERCISE 2.8

■ SOLUTION A ■

EXERCISE 2.9 ¬ The *center* of a ring R consists of the elements a such that $ar = ra$ for all $r \in R$. Prove that the center is a subring of R.

Prove that the center of a division ring is a field. [2.11, IV.2.17, VII.5.14, VII.5.16]

■ SOLUTION Let C be the center of R. In order to prove that C is a subring, we have to show that $1 \in C$, and that $a, b \in C$ implies $a - b \in C$ and $ab \in C$. Clearly $1 \in C$ and distributivity implies that $a, b \in C$ implies $a - b \in C$ since

$$(a - b)r = ar - br = ra - rb = r(a - b)$$

for all $r \in R$. Now, we also have that

$$abr = arb = rab,$$

for all $r \in R$, which implies that C is a subring.

Finally, since the center is a subring, the center of a division ring is also a division ring and it is commutative. In other words, it is a field.

■

EXERCISE 2.10

■ SOLUTION T ■

EXERCISE 2.11 ¬ Let R be a division ring consisting of p^2 elements, where p is a prime. Prove that R is commutative as follows:

- If R is not commutative, then its center C (Exercise 2.9) is a proper subring of R. Prove that C would then consist of p elements.
- Let $r \in R$, $r \notin C$. Prove that the centralizer of r (Exercise 2.10) contains both r and C.
- Deduce that the centralizer of r is the whole of R.
- Derive a contradiction, and conclude that R had to be commutative (hence, a field).

This is a particular case of Wedderburn's theorem: every finite division ring is a field. [IV.2.17, VII.5.16]

■ SOLUTION

- Since C is a subring of R, the underlying abelian group $(C, +)$ is a subgroup of $(R, +)$. By Lagrange's theorem, $|C|$ can only be 1,

p or p^2 because p is prime. But C is a proper subring of R and it has at least two elements (0_R and 1_R, which are different by Exercise 2.1), so $|C| = p$.

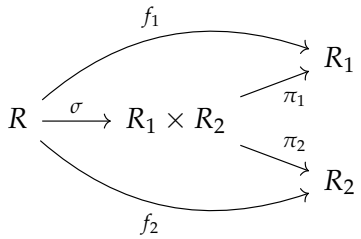
- It is clear that r commutes with itself and with every element of C by the definition of center. Therefore, the centralizer of r contains both r and C.
- By Exercise 2.10, the centralizer of r is a subring of R. As in the first part, Lagrange's theorem implies that it contains 1, p or p^2 elements. Since it contains both C and r (which is not in C), and $|C| = p$, it follows that the centralizer of r has p^2 elements and, hence, is the whole of R.
- Notice that the centralizer of an element of C also is R. By Exercise 2.10, C is the intersection of the centralizers of all elements of R, which is R itself. This contradicts the fact that C has only p elements. Therefore, we conclude that R had to be commutative and, hence, a field. ∎

EXERCISE 2.12

∎ SOLUTION A ∎

EXERCISE 2.13 ▷ Verify that the 'componentwise' product $R_1 \times R_2$ of two rings satisfies the universal property for products in a category, given in §I.5.4. [§2.4]

∎ SOLUTION Let $\pi_1 : (r_1, r_2) \mapsto r_1$ and $\pi_2 : (r_1, r_2) \mapsto r_2$ be the natural projections. If R is any ring with ring homomorphisms $f_1 : R \to R_1$ and $f_2 : R \to R_2$, we ought to find a morphism $\sigma : R \to R_1 \times R_2$ such that the diagram



commutes. Inspired by the proof in Set, we set

$$\sigma(a) := (f_1(a), f_2(a)).$$

This definition manifestly makes the diagram commute. We only have to show that it is a ring homomorphism. For that, let $a, b \in R$. We have that

$$\begin{aligned} \sigma(ab) &= (f_1(ab), f_2(ab)) \\ &= (f_1(a)f_1(b), f_2(a)f_2(b)) \\ &= (f_1(a), f_2(a))(f_1(b), f_2(b)) = \sigma(a)\sigma(b), \end{aligned}$$

since f_1 and f_2 are homomorphisms. The result follows. ∎

EXERCISE 2.14

∎ SOLUTION T ∎

EXERCISE 2.15 ▷ For $m > 1$, the abelian groups $(\mathbb{Z}, +)$ and $(m\mathbb{Z}, +)$ are manifestly isomorphic: the function $\varphi : \mathbb{Z} \to m\mathbb{Z}$, $n \mapsto mn$ is a group isomorphism. Use this isomorphism to transfer the structure of 'ring without identity' $(m\mathbb{Z}, +, \cdot)$ back onto $\mathbb{Z}$: give an explicit formula for the 'multiplication' $\bullet$ this defines on $\mathbb{Z}$ (that is, such that $\varphi(a \bullet b) = \varphi(a) \cdot \varphi(b)$). Explain why structures induced by different positive integers m are nonisomorphic as 'rings without 1'.

(This shows that there are many different ways to give a structure of ring without identity to the *group* $(\mathbb{Z}, +)$. Compare this observation with Exercise 2.6.) [§2.1]

∎ SOLUTION To satisfy the relation $\varphi(a \bullet b) = \varphi(a) \cdot \varphi(b)$, we must define:

$$a \bullet b = \varphi^{-1}(\varphi(a) \cdot \varphi(b)) = mab$$

for all $a, b \in \mathbb{Z}$. Note that we are using the usual multiplication in $\mathbb{Z}$ to compute mab. We can conclude from the relation $\varphi(a \bullet b) = \varphi(a) \cdot \varphi(b)$ and the properties of $\cdot$ that $\bullet$ is associative and distributive over $+$. Therefore, $(\mathbb{Z}, +, \bullet)$ is a 'ring without identity'.

For the second part, let m, n be positive integers and suppose that $(\mathbb{Z}, +, \bullet_m)$ and $(\mathbb{Z}, +, \bullet_n)$ are isomorphic as 'rings without identity', where $\bullet_m$ and $\bullet_n$ are the operations induced by $m\mathbb{Z}$ and $n\mathbb{Z}$, respectively. Then, there is a isomorphism $f : (\mathbb{Z}, +, \bullet_m) \to (\mathbb{Z}, +, \bullet_n)$, which is, in particular, a group isomorphism with respect to $+$. By Exercise 4.15, we know that f is the identity or $f(x) = -x$ for all $x \in \mathbb{Z}$. If we had this last case, then we would get that

$$\begin{aligned} n &= 1 \bullet_n 1 \\ &= (-f(1)) \bullet_n (-f(1)) \\ &= f(1) \bullet_n f(1) \\ &= f(1 \bullet_m 1) \\ &= f(m) \\ &= -m, \end{aligned}$$

which implies that m or n is negative, a contradiction. Therefore, f is the identity and, by a similar computation as the one done above, we have that $m = n$, as desired. We conclude that the structures induced by different positive integers are nonisomorphic as 'rings without 1'. ∎

EXERCISE 2.16

∎ SOLUTION A ∎

EXERCISE 2.17 ¬ Let R be a ring, and let $E = \mathrm{End}_{\mathsf{Ab}}(R)$ be the ring of endomorphisms of the underlying abelian group $(R, +)$. Prove that the center of E is isomorphic to a subring of the center of R. (Prove that if $\alpha \in E$ commutes with all right-multiplications by elements of R, then α is left-multiplication by an element of R; then use Proposition 2.7.)

■ SOLUTION Following the hint, lets suppose that $\alpha \in E$ commutes with all right-multiplications by elements of R. In other words, we suppose that

$$\alpha(ar) = \alpha(a)r$$

for all $a, r \in R$. Taking $a = 1$, we get that

$$\alpha(r) = \alpha(1)r = \lambda_{\alpha(1)}(r),$$

so that α is left-multiplication by $\alpha(1)$. In other words, the following homomorphism

$$\begin{aligned} \varphi : \text{Center of } E &\to R \\ \alpha &\mapsto \alpha(1) \end{aligned}$$

is injective. Now, since every α in the center of E commutes with *both* left- and right-multiplication,

$$\alpha(1)r - r\alpha(1) = \alpha(r) - \alpha(r) = 0 \qquad \text{for all } r \in R,$$

which means that $\operatorname{im}\varphi$ is contained in the center of R. Restricting the codomain we obtain an isomorphism. ■

EXERCISE 2.18

■ SOLUTION T ■

EXERCISE 2.19 Prove that for $n \in \mathbb{Z}$ a positive integer, $\mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z})$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ *as a ring*.

■ SOLUTION By Proposition 2.7, the function

$$\begin{aligned} \lambda : \mathbb{Z}/n\mathbb{Z} &\to \mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z}) \\ r &\mapsto \lambda_r \end{aligned}$$

is an injective ring homomorphism, where λ_r denotes the homomorphism given by $\lambda_r(x) = r \cdot x$ for all $r \in \mathbb{Z}/n\mathbb{Z}$. We claim that λ is surjective. Let α be in $\mathrm{End}_{\mathsf{Ab}}(\mathbb{Z}/n\mathbb{Z})$ and denote $\alpha([1]_n)$ by a. Then,

$$\alpha([m]_n) = m\alpha([1]_n) = ma = a \cdot [m]_n = \lambda_a([m]_n)$$

for all $[m]_n \in \mathbb{Z}/n\mathbb{Z}$, that is, $\alpha = \lambda_a$. Therefore, λ is surjective and so we conclude that it is a ring isomorphism, as desired. ■

3 IDEALS AND QUOTIENT RINGS

EXERCISE 3.1

■ SOLUTION A ■

EXERCISE 3.2 ▷ Let $\varphi : R \to S$ be a ring homomorphism, and let J be an ideal of S. Prove that $I = \varphi^{-1}(J)$ is an ideal of R. [§3.1]

■ SOLUTION It is not hard to simply check that ar and ra are both in I for all $r \in R$ if $a \in I$. However, we can also observe that I is the kernel of

$$R \xrightarrow{\varphi} S \xrightarrow{\pi} S/J,$$

where $\pi : S \to S/J$ is the canonical projection. This implies immediately that I is an ideal. ■

EXERCISE 3.3 ¬ Let $\varphi : R \to S$ be a ring homomorphism, and let J be and ideal of R.

- Show that $\varphi(J)$ need not be an ideal of S.
- Assume that φ is surjective; then prove that $\varphi(J)$ is an ideal of S.
- Assume that φ is surjective, and let $I = \ker \varphi$; thus we may identify S with R/I. Let $\overline{J} = \varphi(J)$, an ideal of R/I by the previous point. Prove that

$$\frac{R/I}{\overline{J}} \cong \frac{R}{I+J}.$$

(Of course this is just a rehash of Proposition 3.11.) [4.11]

■ SOLUTION

- Let $\varphi : \mathbb{Z} \to \mathbb{Q}$ be the inclusion homomorphism. Note that $\mathbb{Z}$ is an ideal of $\mathbb{Z}$ and $\varphi(\mathbb{Z}) = \mathbb{Z}$, which is not an ideal of $\mathbb{Q}$ since $1 \in \mathbb{Z}$ and $\mathbb{Z} \neq \mathbb{Q}$.
- We already know that $\varphi(J)$ is a subgroup of $(S, +)$. Now, let $s \in S$ and $j \in \varphi(J)$ be arbitrary. Since φ is surjective, there are $r \in R$ and $j' \in J$ such that $\varphi(r) = s$ and $\varphi(j') = j$. Since J is an ideal of R, $rj', j'r \in J$, so $sj = \varphi(r)\varphi(j') = \varphi(rj') \in \varphi(J)$ and $js = \varphi(j')\varphi(r) = \varphi(j'r) \in \varphi(J)$. Therefore, $\varphi(J)$ is an ideal of S.
- By the identification of S with R/I, $\overline{J} = \varphi(J)$ corresponds to the ideal J/I. Since $J/I = (I+J)/I$ and $I \subseteq I + J$, it follows from Proposition 3.11 the desired isomorphism. ■

EXERCISE 3.4

■ SOLUTION T ■

EXERCISE 3.5

■ SOLUTION A ■

EXERCISE 3.6 ¬ Let J be a two-sided ideal of the ring $\mathcal{M}_n(R)$ of $n \times n$ matrices over a ring R, and let $I \subseteq R$ be the set of $(1,1)$ entries of matrices in J. Prove that I is a two-sided ideal of R and J consists precisely of those matrices whose entries all belong to I. (Hint: Exercise 3.5.) [3.9]

■ SOLUTION Let a be the $(1,1)$ entry of matrix in J. Multiplying by suitable matrices as in Exercise 3.5, we can assume that this matrix is

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}.$$

If $r \in R$, we can multiply on the left (resp. on the right) by

$$\begin{pmatrix} r & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

to conclude that ra (resp. ar) is in I. That is, I is a two-sided ideal of R.

Also, if a any entry in a matrix in J, we can multiply by suitable matrices in order to make a the $(1,1)$ entry. This implies that $a \in I$. ■

EXERCISE 3.7 Let R be a ring, and let $a \in R$. Prove that Ra is a left-ideal of R and aR is a right-ideal of R. Prove that a is a left-, resp. right-, unit if and only if $R = aR$, resp. $R = Ra$.

■ SOLUTION Note that $Ra \neq \emptyset$ since $a = 1 \cdot a \in Ra$. Furthermore, if $x, y \in Ra$, there are $x', y' \in R$ such that $x = x'a$ and $y = y'a$, so $x - y = x'a - y'a = (x' - y')a \in Ra$. Thus, Ra is a subgroup of $(R, +)$. Finally, for all $r \in R$ and $r'a \in Ra$, we have that $r(r'a) = (rr')a \in Ra$. We conclude that Ra is a left-ideal of R. In the same fashion, we can prove that aR is a right-ideal of R.

For the second part, let $a \in R$ be a left-unit. Thus, there exists $b \in R$ such that $ab = 1$ and so $1 \in aR$. Since aR is a right-ideal, it follows that $r = 1 \cdot r \in aR$ for all $r \in R$ and we have that $R = aR$. Conversely, if $R = aR$, there exists $b \in R$ such that $ab = 1$ and, therefore, a is a left-unit. It can be similarly shown that $a \in R$ is a right-unit if and only if $R = Ra$. ■

EXERCISE 3.8

■ SOLUTION T ■

EXERCISE 3.9

■ SOLUTION A ■

EXERCISE 3.10 ▷ Let $\varphi : k \to R$ be a ring homomorphism, where k is a field and R is a nonzero ring. Prove that φ is *injective*. [§V.4.2, §V.5.2]

■ SOLUTION Observe that $\ker \varphi$ is an ideal of k. Since fields only have $\{0\}$ and k as ideals, it follows that $\ker \varphi = \{0\}$, since a ring homomorphism to a nonzero ring is necessarily non-constant. (It should map identities to identities.) ■

EXERCISE 3.11 Let R be a ring containing $\mathbb{C}$ as a subring. Prove that there are no ring homomorphisms $R \to \mathbb{R}$.

■ SOLUTION Suppose that there were a ring homomorphism $\varphi : R \to \mathbb{R}$. Then, we would have that

$$\varphi(i)^2 = \varphi(i^2) = \varphi(-1) = -\varphi(1) = -1 < 0,$$

a contradiction since $x^2 \geq 0$ for all $x \in \mathbb{R}$. Therefore, there are no ring homomorphisms from R to $\mathbb{R}$. ■

EXERCISE 3.12

■ SOLUTION T ■

EXERCISE 3.13

■ SOLUTION A ■

EXERCISE 3.14 ¬ Prove that the characteristic of an integral domain is either 0 or a prime integer. Do you know any ring of characteristic 1? [V.4.17]

■ SOLUTION Let R be an integral domain of positive characteristic n. Lets suppose that $n = ab$, where $a, b > 1$. Also, let $f : \mathbb{Z} \to R$ be the unique ring homomorphism from $\mathbb{Z}$ to R. Since $\ker f = n\mathbb{Z}$,

$$f(n) = f(ab) = f(a)f(b) = 0.$$

But R is an integral domain, hence either $f(a)$ or $f(b)$ is zero. This contradicts our assumption. Thus n is a prime integer.

If the characteristic of a ring is 1, then it necessarily is the zero-ring. In fact, such a ring has $0 = f(0) = f(1) = 1$, where f is the same homomorphism as before. ■

EXERCISE 3.15 ¬ A ring R is *Boolean* if $a^2 = a$ for all $a \in R$. Prove that $\mathscr{P}(S)$ is Boolean, for every set S (cf. Exercise 1.2). Prove that every nonzero Boolean ring is commutative, and has characteristic 2. Prove that if an integral domain R is Boolean, then $R \cong \mathbb{Z}/2\mathbb{Z}$. [4.23, V.6.3]

■ SOLUTION It is clear that $\mathscr{P}(S)$ is Boolean for every set S since $A^2 = A \cap A = A$ for all $A \subseteq S$.

Let R be a nonzero Boolean ring . Note that $r = r^2 = (-r)^2 = -r$ for all $r \in R$. In particular, $1 = -1$ and so the order of 1 as an element of $(R, +)$ is 2, that is, R is of characteristic 2. Finally, we have that

$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b$$

and this implies that

$$ab + ba = 0 \implies ab = -ba = ba$$

for all $a, b \in R$. Therefore, R is commutative.

For the last part, suppose that R is a Boolean integral domain. If $x \in R$ is nonzero, we conclude from $x^2 = x = x \cdot 1$ that $x = 1$ by the cancellation law. Therefore, R has only two elements and it follows immediately that $R \cong \mathbb{Z}/2\mathbb{Z}$. ■

EXERCISE 3.16

■ SOLUTION T ■

EXERCISE 3.17

■ SOLUTION A ■

4 IDEALS AND QUOTIENTS: REMARKS AND EXAMPLES.

EXERCISE 4.1 ▷ Let R be a ring, and let $\{I_\alpha\}_{\alpha \in A}$ be a family of ideals of R. We let

$$\sum_{\alpha \in A} I_\alpha := \left\{ \sum_{\alpha \in A} r_\alpha \,\middle|\, r_\alpha \in I_\alpha \text{ and } r_\alpha = 0 \text{ for all but finitely many } \alpha \right\}.$$

Prove that $\sum_\alpha I_\alpha$ is an ideal of R and that it is the smallest ideal containing all of the ideals I_α. [§4.1]

■ SOLUTION Distributivity implies immediately that $\sum_\alpha I_\alpha$ is an ideal of R. Now, let I be an ideal of R containing all of the ideals I_α. Since it is a subgroup (of $(R, +)$), it contains $\sum_\alpha I_\alpha$. This means that $\sum_\alpha I_\alpha$ is the smallest ideal containing all of the I_α. ■

EXERCISE 4.2

■ SOLUTION T ■

EXERCISE 4.3 Prove that the ideal $(2, x)$ of $\mathbb{Z}[x]$ is not principal.

■ SOLUTION Suppose that there exists $p(x) \in \mathbb{Z}[x]$ such that $(2, x) = (p(x))$. Since $2 \in (2, x)$, there exists $f(x) \in \mathbb{Z}[x]$ such that $2 = f(x)p(x)$. By Exercise 1.15, $\mathbb{Z}[x]$ is an integral domain, so Exercise 1.14 implies that $\deg(p(x)) = 0$ and there is a nonzero constant $c \in \mathbb{Z}$ such that $p(x) = c$. Since $x \in (2, x)$, there exists $g(x) \in \mathbb{Z}[x]$ such that $x = g(x)p(x) = cg(x)$. Again by Exercise 1.14, $\deg(g(x)) = 1$ and so there are $a, b \in \mathbb{Z}$ such that $g(x) = a + bx$. Thus, since $x = (ac) + (bc)x$, we must have $bc = 1$ and so $c = 1$ or $c = -1$, which are the only units of $\mathbb{Z}$. It follows that $1 \in (2, x)$ and there are $h_1(x), h_2(x) \in \mathbb{Z}[x]$ such that $1 = 2h_1(x) + xh_2(x)$. This implies that the constant term of $2h_1(x)$ equals to 1 because the constant term of $xh_2(x)$ is 0. But all coefficients of $2h_1(x)$ are even and 1 is odd, a contradiction. Therefore, $(2, x)$ cannot be a principal ideal of $\mathbb{Z}[x]$. ■

EXERCISE 4.4

■ SOLUTION A ■

EXERCISE 4.5 ▷ Let I, J be ideals in a ring R, such that $I + J = (1)$. Prove that $IJ = I \cap J$. [§4.1]

■ SOLUTION As we saw in §4.1, $IJ \subseteq I \cap J$. Now, let $a \in I \cap J$. Since $I + J = (1)$, we write $1 = i + j$, where $i \in I$ and $j \in J$. This implies that

$$a = a \cdot 1 = ai + aj \in IJ.$$

The result follows. ■

EXERCISE 4.6

■ SOLUTION T ■

EXERCISE 4.7 ▷ Let $R = k$ be a field. Prove that every nonzero (principal) ideal in $k[x]$ is generated by a unique *monic* polynomial. [§4.2, §VI.7.2]

■ SOLUTION Let I be an ideal of $k[x]$. By Exercise 4.4, I is principal, that is, there exists $f(x) \in k[x]$ such that $I = (f(x))$. If $a \in k$ is the leading coefficient of $f(x)$, take $m(x) = a^{-1}f(x) \in I$. It follows that $m(x)$ is monic and it generates I. Furthermore, if $m'(x)$ is also a monic polynomial that generates I, we have that $m(x)$ divides $m'(x)$ and $m'(x)$ divides $m(x)$. Thus, $\deg(m(x)) = \deg(m'(x))$ and $m'(x) = cm(x)$ for some $c \in k$. Since both of them are monic, we must have $c = 1$ and, therefore, $m(x)$ is unique. ■

EXERCISE 4.8

■ SOLUTION A ■

EXERCISE 4.9 Generalize the result of Exercise 4.8, as follows. Let R be a commutative ring, and let $f(x)$ be a left-zero-divisor in $R[x]$. Prove that $\exists b \in R$, $b \neq 0$, such that $f(x)b = 0$. (Hint: Let $f(x) = a_d x^d + \cdots + a_0$, and let $g(x) = b_e x^e + \cdots + b_0$ be a nonzero polynomial of minimal degree e such that $f(x)g(x) = 0$. Deduce that $a_d g(x) = 0$, and then prove $a_{d-i} g(x) = 0$ for all i, by induction. What does this say about b_e?)

■ SOLUTION Let $f(x)$ and $g(x)$ be as in the hint. Since $f(x)g(x) = 0$, it follows that $a_d b_e = 0$. This implies that the degree of $a_d g(x)$ is less than e. Now, as

$$f(x)(a_d g(x)) = a_d(f(x)g(x)) = 0$$

and $g(x)$ was the nonzero polynomial of minimal degree with this property, we have that $a_d g(x) = 0$. In particular, we have that $a_d b_{e-1} = 0$. Since the coefficient of x^{d+e-1} in $f(x)g(x)$ is $a_d b_{e-1} + a_{d-1} b_e$, this implies that $a_{d-1} b_e = 0$ and thus $a_{d-1} g(x) = 0$. Similarly we conclude that $a_{d-i} g(x) = 0$ for all i.

Since $a_{d-i} g(x) = 0$ for all i, we have in particular that $a_{d-i} b_e = 0$ for all i. In other words, $f(x)b_e = 0$. ■

EXERCISE 4.10

■ SOLUTION T ■

EXERCISE 4.11 Let R be a commutative ring, $a \in R$, and $f_1(x), \ldots, f_r(x) \in R[x]$.

- Prove the equality of ideals

$$(f_1(x), \ldots, f_r(x), x - a) = (f_1(a), \ldots, f_r(a), x - a).$$

- Prove the useful substitution trick

$$\frac{R[x]}{(f_1(x), \ldots, f_r(x), x - a)} \cong \frac{R}{(f_1(a), \ldots, f_r(a))}.$$

(Hint: Exercise 3.3.)

■ SOLUTION

- Let $I = (f_1(x), \ldots, f_r(x), x - a)$ and $J = (f_1(a), \ldots, f_r(a), x - a)$. It suffices to show that the generators of I are in J, and vice versa. Since $x - a$ is monic, we can divide $f_i(x)$ by $x - a$ and so

$f_i(x) = q_i(x)(x-a) + r_i$, where $q_i(x) \in R[x]$ and $r_i \in R$, for all $i \in \{1, \ldots, r\}$. Replacing x by a, we see that $r_i = f_i(a)$, thus

$$f_i(x) = q_i(x)(x-a) + f_i(a) \in J$$

and

$$f_i(a) = f_i(x) - q_i(x)(x-a) \in I$$

for all $i \in \{1, \ldots, r\}$. Therefore, $I = J$.

- Let $\varphi : R[x] \to R$ be the homomorphism of evaluation by a. As in Example 4.7, $\ker \varphi = (x-a)$ and, since φ is surjective,

$$\frac{R[x]}{(x-a)} \cong R.$$

On the other hand, if we take the ideal $J = (f_1(x), \ldots, f_r(x))$ in $R[x]$, we see that $\overline{J} = \varphi(J) = (f_1(a), \ldots, f_r(a))$ and, by Exercise 3.3,

$$\frac{R[x]/(x-a)}{\overline{J}} \cong \frac{R[x]}{J + (x-a)} = \frac{R[x]}{(f_1(x), \ldots, f_r(x), x-a)}.$$

The first isomorphism above implies that

$$\frac{R[x]}{(f_1(x), \ldots, f_r(x), x-a)} \cong \frac{R}{(f_1(a), \ldots, f_r(a))},$$

as desired. ∎

Exercise 4.12

∎ Solution A ∎

Exercise 4.13 ▷ Let R be an integral domain. For all $k = 1, \ldots, n$ prove that $(x_1, \ldots, x_k)$ is prime in $R[x_1, \ldots, x_n]$. [§4.3]

∎ Solution Let $\varphi : R[x_1, \ldots, x_n] \to R[x_{k+1}, \ldots, x_n]$ be the morphism which sets the first k indeterminates to 0. It is clearly surjective and its kernel is $(x_1, \ldots, x_k)$, which implies that

$$\frac{R[x_1, \ldots, x_n]}{(x_1, \ldots, x_k)} \cong R[x_{k+1}, \ldots, x_n].$$

(We can also do this by repeated application of the result in Example 4.7.) Since $R[x_{k+1}, \ldots, x_n]$ is an integral domain (as R is), the result follows. ∎

Exercise 4.14

∎ Solution T ∎

EXERCISE 4.15 Let $\varphi : R \to S$ be a homomorphism of commutative rings, and let $I \subseteq S$ be an ideal. Prove that if I is a prime ideal in S, then $\varphi^{-1}(I)$ is a prime ideal in R. Show that $\varphi^{-1}(I)$ is not necessarily maximal if I is maximal.

■ SOLUTION By Exercise 3.2, we know that $\varphi^{-1}(I)$ is an ideal of R. Now, let $a, b \in R$ be such that $ab \in \varphi^{-1}(I)$, that is, $\varphi(ab) = \varphi(a)\varphi(b) \in I$. Since I is a prime ideal, $\varphi(a) \in I$ or $\varphi(b) \in I$, and so $a \in \varphi^{-1}(I)$ or $b \in \varphi^{-1}(I)$. Therefore, $\varphi^{-1}(I)$ is a prime ideal in R.

Note that $\varphi^{-1}(I)$ need not be maximal if I is maximal. Indeed, consider the inclusion homomorphism $\varphi : \mathbb{Z} \to \mathbb{Q}$. By Exercise 3.8, $I = \{0\}$ is a maximal ideal in $\mathbb{Q}$, but $\varphi^{-1}(I) = \{0\}$ is not maximal in $\mathbb{Z}$. ■

EXERCISE 4.16

■ SOLUTION A ■

EXERCISE 4.17 ¬ (If you know a little topology...) Let K be a compact topological space, and let R be the ring of continuous real-valued functions on K, with addition and multiplication defined pointwise.

(i) For $p \in K$, let $M_p = \{f \in R \mid f(p) = 0\}$. Prove that M_p is a maximal ideal in R.

(ii) Prove that if $f_1, \ldots, f_r \in R$ have no common zeros, then $(f_1, \ldots, f_r) = (1)$. (Hint: Consider $f_1^2 + \cdots + f_r^2$.)

(iii) Prove that every maximal ideal M in R is of the form M_p for some $p \in K$. (Hint: You will use the compactness of K and (ii).)

Conclude that $p \mapsto M_p$ defines a bijection from K to the set of maximal ideals of R. (The set of maximal ideals of a commutative ring R is called the *maximal spectrum* of R; it is contained in the (prime) spectrum Spec R, defined in §4.3. Relating commutative rings and 'geometric' entities such as topological spaces is the business of *algebraic geometry*.)

The compactness hypothesis is necessary: cf. Exercise V.3.10. [V.3.10]

■ SOLUTION

(i) Let $\varphi : R \to \mathbb{R}$ be defined by $f \mapsto f(p)$. This is clearly a surjective (since constant functions are continuous) homomorphism with M_p as kernel. Thus,

$$\frac{R}{M_p} \cong \mathbb{R},$$

which means that M_p is a maximal ideal.

(ii) If $f_1, \ldots, f_r \in R$ have no common zeros, then

$$1 = \frac{f_1^2 + \cdots + f_r^2}{f_1^2 + \cdots + f_r^2} \in (f_1, \ldots, f_r).$$

This implies that $(1) \subseteq (f_1, \ldots, f_r)$ and the result follows.

(iii) Lets suppose that M is a maximal ideal such that $M \nsubseteq M_p$ for all $p \in K$. This implies that for all $p \in K$ we have a continuous function $f_p \in M$ such that $f_p(p) \neq 0$. By continuity, there exists a neighborhood N_p of p such that $f_p(q) \neq 0$ for all $q \in N_p$. The compactness of K implies that $N_{p_1}, \ldots, N_{p_n}$ cover K and thus $f_{p_1}, \ldots, f_{p_n}$ share no common zeros. (Since a common zero would not be in any of the N_{p_k}'s.)

Now, by (ii), $1 \in (f_{p_1}, \ldots, f_{p_n}) \subseteq M$. In other words, $M = R$ and thus M is *not* maximal. This contradiction establishes the result.

The third item says precisely that $p \mapsto M_p$ is a surjective function from K to the maximal spectrum of R. In order to prove injectivity, we need to show that if $p \neq q$ there exists a continuous function f such that $f(p) = 0$ and $f(q) \neq 0$. If K is normal, this is exactly Urysohn's Lemma. Since compact Hausdorff spaces are automatically normal, this suggests that maybe P. Aluffi forgot to add 'Hausdorff' to the hypothesis in the statement of the question. If K is not Hausdorff, there are counter-examples to Urysohn's Lemma. (Any non-normal space suffices.) ∎

EXERCISE 4.18

∎ SOLUTION T ∎

EXERCISE 4.19 Let R be a commutative ring, let P be a prime ideal in R, and let I_j be ideals of R.

(i) Assume that $I_1 \cdots I_r \subseteq P$; prove that $I_j \subseteq P$ for some j.

(ii) By (i), if $P \supseteq \bigcap_{j=1}^{r} I_j$, then P contains one of the ideals I_j. Prove or disprove: if $P \supseteq \bigcap_{j=1}^{\infty} I_j$, then P contains one of the ideals I_j.

∎ SOLUTION

(i) Suppose that none of the ideals I_j is contained in P. Thus, there are $i_j \in I_j$ such that $i_j \notin P$ for all $j \in \{1, \ldots, r\}$. But since $I_1 \cdots I_r \subseteq P$, $i_1 \cdots i_r \in P$ and, since P is a prime ideal, $i_j \in P$ for some $j \in \{1, \cdots, r\}$, a contradiction. Therefore, P must contain one of the ideals I_j.

(ii) Since $I_1 \cdots I_r \subseteq \bigcap_{j=1}^{r} I_j \subseteq P$, it follows from (i) that P contains one of the ideals I_j. However, this statement is not true if we take

an infinite intersection of ideals. For Example, (0) is a prime ideal in $\mathbb{Z}$ since it is an integral domain, and $(0) \supseteq \bigcap_{n=1}^{\infty} n\mathbb{Z}$, but $(0) \not\supseteq n\mathbb{Z}$ for all $n \geq 1$. ∎

EXERCISE 4.20

∎ SOLUTION A ∎

EXERCISE 4.21 ▷ Let k be an algebraically closed field, and let $I \subseteq k[x]$ be an ideal. Prove that I is maximal if and only if $I = (x - c)$ for some $c \in k$. [§4.3, §V.5.2, §VII.2.1, §VII.2.2]

∎ SOLUTION As we saw in Example 4.7,

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

even if k is not algebraically closed. This implies that $(x - c)$ is maximal in $k[x]$ if k is *any* field.

Conversely, let I be a maximal ideal in $k[x]$, where we now suppose that k is algebraically closed. Since $k[x]$ is a PID, $I = (f(x))$ for some $f(x) \in k[x]$. This polynomial is not constant, since it would imply that $I = k[x]$, which is *not* maximal. Now, as $f(x)$ has a root $c \in k$, $f(x) = (x - c)g(x)$ for some $g(x) \in k[x]$. In particular $f(x) \in (x - c)$ and thus $I \subseteq (x - c)$. Finally, since I is maximal, $I = (x - c)$. ∎

EXERCISE 4.22

∎ SOLUTION T ∎

EXERCISE 4.23 A ring R has Krull dimension 0 if every prime ideal in R is maximal. Prove that fields and Boolean rings (Exercise 3.15) have Krull dimension 0.

∎ SOLUTION If K is a field, Exercise 3.8 implies that its only ideals are (0) and K itself. It is clear that the only prime ideal of K is (0) and that it is maximal. Therefore, K has Krull dimension 0.

Let P be a prime ideal of a nonzero Boolean ring R. It follows that R/P is an integral domain and it is clear that it is also Boolean. By Exercise 3.15, $R/P \cong \mathbb{Z}/2\mathbb{Z}$ and, hence, it is indeed a field and so P is maximal. We conclude that nonzero Boolean rings have Krull dimension 0. ∎

EXERCISE 4.24

∎ SOLUTION A ∎

EXERCISE 5.1 ▷ Let R be a ring. The *opposite* ring R° is obtained from R by reversing the multiplication: that is, the product $a \bullet b$ in R° is defined to be $ba \in R$. Prove that the identity map $R \to R^\circ$ is an isomorphism if and only if R is commutative. Prove that $\mathcal{M}_n(\mathbb{R})$ is isomorphic to its opposite (*not* via the identity map!). Explain how to turn right-R-modules into left-R-modules and conversely, if $R \cong R^\circ$. [§5.1, VIII.5.19]

■ SOLUTION The identity map $R \to R^\circ$ is a homomorphism if and only if

$$ab = \mathrm{id}(ab) = \mathrm{id}(a) \bullet \mathrm{id}(b) = \mathrm{id}(b)\,\mathrm{id}(a) = ba,$$

for all $a, b \in R$. In other words, it is a homomorphism if and only if R is commutative.

Finally, the transposition map $A \mapsto A^T$ is an isomorphism from $\mathcal{M}_n(\mathbb{R})$ to its opposite.

Lets say $(M, +, \cdot)$ is a left-R-module and we denote by $r \mapsto r^\circ$ the isomorphism from R to R°. This allows us to define a right-R-module M° whose elements are the same as those of M and whose operations $\oplus$ and $\odot$ are given by

$$m \oplus n = m + n \qquad \text{and} \qquad m \odot r = r^\circ \cdot m.$$

Clearly M and M° are the same as abelian groups. The reader can easily verify that M° also satisfies the axioms in Definition 5.2. ■

EXERCISE 5.2

■ SOLUTION T ■

EXERCISE 5.3 ▷ Let M be a module over a ring R. Prove that $0 \cdot m = 0$ and that $(-1) \cdot m = -m$, for all $m \in M$. [§5.2]

■ SOLUTION By the properties of R-modules, we have that $0 \cdot m = (0 + 0) \cdot m = 0 \cdot m + 0 \cdot m$. It follows from the cancellation law that $0 \cdot m = 0$ for all $m \in M$. Now, note that $m + (-1) \cdot m = 1 \cdot m + (-1) \cdot m = (1 + (-1)) \cdot m = 0 \cdot m = 0 = m + (-m)$. Again by the cancellation law, $(-1) \cdot m = -m$ for all $m \in M$. ■

EXERCISE 5.4

■ SOLUTION A ■

EXERCISE 5.5 Let R be a ring, viewed as an R-module over itself, and let M be an R-module. Prove that $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, M) \cong M$ as R-modules.

■ SOLUTION Observe that any R-module homomorphism $\varphi : R \to M$ satisfies

$$\varphi(r) = \varphi(r \cdot 1) = r\varphi(1)$$

and thus is determined by $\varphi(1)$. This leads us to consider

$$\begin{aligned} f : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R, M) &\to M \\ \varphi &\mapsto \varphi(1). \end{aligned}$$

Our observation says precisely that f is injective. This function is also clearly a surjective morphism of R-modules, hence it is our desired isomorphism. ∎

EXERCISE 5.6

∎ SOLUTION T ∎

EXERCISE 5.7 Let K be a field, and let $k \subseteq K$ be a subfield of K. Show that K is a vector space over k (and in fact a k-algebra) in a natural way. In this situation, we say that K is an *extension* of k.

∎ SOLUTION If we take the inclusion homomorphism $\alpha : k \to K$, we can define $\rho : k \times K \to K$ as in Example 5.6 by

$$\rho(r, s) = rs$$

for all $r \in k$ and $s \in K$, where rs is the multiplication of r and s in K. The axioms of Definition 5.2 are clearly satisfied since K is a field and, thus, K is a vector space over k. Moreover, since k and K are commutative, Definition 5.7 tells us that K is indeed a k-algebra. ∎

EXERCISE 5.8

∎ SOLUTION A ∎

EXERCISE 5.9 ¬ Let R be a commutative ring, and let M be an R-module. Prove that the operation of composition on the R-module $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ makes the latter an R-algebra in a natural way.

Prove that $\mathcal{M}_n(R)$ (cf. Exercise 1.4) is an R-algebra, in a natural way. [VI.1.12, VI.2.3]

∎ SOLUTION Similarly as in Ab, $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ is a ring with addition and composition as operations. Also, since $\mathrm{End}_{R\text{-}\mathsf{Mod}}(M)$ is just another name for $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(M, M)$, it is clearly a R-module, as observed in §5.2. In conclusion, it is an R-algebra in a natural way.

The addition and multiplication of matrices endow $\mathcal{M}_n(R)$ with the structure of a ring. Now, the element-wise multiplication by elements of R promotes $\mathcal{M}_n(R)$ to the status of an R-algebra. ∎

EXERCISE 5.10

∎ SOLUTION T ∎

EXERCISE 5.11 ▷ Let R be a commutative ring, and let M be an R-module. Prove that there is a bijection between the set of $R[x]$-module structures on M (extending the given R-module structure) and $\mathrm{End}_{R\text{-Mod}}(M)$. [§VI.7.1]

■ SOLUTION The set of $R[x]$-module structures on M extending the given R-module structure is in bijection with the set S of ring homomorphisms $\sigma^* : R[x] \to \mathrm{End}_{\mathsf{Ab}}(M)$ such that the restriction of σ^* to R is the ring homomorphism $\sigma : R \to \mathrm{End}_{\mathsf{Ab}}(M)$, which represents the R-module structure on M. Let $\alpha \in \mathrm{End}_{R\text{-Mod}}(M)$. Since $\alpha(rm) = r\alpha(m)$ for all $r \in R$ and $m \in M$, it follows that α commutes with $\sigma(r)$ for all $r \in R$. By Example 2.3 and Exercise 2.6, there exists a unique ring homomorphism $\sigma_\alpha : R[x] \to \mathrm{End}_{\mathsf{Ab}}(M)$ extending σ and sending x to α. Thus, we may define

$$\begin{aligned} f : \mathrm{End}_{R\text{-Mod}}(M) &\longrightarrow S \\ \alpha &\longmapsto \sigma_\alpha. \end{aligned}$$

Now, let $\sigma^* \in S$. We claim that $\sigma^*(x) \in \mathrm{End}_{R\text{-Mod}}(M)$. Indeed, since x commutes with every constant polynomial of $R[x]$, $\sigma^*(x)$ must commute with $\sigma^*(r) = \sigma(r)$ for all $r \in R$. Therefore, $\sigma^*(x)(rm) = r\sigma^*(x)(m)$ for all $r \in R$ and $m \in M$, so $\sigma^*(x) \in \mathrm{End}_{R\text{-Mod}}(M)$ and we can define

$$\begin{aligned} g : S &\longrightarrow \mathrm{End}_{R\text{-Mod}} \\ \sigma^* &\longmapsto \sigma^*(x). \end{aligned}$$

It is clear that f and g are inverses for each other, so they are bijections, as desired. ■

EXERCISE 5.12

■ SOLUTION A ■

EXERCISE 5.13 Let R be an integral domain, and let I be a nonzero *principal* ideal of R. Prove that I is isomorphic to R as an R-module.

■ SOLUTION Let $I = (a)$. Since I is nonzero, so is a. The function

$$\begin{aligned} R &\to I \\ r &\mapsto ra \end{aligned}$$

is clearly a surjective R-module morphism. Since R is an integral domain and $a \neq 0$, $ra = rs$ implies $r = s$ and thus this function is also injective. The result follows. ■

EXERCISE 5.14

■ SOLUTION T ■

EXERCISE 5.15 Let R be a commutative ring, and let I, J be ideals of R. Prove that $I \cdot (R/J) \cong (I+J)/J$ as R-modules.

■ SOLUTION We will prove that $I \cdot (R/J) \cong I/(I \cap J)$ and the exercise will be a consequence of Proposition 5.18. Let $\varphi : I \to I \cdot (R/J)$ be given by

$$\varphi(i) = i(1+J)$$

for all $i \in I$. Note that φ is a homomorphism of R-modules since

$$\varphi(i_1 + i_2) = (i_1 + i_2)(1+J) = i_1(1+J) + i_2(1+J) = \varphi(i_1) + \varphi(i_2)$$

and

$$\varphi(ri) = (ri)(1+J) = r(i(1+J)) = r\varphi(i)$$

for all $i_1, i_2, i \in I$ and $r \in R$. Moreover, it is surjective because, given $\sum_{k=1}^{n} i_k(r_k + J) \in I \cdot (R/J)$, we have that

$$\varphi\Big(\sum_{k=1}^{n} i_k r_k\Big) = \sum_{k=1}^{n} i_k r_k (1+J) = \sum_{k=1}^{n} i_k (r_k + J)$$

and $\sum_{k=1}^{n} i_k r_k \in I$ since I is an ideal of R. By Corollary 5.16,

$$I \cdot (R/J) \cong \frac{I}{\ker \varphi}$$

and note that

$$\begin{aligned}
\ker \varphi &= \{i \in I \mid \varphi(i) = 0_{I\cdot(R/J)}\} \\
&= \{i \in I \mid i(1+J) = J\} \\
&= \{i \in I \mid (i+J) = J\} \\
&= \{i \in I \mid i \in J\} \\
&= I \cap J,
\end{aligned}$$

as desired. ■

EXERCISE 5.16

■ SOLUTION A ■

EXERCISE 5.17 ▷ Let R be a commutative ring, and let I be an ideal of R. Noting that $I^j I^k \subseteq I^{j+k}$, define a ring structure on the direct sum

$$\mathrm{Rees}_R(I) := \bigoplus_{j \geq 0} I^j = R \oplus I \oplus I^2 \oplus I^3 \oplus \cdots .$$

The homomorphism sending R identically to the first term in this direct sum makes $\mathrm{Rees}_R(I)$ into an R-algebra, called the *Rees algebra* of I. Prove that if $a \in R$ is a non-zero-divisor, then the Rees algebra of (a) is isomorphic to the polynomial ring $R[x]$ (as an R-algebra). [5.18]

■ SOLUTION The condition that $I^j I^k \subseteq I^{j+k}$ (which is clear, since we even have equality) hints that we can define in $\mathrm{Rees}_R(I)$ a ring structure based on the polynomial ring. That is, we do element-wise addition and 'polynomial' multiplication. We then write an element of $\mathrm{Rees}_R(I)$ as

$$r + i_1 + i_2 + i_3 + \dots,$$

where this sum is finite (since $\mathrm{Rees}_R(I)$ is a direct sum), r is an element of R, and i_k is a *finite sum* of products of k elements of I. The 'polynomial' multiplication in $\mathrm{Rees}_R(I)$ amounts to forcing the distributive law to hold in this notation. This makes it clear that this is in fact a ring. It is an R-algebra in exactly the same way that $R[x]$ is.

If $a \in R$ is a non-zero-divisor, an element of $\mathrm{Rees}_R((a))$ can be written as

$$r_0 + r_1 a + r_2 a^2 + r_3 a^3 + \dots,$$

where the r_k are in R and this sum is finite. It is clear that

$$r_0 + r_1 a + r_2 a^2 + \dots + r_n a^n \mapsto r_0 + r_1 x + r_2 x^2 + \dots + r_n x^n$$

is an isomorphism of R-algebras. ■

EXERCISE 5.18

■ SOLUTION T ■

6 PRODUCTS, COPRODUCTS, ETC., IN R-MOD

EXERCISE 6.1

■ SOLUTION A ■

EXERCISE 6.2 Prove or disprove that if R is a ring and M is a nonzero R-module, then M is not isomorphic to $M \oplus M$.

■ SOLUTION Take $R = \mathbb{Z}$ and $M = \mathbb{Z}^{\oplus \mathbb{N}}$. We can utilize Exercise 6.5 to conclude that

$$M \oplus M \cong \mathbb{Z}^{\oplus \mathbb{N}^2} \cong \mathbb{Z}^{\oplus \mathbb{Z}} = M.$$

Nevertheless, we can also construct this isomorphism explicitly: let

$$\varphi : M \to M \oplus M$$

be defined by sending $\varphi \in M$ to $(n \mapsto \varphi(2n), n \mapsto \varphi(2n-1))$. This is clearly a R-module isomorphism. ■

EXERCISE 6.3 Let R be a ring, M an R-module, and $p : M \to M$ an R-module homomorphism such that $p^2 = p$. (Such a map is called a *projection*.) Prove that $M \cong \ker p \oplus \operatorname{im} p$.

■ SOLUTION Define $\varphi : \ker p \oplus \operatorname{im} p \to M$ by

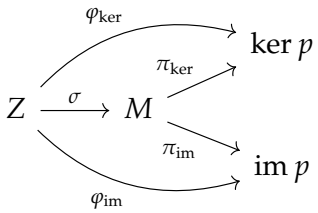
$$\varphi(k, i) = k + i$$

for all $k \in \ker p$ and $i \in \operatorname{im} p$. It is clear that φ is a homomorphism of R-modules. Let's prove it is indeed an isomorphism. Firstly, given $k, k' \in \ker p$, $i, i' \in \operatorname{im} p$, there are $m, m' \in M$ such that $i = p(m)$ and $i' = p(m')$, so

$$\begin{aligned} \varphi(k, i) = \varphi(k', i') &\implies k + i = k' + i' \\ &\implies p(k + i) = p(k' + i') \\ &\implies p(k) + p^2(m) = p(k') + p^2(m') \\ &\implies p(m) = p(m') \\ &\implies i = i' \text{ and } k = k' \end{aligned}$$

and it follows that φ is injective. Now, given $m \in M$, we have that $m = (m - p(m)) + p(m)$. Since $p(m - p(m)) = p(m) - p^2(m) = p(m) - p(m) = 0$, $m - p(m) \in \ker p$ and so $\varphi(m - p(m), p(m)) = m$, implying that φ is also surjective. Therefore, φ is an isomorphism and we have that $M \cong \ker p \oplus \operatorname{im} p$.

We can also prove the desired isomorphism using the universal property of the product of $\ker p$ and $\operatorname{im} p$ in R-Mod. Take $\pi_{\ker} : M \to \ker p$ as $\pi_{\ker}(m) = m - p(m)$ and $\pi_{\text{im}} : M \to \operatorname{im} p$ as $\pi_{im}(m) = p(m)$, for all $m \in M$. Note that $\pi_{\ker}$ really is a homomorphism and that $m - p(m) \in \ker p$ since $p^2 = p$. Now, let Z be an R-module and $\varphi_{\ker} : Z \to \ker p$, $\varphi_{\text{im}} : Z \to \operatorname{im} p$ be homomorphisms of R-modules. If $\sigma : Z \to M$ is an R-module homomorphism such that the diagram



commutes, we have that

$$\begin{aligned} \sigma(m) &= (\sigma(m) - p(\sigma(m))) + p(\sigma(m)) \\ &= (\pi_{\ker} \circ \sigma)(m) + (\pi_{\text{im}} \circ \sigma)(m) \\ &= \varphi_{\ker}(m) + \varphi_{\text{im}}(m) \end{aligned}$$

for all $m \in M$. Thus, σ is uniquely determined by the commutativity of the diagram and it is immediate that setting σ as above really defines an R-module homomorphism. Therefore, M with $\pi_{\ker}$ and π_{im} satisfies the universal property of the product of $\ker p$ and $\operatorname{im} p$ in R-Mod, and so $M \cong \ker p \oplus \operatorname{im} p$. ■

EXERCISE 6.4

■ SOLUTION T ■

EXERCISE 6.5

■ SOLUTION A ■

EXERCISE 6.6 ¬ Let R be a ring, and let $F = R^{\oplus n}$ be a finitely generated free R-module. Prove that $\mathrm{Hom}_{R\text{-Mod}}(F, R) \cong F$. On the other hand, find an example of a ring R and a nonzero R-module M such that $\mathrm{Hom}_{R\text{-Mod}}(M, R) = 0$. [6.8]

■ SOLUTION Following §6.3, we write $j(i)$ for the vector

$$(0, 0, \ldots, 1, \ldots, 0),$$

where the 1 is in the i-th place. (In linear algebra *lingo*, this is the i-th element of the *canonical basis*.) Observe that any element $r \in F$ can be written as

$$r = (r_1, r_2, \ldots, r_n) = r_1 j(1) + r_2 j(2) + \ldots + r_n j(n).$$

We conclude that any morphism $\varphi \in \mathrm{Hom}_{R\text{-Mod}}(F, R)$ satisfies

$$\varphi(r) = r_1 \varphi(j(1)) + r_2 \varphi(j(2)) + \ldots + r_n \varphi(j(n))$$

and thus is determined by the data of $\varphi(j(i))$ for all i. In other words, the function

$$\begin{aligned} \mathrm{Hom}_{R\text{-Mod}}(F, R) &\to F \\ \varphi &\mapsto (\varphi(j(1)), \varphi(j(2)), \ldots, \varphi(j(n))) \end{aligned}$$

is injective. Since the map that assigns

$$(r_1, r_2, \ldots, r_n) \mapsto r_1 e_1 + r_2 e_2 + \ldots + r_n e_n$$

to $(e_1, e_2, \ldots, e_n)$ is its inverse, we conclude that it is bijective. Moreover, since its clear that this is an morphism of R-modules, this is the desired isomorphism.

Finally, consider $M = \mathbb{Q}$ as a $\mathbb{Z}$-module. If $\varphi \in \mathrm{Hom}_{\mathbb{Z}\text{-Mod}}(\mathbb{Q}, \mathbb{Z})$, then

$$f(r) = 2^n f\left(\frac{r}{2^n}\right),$$

so that $f(r)$ is an integer divisible by 2^n for all n. This implies that $f(r) = 0$ for all $r \in \mathbb{Q}$. In other words, $\mathrm{Hom}_{\mathbb{Z}\text{-Mod}}(\mathbb{Q}, \mathbb{Z}) = 0$. ■

The R-module $\mathrm{Hom}_{R\text{-Mod}}(M, R)$ is called the *dual module* of M and is denoted by $M^\vee$.

EXERCISE 6.7 ▷ Let A be any set.

- For any family $\{M_a\}_{a \in A}$ of modules over a ring R, define the *product* $\prod_{a \in A} M_a$ and coproduct $\bigoplus_{a \in A} M_a$. If $M_a \cong R$ for all $a \in A$, these are denoted R^A, $R^{\oplus A}$, respectively.
- Prove that $\mathbb{Z}^{\mathbb{N}} \ncong \mathbb{Z}^{\oplus \mathbb{N}}$. (Hint: Cardinality.)

[§6.1, 6.8]

■ SOLUTION

- The definitions of products and coproducts in R-Mod are the same as the ones given for general categories in Exercise I.5.10. Thus, the product $\prod_{a\in A} M_a$ with R-module homomorphisms $\{\pi_j : \prod_{a\in A} M_a \to M_j\}_{j\in A}$ satisfies the following universal property: for every R-module Z and R-module homomorphisms $\{f_j : Z \to M_j\}_{j\in A}$ there exists a unique homomorphism $\sigma : Z \to \prod_{a\in A} M_a$ such that $\pi_j \circ \sigma = f_j$ for all $j \in A$.

  Similarly, the coproduct $\bigoplus_{a\in A} M_a$ with R-module homomorphisms $\{i_j : M_j \to \bigoplus_{a\in A} M_a\}_{j\in A}$ satisfies the following universal property: for every R-module Z and morphisms $\{f_j : M_j \to Z\}_{j\in A}$ there exists a unique homomorphism $\sigma : \bigoplus_{a\in A} M_a \to Z$ such that $\sigma \circ i_j = f_j$ for all $j \in A$.

  As usual, they do exist in R-Mod. The product is the module obtained by endowing

$$\prod_{a\in A} M_a = \left\{ f : A \to \bigcup_{a\in A} M_a \,\middle|\, (\forall a \in A) : f(a) \in M_a \right\}$$

  with the usual operations and the coproduct is the submodule of $\prod_{a\in A} M_a$ given by the functions f such that $f(a) \neq 0$ for only finitely many $a \in A$. The projections π_j and the inclusions i_j are similar to the case with just two modules. Moreover, the proof that they satisfy the corresponding universal properties is analogous to the proof of Proposition 6.1.

- We claim that $\mathbb{Z}^{\oplus\mathbb{N}}$ is countable as a set, that is, there is a bijective set-function between $\mathbb{N}$ and $\mathbb{Z}^{\oplus\mathbb{N}}$. Let X_n be defined by

$$X_n = \{f \in \mathbb{Z}^{\oplus\mathbb{N}} | (\forall m \geq n) : f(m) = 0\}$$

  for all $n \geq 1$. There is a natural injection $\varphi_n : X_n \to \mathbb{Z}^n$ such that $\varphi_n(f) = (f(0), \ldots, f(n-1))$ for all $f \in X_n$. Since $\mathbb{Z}$ is countable and φ_n is injective, $\mathbb{Z}^n$ is also countable and, thus, X_n is countable for all $n \geq 1$. Finally, note that $\mathbb{Z}^{\oplus\mathbb{N}} = \bigcup_{n\geq 1} X_n$, which is a countable union of countable sets. Therefore, $\mathbb{Z}^{\oplus\mathbb{N}}$ is countable. By the Remark below, $\mathbb{Z}^{\mathbb{N}}$ is not countable and so we conclude that $\mathbb{Z}^{\mathbb{N}} \ncong \mathbb{Z}^{\oplus\mathbb{N}}$. ■

Remark. In the proof above, we used some results about countable sets that we did not prove. Their proof do not fit here and the reader is encouraged to check these results in other books. However, we shall prove one of them, which involves the famous Cantor's diagonal argument.

Proposition. Let A and B be sets such that $A \neq \emptyset$ and B has at least two distinct elements. Then, any function $f : A \to B^A$ cannot be surjective.

Proof. Let $b, b' \in B$ be two distinct elements of B. Given $f : A \to B^A$, define $\varphi : A \to B$ by

$$\varphi(x) = \begin{cases} b', \text{ if } (f(x))(x) = b \\ b, \text{ otherwise} \end{cases}$$

for all $x \in A$. Note that $\varphi \in B^A$ and that $\varphi(x) \neq (f(x))(x)$ for all $x \in A$. Therefore, $\varphi \notin \operatorname{im} f$ and it follows that f is not surjective.

The German mathematician Georg Cantor (1845-1918) proved this result and used it to show, for example, that the set of the real numbers is uncountable and that $\mathcal{P}(A)$ has a strictly greater cardinality than A itself, for every set A. In our case, we can use it to show that there is no bijection between $\mathbb{N}$ and $\mathbb{Z}^{\mathbb{N}}$, so $\mathbb{Z}^{\mathbb{N}}$ is not countable.

EXERCISE 6.8

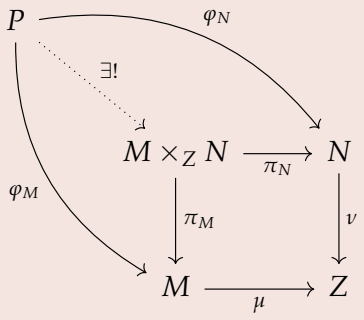
■ SOLUTION T ■

EXERCISE 6.9

■ SOLUTION A ■

EXERCISE 6.10 ▷ (Cf. Exercise I.5.12.) Let M, N, and Z be R-modules, and let $\mu : M \to Z$, $\nu : N \to Z$ be homomorphisms of R-modules.

Prove that R-Mod has 'fibered products': there exists an R-module $M \times_Z N$ with R-module homomorphisms $\pi_M : M \times_Z N \to M$, $\pi_N : M \times_Z N \to N$, such that $\mu \circ \pi_M = \nu \circ \pi_N$, and which is universal with respect to this requirement. That is, for each R-module P and R-module homomorphisms $\varphi_M : P \to M$, $\varphi_N : P \to N$ such that $\mu \circ \varphi_M = \nu \circ \varphi_N$, there exists a unique R-module homomorphism $P \to M \times_Z N$ making the diagram



commute. The module $M \times_Z N$ may be called the *pull-back* of M along ν (or of N along μ, since the construction is symmetric). 'Fiber diagrams'

$$\begin{array}{ccc} M \times_Z N & \longrightarrow & N \\ \downarrow & \square & \downarrow \nu \\ M & \xrightarrow[\mu]{} & Z \end{array}$$

are commutative, but 'even better' than commutative; they are often decorated by a square, as shown here. [§6.1, 6.11, §IX.1.4]

■ SOLUTION As we did in Exercise I.5.12, we define the module $M \times_Z N$ as

$$M \times_Z N := \{(x, y) \in M \oplus N \mid \mu(x) = \nu(y)\}$$

and the projections π_M and π_N as the restrictions of the projections from $M \oplus N$ to M and N, respectively. Since we already proved most of this in Set, we only have to prove that $M \times_Z N$ is actually an R-module and that the morphism $P \to M \times_Z N$ is a morphism of R-modules.

In order to prove that $M \times ZN$ is a submodule of $M \oplus N$, it suffices to show that $r_1(x_1, y_1) + r_2(x_2, y_2)$ is in $M \times_Z N$ as long as $(x_1, y_1), (x_1, y_2) \in M \times_Z N$ and $r_1, r_2 \in R$. In other words, that

$$\mu(r_1 x_1 + r_2 x_2) = \nu(r_1 y_1 + r_2 y_2).$$

This follows from the fact that μ and ν are homomorphisms of R-modules.

As before, the commutativity of the diagram forces the morphism $P \to M \times_Z N$ to be

$$z \mapsto (\varphi_M(z), \varphi_N(z)),$$

which is clearly a morphism of R-modules. ■

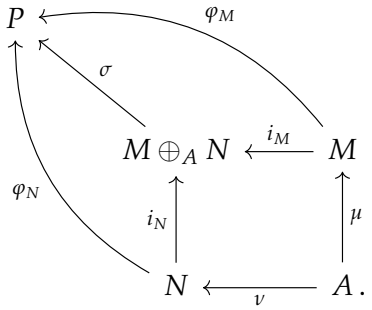
EXERCISE 6.11 ▷ Define a notion of *fibered coproduct* of two R-modules M, N, along an R-module A, in style of Exercise 6.10 (and cf. Exercise I.5.12)

$$\begin{array}{ccc} A & \xrightarrow{\nu} & N \\ {\scriptstyle\mu}\downarrow & & \downarrow \\ M & \longrightarrow & M \oplus_A N \end{array}$$

Prove that fibered coproducts exist in R-Mod. The fibered coproduct $M \oplus_A N$ is called the *push-out* of M along ν (or of N along μ). [§6.1]

■ SOLUTION We define fibered coproducts similarly to the previous exercise. Let M, N and A be R-modules and $\mu : A \to M$, $\nu : A \to N$ be homomorphisms of R-modules. A module $M \oplus_A N$ with R-module

homorphisms $i_M : M \to M \oplus_A N$, $i_N : N \to M \oplus_A N$ is a fibered coproduct of M and N along A if $i_M\mu = i_N\nu$ and the following universal property is satisfied: for every R-module P and R-module homomorphisms $\varphi_M : M \to P$, $\varphi_N : N \to P$ such that $\varphi_M\mu = \varphi_N\nu$, there exists a unique R-module homomorphism $\sigma : M \oplus_A N \to P$ making the diagram below commute:



The proof of the existence of fibered coproducts in R-Mod is similar to Exercise II.3.9. Let $i_M^* : M \to M \oplus N$, $i_N^* : N \to M \oplus N$ be the natural injections of M and N into $M \oplus N$. Let $S \subseteq M \oplus N$ be the submodule generated by the elements of the form

$$(i_M^* \circ \mu)(x) - (i_N^* \circ \nu)(x)$$

for all $x \in A$. We define

$$M \oplus_A N = (M \oplus N)/S$$

and, if π is the canonical projection to the quotient, we take $i_M = \pi i_M^*$ and $i_N = \pi i_N^*$. Note that $i_M\mu = i_N\nu$ by the definition of S.

Let P be another R-module together with R-module homomorphisms $\varphi_M : M \to P$, $\varphi_N : N \to P$ such that $\varphi_M\mu = \varphi_N\nu$. By the universal property of coproducts in R-Mod, there exists a unique R-module homomorphism $\varphi : M \times N \to P$ such that $\varphi_M = \varphi i_M^*$ and $\varphi_N = \varphi i_N^*$. Let's show that $S \subseteq \ker\varphi$. Since S is generated by the elements of the form given above, it suffices to show that they are in this kernel. Since $\varphi_M\mu = \varphi_N\nu$,

$$\begin{aligned}\varphi((i_M^*\mu)(x) - (i_N^*\nu)(x)) &= ((\varphi i_M^*)\mu)(x) - ((\varphi i_N^*)\nu)(x)\\ &= (\varphi_M\mu)(x) - (\varphi_N\nu)(x)\\ &= 0_P\end{aligned}$$

for all $x \in A$, and it follows that $S \subseteq \ker\varphi$. By Theorem 5.14, there exists a unique R-module homomorphism $\sigma : M \oplus_A N \to P$ such that $\varphi = \sigma\pi$. Hence, the diagram shown above commutes because

$$\sigma i_M = \sigma(\pi i_M^*) = (\sigma\pi)i_M^* = \varphi i_M^* = \varphi_M$$

and, similarly, $\sigma i_N = \varphi_N$. Finally, suppose that there exists another $\rho : M \oplus_A N \to P$ such that the diagram above commutes. Since

$\varphi_M = \rho i_M = (\rho\pi)i_M^*$ and $\varphi_N = \rho i_N = (\rho\pi)i_N^*$, the uniqueness of φ and σ implies that $\varphi = \rho\pi$ and so $\rho = \sigma$. Therefore, σ is the only homomorphism such that the diagram above commutes. We conclude that $M \oplus_A N$ with i_M and i_N is the desired fibered coproduct. ∎

EXERCISE 6.12

∎ SOLUTION T ∎

EXERCISE 6.13

∎ SOLUTION A ∎

EXERCISE 6.14 ▷ Prove that the ideal $(x_1, x_2, \dots)$ of the ring $R = \mathbb{Z}[x_1, x_2, \dots]$ is not finitely generated (as an ideal, i.e., as an R-module). [§6.4]

∎ SOLUTION Let $I = (x_1, x_2, \dots)$ and lets suppose that I is finitely generated. In other words, there is a finite set $S = \{f_1, \dots, f_n\} \subset I$ such that $I = \langle S \rangle$. Since S is finite, there's a finite number of the x_i appearing in $f_1, \dots, f_n$. Let x_k be such that x_i does not appear in the polynomials of S for $i \geq k$.

Since $x_k \in I$, we can write

$$x_k = f_1 h_1 + \dots + f_n h_n,$$

for polynomials $h_1, \dots, h_n \in R$. By evaluating every variable *except* x_k to 0 we find that

$$x_k = 0,$$

which is an absurd. The result follows. ∎

EXERCISE 6.15 ▷ Let R be a commutative ring. Prove that a *commutative* R-algebra S is finitely generated *as an algebra* over R if and only if it is finitely generated *as a commutative algebra* over R. (Cf. §6.5.) [§6.5]

∎ SOLUTION ($\Longleftarrow$) Suppose that S is finitely generated as a commutative algebra over R. Thus, there exists a surjective homomorphism of R-algebras $\varphi : R[x_1, \dots, x_n] \to S$ for some $n \in \mathbb{N}$. On the other hand, by the universal property of free algebras, there exists an R-algebra homomorphism $\psi : R\langle x_1, \dots, x_n \rangle \to R[x_1, \dots, x_n]$ such that $\psi(x_i) = x_i$ for all $i \in \{1, \dots, n\}$. We claim that ψ is surjective. Indeed, every polynomial $p(x) \in R[x_1, \dots, x_n]$ can be viewed as a polynomial in $R\langle x_1, \dots, x_n \rangle$ and, since ψ is a homomorphism and it preserves the indeterminates, it follows that $\psi(p(x)) = p(x)$ and ψ is surjective. Therefore, $\varphi \circ \psi$ is a surjective homomorphism from $R\langle x_1, \dots, x_n \rangle$ to S and we conclude that S is finitely generated as an algebra over R.

($\Longrightarrow$) Assume that R is finitely generated as an algebra over R. Thus, there exists a surjective homomorphism of R-algebras φ :

$R\langle x_1, \ldots, x_n\rangle \to S$. If $j : \{1, \ldots, n\} \to R\langle x_1, \ldots, x_n\rangle$ denotes the inclusion from $\{1, \ldots, n\}$ to $R\langle x_1, \ldots, x_n\rangle$, we can take the function $f = \varphi \circ j$. Since S is commutative, this induces a function $\varphi^* : R[x_1, \ldots, x_n] \to S$ such that $f = \varphi^* \circ j^*$, where $j^* : \{1, \ldots, n\} \to R[x_1, \ldots, x_n]$ denotes the inclusion from $\{1, \ldots, n\}$ to $R[x_1, \ldots, x_n]$. Let ψ be as in the previous paragraph. We claim that the following diagram commutes:

$$\begin{array}{ccc} R\langle x_1, \ldots, x_n\rangle & \xrightarrow{\varphi} & S \\ \psi \downarrow & \nearrow_{\varphi^*} & \\ R[x_1, \ldots, x_n] & & \end{array} .$$

By the definition of ψ, we have that $j^* = \psi \circ j$ and so $(\varphi^* \circ \psi) \circ j = \varphi^* \circ j^* = f$. By the universal property of free algebras, φ is the unique homomorphism satisfying this relation and, hence, $\varphi = \varphi^* \circ \psi$, that is, the diagram commutes. Therefore, since φ is surjective, we conclude that φ^* is also surjective and so S is finitely generated as a commutative algebra over R. ∎

EXERCISE 6.16

∎ SOLUTION T ∎

EXERCISE 6.17

∎ SOLUTION A ∎

EXERCISE 6.18 ▷ Let M be an R-module, and let N be a submodule of M. Prove that if N and M/N are both finitely generated, then M is finitely generated. [§6.4]

∎ SOLUTION Lets says that N is generated by $x_1, \ldots, x_n$ and M/N by $y_1 + N, \ldots, y_m + N$. If x is any element of M, then there exist $r_1, \ldots, r_m \in R$ such that

$$x + N = r_1 y_1 + \ldots + r_m y_m + N.$$

Now, since $x - (r_1 y_1 + \ldots + r_m y_m) \in N$, there exist $s_1, \ldots, s_n \in R$ such that

$$x - (r_1 y_1 + \ldots + r_m y_m) = s_1 x_1 + \ldots + s_n x_n.$$

This implies that M is generated by $x_1, \ldots, x_n, y_1, \ldots, y_m$. ∎

Remark. We can also prove it in a more abstract way if the reader has already seen the results in section 7. By the hypothesis of the exercise's statement, we have the following morphisms:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^{\oplus n} & \hookrightarrow & R^{\oplus n} \oplus R^{\oplus m} & \twoheadrightarrow & R^{\oplus m} & \longrightarrow & 0 \\ & & \downarrow & & & & \downarrow & & \\ 0 & \longrightarrow & N & \hookrightarrow & M & \twoheadrightarrow & M/N & \longrightarrow & 0, \end{array}$$

where both rows are clearly exact. If we had a (not necessarily surjective) morphism $R^{\oplus n} \oplus R^{\oplus m} \to M$ in the middle column making this diagram commute, the snake lemma (Lemma 7.8) would imply that it is surjective, proving that M is finitely generated. (We can also use the result from Exercise 7.13.)

This morphism can be obtained in the following way: we obtain a morphism (called a *lift*) $R^{\oplus m} \to M$, which makes

$$\begin{array}{ccc} R^{\oplus m} & \twoheadrightarrow & M/N \\ & \searrow & \uparrow \\ & & M \end{array}$$

commute, by defining it on each $j(i)$ (notation of §6.3) and using the surjectivity. Then, by considering the direct sum of this morphism and of

$$R^{\oplus n} \twoheadrightarrow N \hookrightarrow M,$$

we obtain the desired morphism. The reader will observe that the universal property of the coproduct is exactly what is needed to have commutativity.

7 COMPLEXES AND HOMOLOGY

EXERCISE 7.1

■ SOLUTION T ■

EXERCISE 7.2

■ SOLUTION A ■

EXERCISE 7.3 Assume that the complex

$$\cdots \longrightarrow 0 \longrightarrow L \longrightarrow M \xrightarrow{\varphi} M' \longrightarrow N \longrightarrow 0 \longrightarrow \cdots$$

is exact. Show that, up to natural identifications, $L = \ker \varphi$ and $N = \operatorname{coker} \varphi$.

■ SOLUTION Let $\alpha : L \to M$ be the homomorphism preceding φ in the complex. By Example 7.1, α is injective and so we may identity L with $\operatorname{im} \alpha$. Since the complex is exact, $\operatorname{im} \alpha = \ker \varphi$ and it follows that $L = \ker \varphi$.

Now, let $\beta : M' \to N$ be the homomorphism after φ in the complex. By Example 7.2 and Corollary 5.16, β is surjective and so we may identity N with $M'/\ker \beta$. Since the complex is exact, $\ker \beta = \operatorname{im} \varphi$ and it follows that $N = M'/\operatorname{im} \varphi = \operatorname{coker} \varphi$. ■

EXERCISE 7.4 Construct short exact sequences of $\mathbb{Z}$-modules

$$0 \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow \mathbb{Z} \longrightarrow 0$$

and

$$0 \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow \mathbb{Z}^{\oplus\mathbb{N}} \longrightarrow 0.$$

(Hint: David Hilbert's Grand Hotel.)

■ SOLUTION Since, as we saw in §7.2, $0 \to A \to A \oplus B \to B \to 0$ is an exact sequence, it suffices to show that

$$\mathbb{Z}^{\oplus\mathbb{N}} \cong \mathbb{Z}^{\oplus\mathbb{N}} \oplus \mathbb{Z} \quad \text{and} \quad \mathbb{Z}^{\oplus\mathbb{N}} \cong \mathbb{Z}^{\oplus\mathbb{N}} \oplus \mathbb{Z}^{\oplus\mathbb{N}}.$$

The first isomorphism consists of simply sending $\varphi \in \mathbb{Z}^{\oplus\mathbb{N}}$ to $(n \mapsto \varphi(n+1), \varphi(1))$. The second isomorphism was established in Exercise 6.2. ■

EXERCISE 7.5

■ SOLUTION A ■

EXERCISE 7.6

■ SOLUTION T ■

EXERCISE 7.7 ▷ Let

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

be a short exact sequence of R-modules, and L be an R-module.

(i) Prove that there is an exact sequence

$$0 \to \mathrm{Hom}_{R\text{-Mod}}(P, L) \to \mathrm{Hom}_{R\text{-Mod}}(N, L) \to \mathrm{Hom}_{R\text{-Mod}}(M, L).$$

(ii) Redo Exercise 6.17.

(Use the exact sequence $0 \to I \to R \to R/I \to 0$.)

(iii) Construct an example showing that the rightmost homomorphism in (i) need not be onto.

(iv) Show that if the original sequence splits, then the rightmost homomorphism in (i) *is* onto.

■ SOLUTION

(i) Let $\alpha : M \to N$ and $\beta : N \to P$ be the homomorphisms of the exact sequence. Define

$$\varphi : \mathrm{Hom}_{R\text{-Mod}}(P, L) \to \mathrm{Hom}_{R\text{-Mod}}(N, L)$$
$$f \longmapsto f \circ \beta$$

and

$$\psi : \mathrm{Hom}_{R\text{-Mod}}(N, L) \to \mathrm{Hom}_{R\text{-Mod}}(M, L)$$
$$g \longmapsto g \circ \alpha.$$

It is clear that both φ and ψ are homomorphisms of R-modules (or abelian groups, depending on the case). Let's prove that the corresponding sequence is exact.

Firstly, we claim that it is exact at $\mathrm{Hom}_{R\text{-Mod}}(P, L)$. Suppose $f \in \mathrm{Hom}_{R\text{-Mod}}(P, L)$ is such that $\varphi(f) = 0$, that is, $f \circ \beta = 0$, where 0 denotes the trivial homomorphism. By the exactness of the first sequence, β is surjective and so it has a right-inverse β' as set-function. It follows that

$$f = f(\beta\beta') = (f\beta)\beta' = 0 \circ \beta' = 0$$

and so $\ker \varphi = \{0\}$, as desired.

Now, let's prove that it is exact at $\mathrm{Hom}_{R\text{-Mod}}(N, L)$. Take $g \in \mathrm{im}\, \varphi$, that is, $g = f \circ \beta$ for some $f \in \mathrm{Hom}_{R\text{-Mod}}(P, L)$. By the exactness of the first sequence, $\beta \circ \alpha = 0$ and so

$$\psi(g) = g \circ \alpha = f \circ (\beta \circ \alpha) = f \circ 0 = 0.$$

Thus, $g \in \ker \psi$ and $\mathrm{im}\, \varphi \subseteq \ker \psi$. On the other hand, if $g \in \ker \psi$, then $g \circ \alpha = 0$. This implies that $\mathrm{im}\, \alpha \subseteq \ker g$ and, by Theorem 5.14, there exists a homomorphism $f : N/\mathrm{im}\, \alpha \to L$ such that $g = f \circ \pi$, where π is the canonical projection. But we know that $\mathrm{im}\, \alpha = \ker \beta$ and, since β is surjective, Corollary 5.16 tells us that $N/\mathrm{im}\, \alpha = N/\ker \beta \cong P$. Therefore, we can naturally identify π as β and the domain of f as P, so $f \in \mathrm{Hom}_{R\text{-Mod}}(P, L)$ and $g = f \circ \beta = \varphi(f) \in \mathrm{im}\, \varphi$, proving the other inclusion.

We conclude that the sequence that arises is indeed exact.

(ii) Firstly, note that, if R is noncommutative, the structures presented are not necessarily R-modules. Hence, we will prove that they are isomorphic as abelian groups. Consider the following exact sequence:

$$0 \longrightarrow I \xrightarrow{i} R \xrightarrow{\pi} R/I \cong M \longrightarrow 0\,.$$

By (i), it induces the exact sequence:

$$0 \longrightarrow H(M, N) \xrightarrow{\varphi} H(R, N) \xrightarrow{\psi} H(I, N)\,,$$

where "H" abbreviates "$\mathrm{Hom}_{R\text{-Mod}}$". By the exactness, it follows that $\mathrm{Hom}_{R\text{-Mod}}(M, N) \cong \mathrm{im}\, \varphi = \ker \psi$. Notice that $\ker \psi = \{f \in$

$\mathrm{Hom}_{R\text{-Mod}}(R,N) \mid f \circ i = 0\} = \{f \in \mathrm{Hom}_{R\text{-Mod}}(R,N) \mid I \subseteq \ker f\}$. If $S = \{n \in N \mid (\forall a \in I), an = 0\}$, define:

$$\begin{aligned} \sigma : \ker \psi &\longrightarrow S \\ f &\longmapsto f(1). \end{aligned}$$

This function is well-defined because $af(1) = f(a) = 0$ for all $a \in I$. It is clear that σ is a homomorphism of abelian groups and, if R is commutative, it is a homomorphism of R-modules too. Finally, σ is bijective because its inverse is

$$\begin{aligned} \sigma^{-1} : S &\longrightarrow \ker \psi \\ n &\longmapsto (a \mapsto an), \end{aligned}$$

which is also well-defined and is a homomorphism. Therefore, we conclude the desired isomorphism.

The second part is a consequence of the first. The proof is in Exercise 6.17.

(iii) Consider the following exact sequence:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0\,.$$

Now, if we take the $\mathbb{Z}$-module L as $\mathbb{Z}$ itself, the induced homomorphism $\psi : \mathrm{Hom}_{\mathbb{Z}\text{-Mod}}(\mathbb{Z},\mathbb{Z}) \to \mathrm{Hom}_{\mathbb{Z}\text{-Mod}}(\mathbb{Z},\mathbb{Z})$ is given by

$$\psi(f)(x) = f(2x) = 2f(x)$$

for all $x \in \mathbb{Z}$ and $f \in \mathrm{Hom}_{\mathbb{Z}\text{-Mod}}(\mathbb{Z},\mathbb{Z})$. We see that ψ is not onto since the identity homomorphism is not in $\operatorname{im}\psi$.

(iv) If the original sequence splits, there are R-modules M',P' and a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M & \xrightarrow{\alpha} & N & \xrightarrow{\beta} & P & \longrightarrow & 0 \\ & & \downarrow\sim & & \downarrow\sim & & \downarrow\sim & & \\ 0 & \longrightarrow & M' & \xrightarrow{i_{M'}} & M' \oplus P' & \xrightarrow{\pi_{N'}} & P' & \longrightarrow & 0 \end{array}$$

in which the vertical maps are isomorphisms. We will abbreviate "$\mathrm{Hom}_{R\text{-Mod}}$" by just "$H$", as we did in (ii). The induced exact sequences from (i) create the following diagram:

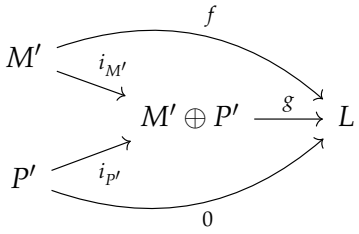
$$\begin{array}{ccccccccc} 0 & \longrightarrow & H(P',L) & \longrightarrow & H(M' \oplus P', L) & \longrightarrow & H(M',L) & & \\ & & \downarrow\sim & & \downarrow\sim & & \downarrow\sim & & \\ 0 & \longrightarrow & H(P,L) & \longrightarrow & H(N,L) & \longrightarrow & H(M,L)\,. & & \end{array}$$

The vertical maps are the isomorphisms that take a homomorphism and composes with the isomorphisms of the first diagram.

Note that this diagram also commutes because the other one commutes. Now, if we consider only this part of the diagram:

$$\begin{array}{ccc} H(M' \oplus P', L) & \xrightarrow{\psi'} & H(M', L) \\ {\scriptstyle \Phi_1}\downarrow & & \downarrow{\scriptstyle \Phi_2} \\ H(N, L) & \xrightarrow{\psi} & H(M, L)\,, \end{array}$$

we see that ψ is onto if ψ' is onto. Indeed, if ψ' is surjective, so is $\Phi_2 \circ \psi' = \psi \circ \Phi_1$ and we must have that ψ is surjective. Therefore, we just need to check that ψ' is onto, that is, if for every $f \in H(M', L)$ there exists $g \in H(M' \oplus P', L)$ such that $f = \psi'(g) = g \circ i_{M'}$. By the universal property of coproducts in R-Mod, there is a homomorphism $g : M' \oplus P' \to L$ such that the diagram



commutes, and so $f = \psi'(g)$, as desired. ∎

EXERCISE 7.8

∎ SOLUTION T ∎

EXERCISE 7.9

∎ SOLUTION A ∎

EXERCISE 7.10 ▷ In the situation of the snake lemma, assume that λ and ν are isomorphisms. Use the snake lemma and prove that μ is an isomorphism. This is called the 'short five-lemma', as it follows immediately from the five-lemma (cf. Exercise 7.14), as well as from the snake lemma. [VIII.6.21, IX.2.4]

∎ SOLUTION If λ and ν are isomorphisms,

$$\ker \lambda = \operatorname{coker} \lambda = \ker \nu = \operatorname{coker} \nu = 0.$$

The snake lemma then implies that

$$0 \to 0 \to \ker \mu \to 0 \to 0 \operatorname{coker} \mu \to 0 \to 0.$$

By Exercise 7.1, $\ker \mu = \operatorname{coker} \mu = 0$, which means that μ is an isomorphism. ∎

EXERCISE 7.11 ▷ Let

$$0 \longrightarrow M_1 \longrightarrow N \longrightarrow M_2 \longrightarrow 0 \qquad (*)$$

be an exact sequence of R-modules. (This may be called an 'extension' of M_2 by M_1.) Suppose there is *any* R-module homomorphism $N \to M_1 \oplus M_2$ making the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_1 & \longrightarrow & N & \longrightarrow & M_2 & \longrightarrow & 0 \\ & & \| & & \downarrow & & \| & & \\ 0 & \longrightarrow & M_1 & \longrightarrow & M_1 \oplus M_2 & \longrightarrow & M_2 & \longrightarrow & 0 \end{array}$$

commute, where the bottom sequence is the standard sequence of a direct sum. Prove that (*) splits. [§7.2]

■ SOLUTION This is an immediate consequence of Exercise 7.10: since the identities id_{M_1} and id_{M_2} are, in particular, isomorphims, it follows that the homomorphism $N \to M_1 \oplus M_2$ is indeed an isomorphism and, therefore, (*) splits. ■

EXERCISE 7.12

■ SOLUTION T ■

EXERCISE 7.13

■ SOLUTION A ■

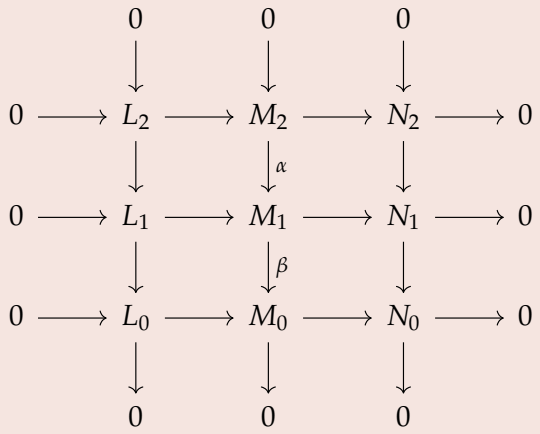
EXERCISE 7.14 ¬ Prove the 'five-lemma': if

$$\begin{array}{ccccccccc} A_1 & \longrightarrow & B_1 & \longrightarrow & C_1 & \longrightarrow & D_1 & \longrightarrow & E_1 \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \epsilon} \\ A_0 & \longrightarrow & B_0 & \longrightarrow & C_0 & \longrightarrow & D_0 & \longrightarrow & E_0 \end{array}$$

is a commutative diagram of R-modules with exact rows, β and δ are isomorphisms, α is an epimorphism, and ϵ is a monomorphism, then γ is an isomorphism. (You can avoid the needed diagram chase by pasting together results from the previous exercises.) [7.10]

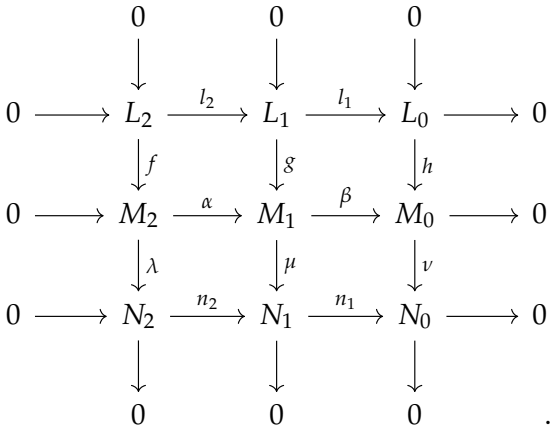
■ SOLUTION By the two preceding exercises, γ is both an epimorphism and a monomorphism. Since we are in R-Mod this implies that γ is an isomorphism. (As we observed before, both exercises are needed as their correct conclusions are that γ is a monomorphism and an epimorphism, respectively.) ■

EXERCISE 7.15 ¬ Consider the following commutative diagram of R-modules:



Assume that the three rows are exact and the two rightmost columns are exact. Prove that the left column is exact. Second version: assume that the three rows are exact and the two leftmost columns are exact; prove that the right column is exact. This is the 'nine-lemma'. (You can avoid a diagram chase by applying the snake lemma; for this, you will have to turn the diagram by 90°.) [7.16]

■ SOLUTION Let's turn the diagram by 90°, reflect it and give names for the homomorphisms:



Since the columns of this diagram are exact, we know that

$$\ker f = \ker g = \ker h = 0$$

and

$$\operatorname{coker} \lambda = \operatorname{coker} \mu = \operatorname{coker} \nu = 0.$$

For the first version, suppose that the two bottom rows are exact. Applying the snake lemma to them, we get the exact sequence

$$0 \longrightarrow \ker \lambda \xrightarrow{\alpha} \ker \mu \xrightarrow{\beta} \ker \nu \longrightarrow 0\,,$$

where α and β are restricted to $\ker\lambda$ and $\ker\mu$, respectively. By the exactness of the columns, we can change it to

$$0 \longrightarrow \operatorname{im} f \xrightarrow{\alpha} \operatorname{im} g \xrightarrow{\beta} \operatorname{im} h \longrightarrow 0$$

and, since f, g and h are injective, we have the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & L_2 & \xrightarrow{l_2} & L_1 & \xrightarrow{l_1} & L_0 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & \operatorname{im} f & \xrightarrow{\alpha} & \operatorname{im} g & \xrightarrow{\beta} & \operatorname{im} h & \longrightarrow & 0\,, \end{array}$$

where the vertical maps are isomorphisms. Thus, these sequences are the same, up to natural identifications. Indeed, one can check that the exactness of the bottom row implies that the top row is exact, as desired.

The second case is similar. Suppose that the two top rows are exact. Applying the snake lemma to them, we get the exact sequence

$$0 \longrightarrow \operatorname{coker} f \xrightarrow{\widetilde{\alpha}} \operatorname{coker} g \xrightarrow{\widetilde{\beta}} \operatorname{coker} k \longrightarrow 0\,,$$

where $\widetilde{\alpha}$ and $\widetilde{\beta}$ are given by $\widetilde{\alpha}(x + \operatorname{im} f) = \alpha(x) + \operatorname{im} g$ and $\widetilde{\beta}(x + \operatorname{im} g) = \beta(x) + \operatorname{im} h$. This homomorphisms are well-defined and arise from the snake lemma, making the diagram drawn after Remark 7.11 commute. By the exactness of the columns, we can write it as

$$0 \longrightarrow \frac{M_2}{\ker\lambda} \xrightarrow{\widetilde{\alpha}} \frac{M_1}{\ker\mu} \xrightarrow{\widetilde{\beta}} \frac{M_0}{\ker\nu} \longrightarrow 0\,.$$

Since λ, μ and ν are surjective, Corollary 5.16 implies that there are isomorphisms $\varphi_2 : M_2/\ker\lambda \to N_2$, $\varphi_1 : M_1/\ker\mu \to N_1$ and $\varphi_0 : M_0/\ker\nu \to N_0$ such that $\lambda = \varphi_2\pi_2$, $\mu = \varphi_1\pi_1$ and $\nu = \varphi_0\pi_0$, where π_2, π_1 and π_0 are the corresponding projections. Thus, we have the following commutative diagram:

$$\begin{array}{ccccccccc} & & M_2 & \xrightarrow{\alpha} & M_1 & \xrightarrow{\beta} & M_3 & & \\ & & \downarrow{\scriptstyle \pi_2} & & \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_3} & & \\ 0 & \longrightarrow & \frac{M_2}{\ker\lambda} & \xrightarrow{\widetilde{\alpha}} & \frac{M_1}{\ker\mu} & \xrightarrow{\widetilde{\beta}} & \frac{M_0}{\ker\nu} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \varphi_2} & & \downarrow{\scriptstyle \varphi_1} & & \downarrow{\scriptstyle \varphi_0} & & \\ 0 & \longrightarrow & N_2 & \xrightarrow{n_2} & N_1 & \xrightarrow{n_1} & N_0 & \longrightarrow & 0\,. \end{array}$$

It is not as clear as in the other case that this diagram really commutes. But note that

$$n_2(\varphi_2\pi_2) = n_2\lambda = \mu\alpha = (\varphi_1\pi_1)\alpha = \varphi_1(\pi_1\alpha)\varphi_1(\widetilde{\alpha}\pi_2)$$

and, since π_2 is an epimorphism, $n_2\varphi_2 = \varphi_1\widetilde{\alpha}$. Similarly, we have that $n_1\varphi_1 = \varphi_0\widetilde{\beta}$, so the diagram indeed commutes. Therefore, since φ_2, φ_1 and φ_0 are isomorphisms, the bottom two rows of the diagram above are essentially the same, up to natural identifications. As in the last case, it follows that $N_\bullet$ is exact. ∎

EXERCISE 7.16

∎ SOLUTION T ∎

EXERCISE 7.17

∎ SOLUTION A ∎

IV

GROUPS, SECOND ENCOUNTER

1 THE CONJUGATION ACTION

EXERCISE 1.1 ▷ Let p be a prime integer, let G be a p-group, and let S be a set such that $|S| \not\equiv 0 \mod p$. If G acts on S, prove that the action must have fixed points. [§1.1, §2.3]

■ SOLUTION G ■

EXERCISE 1.2

■ SOLUTION T ■

EXERCISE 1.3 Prove that the center of S_n is trivial for $n \geq 3$. (Suppose that $\sigma \in S_3$ sends a to $b \neq a$, and let $c \neq a, b$. Let τ be the permutation that acts solely by swapping b and c. Then compare the action of $\sigma\tau$ and $\tau\sigma$ on a.)

■ SOLUTION Let $\sigma \in S_3$ be a permutation different from the identity. Thus, there are a, b and c distinct such that σ sends a to b. Let τ be the permutation that acts solely by swapping b and c. Now, note that $\sigma\tau$ sends a to b and then to c, while $\tau\sigma$ sends a to a and then to b. Therefore, $\sigma\tau \neq \tau\sigma$ and $\sigma \notin Z(S_n)$. We conclude that the center of S_n is trivial for $n \geq 3$. ■

EXERCISE 1.4

■ SOLUTION A ■

EXERCISE 1.5 ▷ Let G be a group. Prove that $G/Z(G)$ is isomorphic to the group $\mathrm{Inn}(G)$ of *inner* automorphisms of G. (Cf. Exercise II.4.8.) Then prove Lemma 1.5 again by using the result of Exercise II.6.7. [§1.2]

■ SOLUTION G ■

EXERCISE 1.6

■ SOLUTION T ■

EXERCISE 1.7 Prove or disprove that if p is prime, then every group of order p^3 is commutative.

■ SOLUTION This statement is false. For example, D_8 and Q_8 (see Exercise III.2) are both noncommutative and have order $8 = 2^3$. ■

EXERCISE 1.8

■ SOLUTION A ■

EXERCISE 1.9 ¬ Let p be a prime number, G a p-group, and H a nontrivial normal subgroup of G. Prove that $H \cap Z(G) \neq \{e\}$. (Hint: Use the class formula.) [3.11]

■ SOLUTION G ■

EXERCISE 1.10

■ SOLUTION T ■

EXERCISE 1.11 Let G be a finite group, and suppose there exist representatives $g_1, \ldots, g_r$ of the r distinct conjugacy classes in G, such that $\forall i, j,\ g_i g_j = g_j g_i$. Prove that G is commutative. (Hint: What can you say about the sizes of the conjugacy classes?)

■ SOLUTION Note that $|Z(g_i)| \geq r$ since $\{g_1, \ldots, g_r\} \subseteq Z(g_i)$ for all i. By Proposition II.9.9 and Lagrange's theorem, we have that

$$|[g_i]| = [G : Z(g_i)] = \frac{|G|}{|Z(g_i)|} \leq \frac{|G|}{r}$$

for all i. Since the conjugacy class of the identity has only one element, we may assume that $g_1 = e$. Thus,

$$|G| = \sum_{i=1}^{r} |[g_i]| = 1 + \sum_{i=2}^{r} |[g_i]| \leq 1 + \sum_{i=2}^{r} \frac{|G|}{r} = 1 + \frac{r-1}{r}|G|,$$

which implies that $r \geq |G|$. But $r \leq |G|$ and so we must have $r = |G|$, following that each conjugacy class has only one element and, therefore, G is commutative. ■

EXERCISE 1.12

■ SOLUTION A ■

EXERCISE 1.13 ▷ Let G be a noncommutative group of order 6. As observed in Example 1.10, G must have trivial center and exactly two conjugacy classes, of order 2 and 3.

- Prove that if every element of a group has order ≤ 2, then the group is commutative. Conclude that G has an element y of order 3.
- Prove that $\langle y \rangle$ is normal in G.
- Prove that $[y]$ is the conjugacy class of order 2 and $[y] = \{y, y^2\}$.
- Prove that there is an $x \in G$ such that $yx = xy^2$.

- Prove that x has order 2.
- Prove that x and y generate G.
- Prove that $G \cong S_3$.

[§1.3, §2.5]

■ SOLUTION G ■

EXERCISE 1.14

■ SOLUTION T ■

EXERCISE 1.15 Suppose that the class formula for a group G is $60 = 1 + 15 + 20 + 12 + 12$. Prove that the only *normal* subgroups of G are $\{e\}$ and G.

■ SOLUTION By the definition of the class formula, we know that there are 5 conjugacy classes and that their sizes are 1, 12, 12, 15 and 20. Let N be a nontrivial normal subgroup of G. Since it is normal, it is the union of some conjugacy classes of G, so the order of N is the sum of some of the numbers listed above. We know for sure that $e \in N$, so it has to contain the conjugacy class of e, which has only one element. By Lagrange's theorem, $|N|$ divides 60 and, by the considerations above, it must be 15, 20, 30 or 60. It is easy to see that it is impossible to choose some numbers between $12, 12, 15$ and 20, add them to 1 and get 15, 20 or 30, so we must have $|N| = 60$ and, therefore, $N = G$. We conclude that the only normal subgroups of G are $\{e\}$ and G. ■

EXERCISE 1.16

■ SOLUTION A ■

EXERCISE 1.17 ¬ Let H be a proper subgroup of a finite group G. Prove that G is *not* the union of the conjugates of H. (Hint: You know the number of conjugates of H; keep in mind that any two subgroups overlap, at least at the identity.) [1.18, 1.20]

■ SOLUTION G ■

EXERCISE 1.18

■ SOLUTION T ■

EXERCISE 1.19 Let H be a proper subgroup of a finite group G. Prove that there exists a $g \in G$ whose conjugacy class is disjoint from H.

■ SOLUTION By Exercise 1.17, G is not the union of conjugates of H, so there exists $g \in G$ such that $g \notin aHa^{-1}$ for all $a \in G$. If H contained

aga^{-1} for some $a \in G$, we would have that $g \in a^{-1}Ha$, a contradiction. Therefore, the conjugacy class of g must be disjoint from H. ∎

EXERCISE 1.20

■ SOLUTION A ∎

EXERCISE 1.21 ▷ Let H, K be subgroups of a group G, with $H \subseteq N_G(K)$. Verify that the function $\gamma : H \to \mathrm{Aut}_{\mathsf{Grp}}(K)$ defined by conjugation is a homomorphism of groups and that $\ker \gamma = H \cap Z_G(K)$, where $Z_G(K)$ is the centralizer of K. [§1.4, 1.22]

■ SOLUTION G ∎

EXERCISE 1.22

■ SOLUTION T ∎

2 THE SYLOW THEOREMS

EXERCISE 2.1

■ SOLUTION A ∎

EXERCISE 2.2 ▷ Let G be a group. A subgroup H of G is *characteristic* if $\varphi(H) \subseteq H$ for every automorphism φ of G.

- Prove that characteristic subgroups are normal.
- Let $H \subseteq K \subseteq G$, with H characteristic in K and K normal in G. Prove that H is normal in G.
- Let G, K be groups, and assume that G contains a single subgroup H isomorphic to K. Prove that H is normal in G.
- Let K be a normal subgroup of a finite group G, and assume that $|K|$ and $|G/K|$ are relatively prime. Prove that K is characteristic in G.

[§2.1, §2.4, 2.13, §3.3]

■ SOLUTION G ∎

EXERCISE 2.3 Prove that a nonzero abelian group G is simple if and only if $G \cong \mathbb{Z}/p\mathbb{Z}$ for some positive prime integer p.

■ SOLUTION ($\Longrightarrow$) Let G be a nonzero abelian group that is simple and take any element $g \in G$ different from the identity element. Since G is abelian and simple, $\langle g \rangle \neq \{e\}$ is a normal subgroup of G and so $\langle g \rangle = G$. Thus, G is cyclic and so it is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$ for some $n > 1$. Since $\mathbb{Z}$ is clearly non-simple, it follows that we have the

second case. On the other hand, if $n = ab$, where $a, b > 1$, then $\langle [a]_n \rangle$ is a proper, nontrivial and normal subgroup of $\mathbb{Z}/n\mathbb{Z}$ and this group is not simple. Therefore, we must have $G \cong \mathbb{Z}/p\mathbb{Z}$ for some positive prime integer p.

($\Longleftarrow$) Let p be a positive prime integer. By Lagrange's theorem, the only subgroups of $\mathbb{Z}/p\mathbb{Z}$ are $\{[0]_p\}$ and $\mathbb{Z}/p\mathbb{Z}$ itself, so $\mathbb{Z}/p\mathbb{Z}$ is simple. ∎

EXERCISE 2.4

■ SOLUTION T ∎

EXERCISE 2.5

■ SOLUTION A ∎

EXERCISE 2.6 Prove that there are no simple groups of order 4, 8, 9, 16, 25, 27, 32, or 49. In fact, prove that no p-group of order $\geq p^2$ is simple.

■ SOLUTION G ∎

EXERCISE 2.7 Prove that there are no simple groups of order 6, 10, 14, 15, 20, 21, 22, 26, 28, 33, 34, 35, 38, 39, 42, 44, 46, 51, 52, 55, 57, or 58. (Hint: Example 2.4)

■ SOLUTION This is an immediate consequence of Example 2.4. Indeed, note that all these numbers are of the form mp where $1 < m < p$ and p is a prime integer. ∎

EXERCISE 2.8

■ SOLUTION T ∎

EXERCISE 2.9

■ SOLUTION A ∎

EXERCISE 2.10 ¬ Let P be a p-Sylow subgroup of a finite group G, and act with P by conjugation on the set of p-Sylow subgroups of G. Show that P is the unique fixed point of this action. (Hint: Use Exercise 2.9.) [2.11]

■ SOLUTION G ∎

EXERCISE 2.11 ▷ Use the second Sylow theorem, Corollary 1.14, and Exercise 2.10 to paste together an alternative proof of the third Sylow theorem. [§2.4]

THEOREM 2.8 (Second Sylow theorem). Let G be a finite group, let P be a p-Sylow subgroup, and let $H \subseteq G$ be a p-group. Then H is contained in a conjugate of P: there exists $g \in G$ such that $H \subseteq gPg^{-1}$.

Corollary 2.14 Let $H \subseteq G$ be a subgroup. If $[G : H]$ is finite, then the number of subgroups conjugate to H is finite and divides $[G : H]$.

THEOREM 2.11 (Third Sylow theorem). Let p be a prime integer, and let G be a finite group of order $|G| = p^r m$. Assume that p does not divide m. Then the number of p-Sylow subgroups of G divides m and is congruent to 1 modulo p.

■ SOLUTION With the notation as above, let S be the set of p-Sylow subgroups of G and let P be one of them. By the second Sylow theorem, every p-Sylow subgroup in S is a conjugate of P, so $|S|$ also counts the number of conjugates of P and Corollary 2.14 tells us that $|S|$ divides $[G : P] = m$. Now, if we let P act on S by conjugation, it follows from Exercise 2.10 that P is the unique fixed point of this action. Therefore, by Corollary 1.3, $|S| \equiv 1 \mod p$. ■

EXERCISE 2.12

■ SOLUTION T ■

EXERCISE 2.13

■ SOLUTION A ■

EXERCISE 2.14 Prove that there are no simple groups of order 18, 40, 45, 50, or 54.

■ SOLUTION G ■

EXERCISE 2.15 Classify all groups of order $n \leq 15$, $n \neq 8, 12$: that is, produce a list of nonisomorphic groups such that every group of order $n \neq 8, 12$, $n \leq 15$ is isomorphic to one group in the list.

■ SOLUTION By Exercise II.1.6, we already know the classification for $n \leq 5$, as listed below. Let's find it for the other orders.

- $n = 1$: The only group of order 1 is the trivial group.
- $n = 2$: The only group of order 2 is C_2.
- $n = 3$: The only group of order 3 is C_3.
- $n = 4$: The groups of order 4 are C_4 and $C_2 \times C_2$.
- $n = 5$: The only group of order 5 is C_5.

- $n = 6$: Let G be a group of order 6 and suppose that it is abelian. By Cauchy's theorem, there are elements $g, h \in G$ of order 2 and 3, respectively. It follows from Exercise II.1.14 that $|gh| = 6$ and so G is cyclic and $G \cong C_6$. On the other hand, if G is noncommutative, Exercise 1.13 implies that $G \cong S_3$. Therefore, the groups of order 6 are C_6 and S_3.

- $n = 7$: It is similar to what have been done for $n = 5$ in Exercise II.1.6. By Lagrange's theorem, elements different from the identity in a group of order 7 must also be of order 7, so this group is cyclic. Thus, the only group of order 7 is C_7.

- $n = 9$: Let G be a group of order 9 and suppose that it is not cyclic. By Lagrange's theorem, every element besides the identity is of order 3. Moreover, by Exercise 1.6, we also know that G is commutative. Let $a \in G$ be any element different from e and take $b \in G$ such that $b \neq e, a, a^2$. We claim that G is generated by a and b. Firstly, note that $\{a, a^2\} \cap \{b, b^2\} = \emptyset$ because otherwise we would have $b = a$ or $b = a^2$. Thus, if $a^x = b^y$ then necessarily x and y are multiples of 3, which is the order of a and b. Now, let's prove that $\langle a, b\rangle$ has 9 elements and, therefore, $G = \langle a, b\rangle$. If $a^x b^y = a^z b^w$ with $x, y, z, w \in \{0, 1, 2\}$, then $a^{x-z} = b^{w-y}$ and so $x \equiv z \mod 3$ and $w \equiv y \mod 3$, following that $x = z$ and $w = y$. This implies that $\langle a, b\rangle$ is in bijection with $\{0, 1, 2\} \times \{0, 1, 2\}$ and so it has 9 elemtents, as desired. Finally, we can define $\varphi : C_3 \times C_3 \to G$ by

  $$\varphi([x]_3, [y]_3) = a^x b^y$$

  for all $([x]_3, [y]_3) \in C_3 \times C_3$, which is an isomorphism by the considerations above. We conclude that the groups of order 9 are C_9 and $C_3 \times C_3$.

  In general, any group of order p^2 where p is prime is isomorphic to C_{p^2} or $C_p \times C_p$. A proof similar to the one given here will hold.

- $n = 10$: Let G be a group of order 10 and suppose that it is abelian. Similar as for $n = 6$, Cauchy's theorem implies that there are elements of order 2 and 5 and so it follows from Exercise II.1.14 that G is cyclic and $G \cong C_{10}$. On the other hand, if G is noncommutative, Claim 2.17 tells us that $G \cong D_{10}$ since $10 = 2 \cdot 5$ and 5 is an odd prime. Therefore, the groups of order 10 are C_{10} and D_{10}.

- $n = 11$: Since 11 is prime, the only group of order 11 is C_{11}, as in the previous cases where n was a prime number.

- $n = 13$: Since 13 is prime, the only group of order 13 is C_{13}.

- $n = 14$: This case is very similar to the case $n = 10$ since $14 = 2 \cdot 7$ and 7 is an odd prime. Thus, the groups of order 14 are C_{14} and D_{14}.

- $n = 15$: Since $15 = 3 \cdot 5$, 3 and 5 are primes and $5 \not\equiv 1 \mod 3$, it follows from Claim 2.16 that the only group of order 15 is C_{15}. ∎

Remark. We could have worked what are the groups of order 8 and 12, but the discussion would be too long compared to what we did. Thus, we bring here just a list of them:

- $n = 8$: The groups of order 8 are C_8, $C_4 \times C_2$, $C_2 \times C_2 \times C_2$, D_8 and Q_8 (see Exercise III.2).
- $n = 12$: The groups of order 12 are C_{12}, $C_6 \times C_2$, D_{12}, A_4 and Dic_3.

  The groups A_n is called the *alternating group of degree n*. It is the subgroup of S_n composed of the *even* permutations, as we shall define. Any permutation in S_n can be decomposed as a product of transpositions (permutations that only change two elements) and the parity of the number of transpositions is invariant. In this sense, a permutation is *even* if this number is even or *odd* otherwise. Aluffi will introduce these concepts and this group in section 4.

  The groups Dic_n are called the *dicyclic groups*. They have the following presentation:

$$\mathrm{Dic}_n = (a, x | a^{2n} = e, x^2 = a^n, x^{-1}ax = a^{-1}).$$

  From these relations, it follows that every element of Dic_n can be uniquely written as $a^k x^l$, where $0 \leq k < 2n$ and $l = 0$ or 1. Thus, the order of Dic_n is $4n$. The quaternionic group Q_8 presented in Exercise III.2 is isomorphic to Dic_2.

EXERCISE 2.16

■ SOLUTION T ■

EXERCISE 2.17

■ SOLUTION A ■

EXERCISE 2.18 ▷ Give an alternative proof of Claim 2.16 as follows: use the third Sylow theorem to count the number of elements of order p and q in G; use this to show that there are elements in G of order neither 1 nor p nor q; deduce that G is cyclic. [§2.5]

■ SOLUTION G ■

EXERCISE 2.19 ▷ Let G be a noncommutative group of order pq, where $p < q$ are primes.

- Show that $q \equiv 1 \mod p$.

- Show that the center of G is trivial.
- Draw the lattice of subgroups of G.
- Find the number of elements of each possible order in G.
- Find the number and the size of the conjugacy classes in G.

[§2.5]

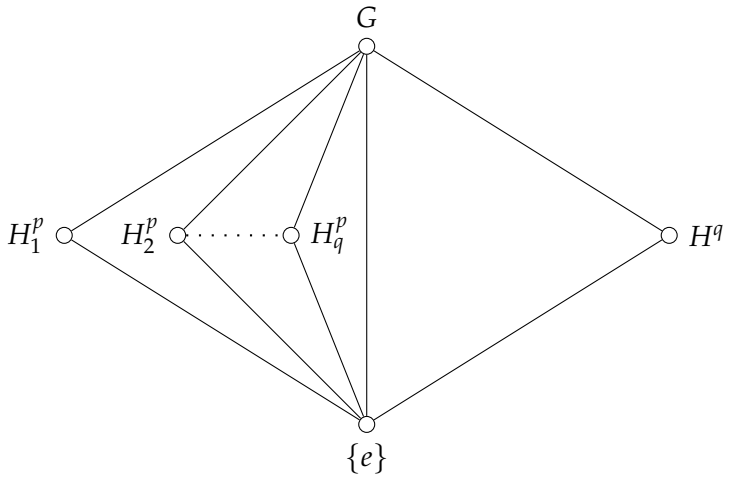
■ SOLUTION

- If q were not congruent to 1 modulo p, Claim 2.16 (see Exercise 2.18) would imply that G is abelian, a contradiction. Therefore, we must have $q \equiv 1 \mod p$.
- This follows immediately from Exercise 1.6.
- Let's find how are the subgroups of G. By the third Sylow theorem, the number N_q of subgroups of order q of G divides p and is congruent to 1 modulo q. Since the only positive divisors of p are 1 and p, and $p < q$, we must have $N_q = 1$. This also implies that G has exactly $q - 1$ elements of order q and, thus, G has $pq - q$ elements of order different from 1 and q. By Lagrange's theorem, these elements can only have order p or pq, but, since G is not abelian, it is not cyclic, so it follows that G has $pq - q$ elements of order p. Since

$$pq - q = q(p-1) \geq 2(p-1) = 2p - 2 \geq 2p - p = p,$$

G must have at least two subgroups of order p. Again by the third Sylow theorem we know that the number N_p of subgroups of order p of G must divide q and so $N_p = q$. If $H_1^p, \ldots, H_q^p$ are these q subgroups of order p and H^q is the subgroup of order q, we conclude that the lattice of subgroups of G is the one below.

Note that here we have another proof for the first item.



- We did this in the previous item. By Lagrange's theorem, the possible orders for the elements of G are 1, p, q and pq. we have

found that there are 1 element of order 1 (the identity), $pq - q$ elements of order p, $q - 1$ elements of order q and no elements of order pq.

- The size of each conjugacy class must divide the order of G, so the possible sizes for them are 1, p and q. Since the center of G is trivial, the conjugacy class of the identity is the only trivial one. Let n_p and n_q denote the number of conjugacy classes of sizes p and q, respectively. By the class formula, $pq = 1 + n_p p + n_q q$ and, modulo p, we have that $n_q \equiv -1 \mod p$ since $q \equiv 1 \mod p$. It follows that $n_q = p - 1$ because $n_q q < pq$ and so $n_p = \frac{q-1}{p}$. Therefore, there are $p + \frac{q-1}{p}$ conjugacy classes: 1 of size 1, $\frac{q-1}{p}$ of size p and $p - 1$ of size q. ∎

EXERCISE 2.20

∎ SOLUTION T ∎

EXERCISE 2.21

∎ SOLUTION A ∎

EXERCISE 2.22 Let G be a finite group, $n = |G|$, and p be a prime divisor of n. Assume that the only divisor of n that is congruent to 1 modulo p is 1. Prove that G is simple.

∎ SOLUTION G ∎

EXERCISE 2.23 ¬ Let N_p denote the number of p-Sylow subgroups of a group G. Prove that if G is simple, then $|G|$ divides $N_p!$ for all primes p in the factorization of G. More generally, prove that if G is simple and H is a subgroup of G of index $N > 1$, then $|G|$ divides $N!$. (Hint: Exercise II.9.12.) This problem capitalizes on the idea behind Example 2.15. [2.25]

∎ SOLUTION For the first part, we will suppose that G is not a p-Sylow subgroup itself. Therefore, $N_p > 1$ for all primes p in the factorization of G. Indeed, if $N_p = 1$, this p-Sylow subgroup would be a proper, nontrivial normal subgroup of G, contradicting that G is simple. Now, for a given prime p in the factorization of G, let X be the set of p-Sylow subgroups of G. Note that G acts by conjugation on X and, since $N_p > 1$, the second Sylow theorem guarantees that this action is nontrivial. Therefore, there is a nontrivial group homomorphism $G \to S_X$ and, since G is simple, Exercise 2.5 implies that this homomorphism is injective. It follows that G can be viewed as a subgroup of S_X and, by Lagrange's theorem, we conclude that $|G|$ divides $|S_X| = |X|! = N_p!$.

For the second part, let G act on G/H by left-multiplication. Since $N > 1$, this action is nontrivial and so there exists a nontrivial group homomorphism $G \to S_{G/H}$. Again by Exercise 2.5, this homomor-

phism is injective and we may realize G as a subgroup of $S_{G/H}$. Finally, Lagrange's theorem implies that $|G|$ divides $|S_{G/H}| = |G/H|! = [G : H]! = N!$, as desired. ∎

EXERCISE 2.24

∎ SOLUTION T ∎

EXERCISE 2.25

∎ SOLUTION A ∎

3 COMPOSITION SERIES AND SOLVABILITY

EXERCISE 3.1 Prove that $\mathbb{Z}$ has normal series of arbitrary lengths. (Thus, $\ell(\mathbb{Z})$ is not finite.)

∎ SOLUTION G ∎

EXERCISE 3.2

∎ SOLUTION T ∎

EXERCISE 3.3 ▷ Prove that every finite group has a composition series. Prove that $\mathbb{Z}$ does not have a composition series. [§3.1]

∎ SOLUTION Let G be a finite group. We will prove that G has a composition series by induction on the order of G. If $|G| = 1$, G is the trivial group and so has a composition series. Now, suppose that $|G| > 1$ and that every group of order less than $|G|$ has a composition series. Let $N \subseteq G$ be a proper normal subgroup of maximal order. We claim that G/N is simple. Indeed, if it were not simple, it would have a proper, nontrivial and normal subgroup which would correspond (by Propositions II.8.9 and II.8.10) to a normal subgroup H of G such that $N \subsetneq H \subsetneq G$, contradicting the definition of N. Since N is a proper subgroup, $|N| < |G|$ and, by the inductive hypothesis, N has a composition series. Thus, concatenating $G \supsetneq N$ to a composition series for N, we get a composition series for G, as desired.

For the second part, note that, in a composition series, the group appearing just before $\{e\}$ is simple. Thus, it suffices to show that $\mathbb{Z}$ does not have simple subgroups and, since it is abelian, this is equivalent to show that every nontrivial subgroup of $\mathbb{Z}$ has proper and nontrivial subgroups, which is clearly true. We conclude that $\mathbb{Z}$ does not have a composition series. ∎

EXERCISE 3.4

∎ SOLUTION A ∎

EXERCISE 3.5 ▷ Show that if H, K are *normal* subgroups of a group G, then HK is a normal subgroup of G. [§3.1]

■ SOLUTION G ■

EXERCISE 3.6

■ SOLUTION T ■

EXERCISE 3.7 ▷ Locate and understand a proof of (the general form of) Schreier's theorem that does not use the Jordan-Hölder theorem. Then obtain an alternative proof of the Jordan-Hölder, using Schreier's. [§3.2]

THEOREM 3.2 (Jordan-Hölder). Let G be a group, and let

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_n = \{e\},$$

$$G = G'_0 \supsetneq G'_1 \supsetneq G'_2 \supsetneq \cdots \supsetneq G'_m = \{e\}$$

be two composition series for G. Then $m = n$, and the lists of quotient groups $H_i = G_i/G_{i+1}$, $H'_i = G'_i/G'_{i+1}$ agree (up to isomorphism) after a permutation of indices.

■ SOLUTION Here is the theorem:

(Schreier's theorem). Any two normal series of a group G ending with $\{e\}$ admit equivalent refinements.

To prove it, we need the following lemma:

(Zassenhaus's lemma). Let H and K be subgroups of a group G and let H' and K' be normal subgroups of H and K respectively. Then

- $H'(H \cap K')$ is a normal subgroup of $H'(H \cap K)$.
- $K'(H' \cap K)$ is a normal subgroup of $K'(H \cap K)$.
- $(H' \cap K)(H \cap K')$ is a normal subgroup of $H \cap K$.

Moreover,

$$\frac{H'(H \cap K)}{H'(H \cap K')} \cong \frac{H \cap K}{(H' \cap K)(H \cap K')} \cong \frac{K'(H \cap K)}{K'(H' \cap K)}.$$

This lemma is also known as the *butterfly lemma* because the lattice with the subgroups that arise from it resembles a butterfly.

Proof of the lemma. Firstly, note that the groups appearing in the first two items are indeed groups since H' and K' are normal in H and K respectively (see Proposition II.8.11). It is also clear that $H' \cap K$ and $H \cap K'$ are normal subgroups of $H \cap K$ so Exercise 3.5 implies the third item. To prove the first two items, we will prove directly that they are kernels of homomorphisms.

If $L = (H' \cap K)(H \cap K')$, let $\varphi : H'(H \cap K) \to (H \cap K)/L$ be defined as follows. For $h \in H'$ and $x \in H \cap K$, let $\varphi(hx) = xL$. We will show that φ is well-defined and a homomorphism. Let $h_1, h_2 \in H'$ and $x_1, x_2 \in H \cap K$. If $h_1 x_1 = h_2 x_2$, then $h_2^{-1} h_1 = x_2 x_1^{-1} \in H' \cap (H \cap K) = H' \cap K \subseteq L$, so $x_1 L = x_2 L$. Thus, φ is well-defined. Since H' is normal in H, there is h_3 in H' such that $x_1 h_2 = h_3 x_1$. Then

$$\begin{aligned}\varphi((h_1 x_1)(h_2 x_2)) &= \varphi((h_1 h_3)(x_1 x_2)) \\ &= (x_1 x_2)L \\ &= (x_1 L)(x_2 L) \\ &= \varphi(h_1 x_1)\varphi(h_2 x_2)\end{aligned}$$

and φ is a homomorphism.

Obviously φ is surjective. Finally if $h \in H'$ and $x \in H \cap K$, then $\varphi(hx) = xL = L$ if and only if $x \in L$, or if and only if $hx \in H'L = H'(H' \cap K)(H \cap K') = H'(H \cap K')$. Hence, $\ker \varphi = H'(H \cap K')$, proving the first item and one of isomorphisms by Corollary II.8.2. The other part follows by symmetry.

Proof of Schreier's theorem. Let G be a group and let

$$G = H_0 \supsetneq H_1 \supsetneq H_2 \supsetneq \cdots \supsetneq H_n = \{e\},$$

$$G = K_0 \supsetneq K_1 \supsetneq K_2 \supsetneq \cdots \supsetneq K_m = \{e\}$$

be two normal series for G ending with $\{e\}$. For $i \in \{0, \ldots, n-1\}$, we form the chain of (not necessarily distinct) groups

$$H_i = H_{i+1}(H_i \cap K_0) \supseteq H_{i+1}(H_i \cap K_1) \supseteq \cdots \supseteq H_{i+1}(H_i \cap K_m) = H_{i+1}.$$

We refine the first normal series by inserting the above chain between H_i and H_{i+1}. In a symmetric fashion, for $j \in \{0, \ldots, m-1\}$, we insert the chain

$$K_j = K_{j+1}(K_j \cap H_0) \supseteq K_{j+1}(K_j \cap H_1) \supseteq \cdots \supseteq K_{j+1}(K_j \cap H_n) = K_{j+1}$$

between K_j and K_{j+1}. By Zassenhaus's lemma, we have

$$\frac{H_{i+1}(H_i \cap K_j)}{H_{i+1}(H_i \cap K_{j+1})} \cong \frac{K_{j+1}(K_j \cap H_i)}{K_{j+1}(K_j \cap H_{i+1})}$$

for $0 \leq i \leq n-1$ and $0 \leq j \leq m-1$. This implies that the number of repetitions in both series is the same, so we can remove repeated groups to obtain refinements for both series that have the same length and the same quotients, as desired.

This theorem gives a simple proof for the Jordan-Hölder theorem. If we have two composition series for a group G, Schreier's theorem implies that they have equivalent refinements. But composition series cannot be further refined since each quotient is already simple. Therefore, the composition series must be equivalent, that is, they have the same length and the lists of quotient groups agree up to isomorphism after a permutation of indices. ∎

EXERCISE 3.8

■ SOLUTION A ■

EXERCISE 3.9 Let G be a nontrivial p-group. Construct explicitly an abelian series for G, using the fact that the center of a nontrivial p-group is nontrivial (Corollary 1.9). This gives an alternative proof of the fact that p-groups are solvable (Example 3.12).

■ SOLUTION G ■

EXERCISE 3.10

■ SOLUTION T ■

EXERCISE 3.11 ¬ Let H be a nontrivial normal subgroup of a nilpotent group G (cf. Exercise 3.10). Prove that H intersects $Z(G)$ nontrivially. (Hint: Let $r \geq 1$ be the smallest index such that $\exists h \neq e$, $h \in H \cap Z_r$. Contemplate a well-chosen commutator $[g,h]$. Since p-groups are nilpotent, this strengthens the result of Exercise 1.9. [3.14]

■ SOLUTION As in the hint, let $r \geq 1$ be the smallest index such that there exists $h \neq e$ in $H \cap Z_r$. Note that, since G is nilpotent and H is nontrivial, such index r really exists. We claim that $h \in Z(G)$. Firstly, we have that $[g,h] = ghg^{-1}h^{-1} \in H$ for all $g \in G$, because $ghg^{-1} \in H$ since H is normal. Now, let $\pi : G \to G/Z_{r-1}$ be the canonical projection. Since $h \in Z_r$, we know that that $\pi(h)$ is in the center of G/Z_{r-1}, so

$$\pi([g,h]) = [\pi(g), \pi(h)] = eZ_{r-1} \implies [g,h] \in Z_{r-1}$$

for all $g \in G$. Therefore, it follows that $[g,h] \in H \cap Z_{r-1} = \{e\}$, that is, $[g,h] = e$ for all $g \in G$. This implies that $h \in Z(G)$ and, thus, H intersects $Z(G)$ nontrivially. ■

EXERCISE 3.12

■ SOLUTION A ■

EXERCISE 3.13 ¬ For a group G, let $G^{(i)}$ denote the iterated commutator, as in §3.3. Prove that each $G^{(i)}$ is characteristic (hence normal) in G. [3.14]

■ SOLUTION G ■

EXERCISE 3.14

■ SOLUTION T ■

EXERCISE 3.15 Let p, q be prime integers, and let G be a group of order p^2q. Prove that G is solvable. (This is a particular case of *Burnside's theorem:* for p, q primes, every group of order p^aq^b is solvable.)

■ SOLUTION If $p = q$ then G is a p-group and it is solvable by Example 3.12. Thus, suppose that $p \neq q$. Firstly, we claim that any group H of order pq is solvable. Indeed, if H is abelian, it is immediately solvable. Otherwise, if we take $m = \max\{p, q\}$, Exercise 2.19 implies that H has only one m-Sylow subgroup P, which must be normal, so we have the following composition series for H:

$$H \supsetneq P \supsetneq \{e\}.$$

Since all composition factors are cyclic, H is solvable by Proposition 3.11.

Now, if G has a proper, nontrivial and normal subgroup N, it follows that N and G/N are solvable since their order can only be p, p^2, q or pq. By Corollary 3.13, this implies that G is also solvable, so it suffices to show that such N really exists. To prove this, we will compute the possible values for the numbers N_p and N_q of p- and q-Sylow subgroups of G, respectively, and show that $N_p = 1$ or $N_q = 1$, which implies that at least one of these Sylow subgroups is normal.

Suppose that $N_q \neq 1$. By the third Sylow theorem, N_q divides p^2 and is congruent to 1 modulo q. If $N_q = p$, we know that $p \equiv 1 \mod q$ and so $q < p$. Again by the third Sylow theorem, N_p divides q and is congruent to 1 modulo p. Since $q < p$, we must have $N_p = 1$, as desired. On the other hand, if $N_q = p^2$ then G has $p^2(q-1) = p^2q - p^2$ elements of order q since distinct subgroups of order q meet only at the identity. Therefore, we have only p^2 elements of order 1, p or p^2 and so there is enough room to just one p-Sylow subgroup, following that $N_p = 1$. We conclude that G has a proper, nontrivial and normal subgroup and so G is solvable. ■

EXERCISE 3.16

■ SOLUTION A ■

EXERCISE 3.17 Prove that the Feit-Thompson theorem is equivalent to the assertion that every noncommutative finite simple group has even order.

■ SOLUTION G ■

4 THE SYMMETRIC GROUP

EXERCISE 4.1

■ SOLUTION T ■

EXERCISE 4.2

■ SOLUTION A ■

EXERCISE 4.3 Assume σ has type $[\lambda_1, \ldots, \lambda_r]$ and that the λ_i's are pairwise relatively prime. What is $|\sigma|$? What can you say about $|\sigma|$, without the additional hypothesis on the numbers λ_i?

■ SOLUTION Since σ has type $[\lambda_1, \ldots, \lambda_r]$, its decomposition as the product of disjoint cycles is of the form

$$\sigma = (a_1 \ldots a_{\lambda_1})(b_1 \ldots b_{\lambda_2}) \cdots (c_1 \ldots c_{\lambda_r}).$$

By Lemma 4.2, we have that

$$\sigma^n = (a_1 \ldots a_{\lambda_1})^n (b_1 \ldots b_{\lambda_2})^n \cdots (c_1 \ldots c_{\lambda_r})^n$$

so, if $\sigma^n = e$, we must have that λ_i divides n for all $1 \leq i \leq r$ since the cycles are disjoint. Thus, the lcm of $\lambda_1, \ldots, \lambda_r$ divides $|\sigma|$. On the other hand, it is clear by the considerations above that $\sigma^{\operatorname{lcm}(\lambda_1,\ldots,\lambda_r)} = e$ and we conclude that $|\sigma| = \operatorname{lcm}(\lambda_1, \ldots, \lambda_r)$. In particular, if the λ_i's are pairwise relatively prime, $|\sigma| = \lambda_1 \cdots \lambda_r$. ■

EXERCISE 4.4 Make sense of the 'Taylor series' of the infinite product

$$\frac{1}{(1-x)} \cdot \frac{1}{(1-x^2)} \cdot \frac{1}{(1-x^3)} \cdot \frac{1}{(1-x^4)} \cdot \frac{1}{(1-x^5)} \cdot \ldots .$$

Prove that the coefficient of x^n in this series is the number of partitions of n.

■ SOLUTION G ■

EXERCISE 4.5

■ SOLUTION T ■

EXERCISE 4.6

■ SOLUTION A ■

EXERCISE 4.7 ▷ Prove that S_n is generated by (12) and $(12 \ldots n)$.
(Hint: It is enough to get all transpositions. What is the conjugate of (12) by $(12 \ldots n)$?) [4.9, §VII.7.5]

■ SOLUTION Let G be the subgroup of S_n generated by (12) and $(12 \ldots n)$. By Lemma 4.5, $\tau^{-1}(12)\tau = (1\tau\ 2\tau)$ for all $\tau \in S_n$. Thus, it follows that

$$((12 \ldots n)^k)^{-1}(12)(12 \ldots n)^k = (k\ k+1) \in G$$

for all $0 \leq k < n$. Now, let $\sigma \in S_n$ be any transposition. We may suppose that $\sigma = (ab)$, where $1 \leq a < b \leq n$. Take $\tau = (a\ a+1)(a+1\ a+2)\cdots(b-1\ b)$, which is in G. We have that

$$\tau^{-1}(a\ a+1)\tau = (a\tau\ (a+1)\tau) = (ba) = \sigma$$

and so $\sigma \in G$. Therefore, G contains all transpositions and, by Lemma 4.11, we conclude that $G = S_n$, as desired. ∎

EXERCISE 4.8 ¬ For $n > 1$, prove that the subgroup H of S_n consisting of permutations fixing 1 is isomorphic to S_{n-1}. Prove that there are no proper subgroups of S_n properly containing H. [VII.7.17]

∎ SOLUTION G ∎

EXERCISE 4.9

∎ SOLUTION T ∎

EXERCISE 4.10

∎ SOLUTION A ∎

EXERCISE 4.11 Let p be a prime integer. Compute the number of p-Sylow subgroups of S_p. (Use Exercise 4.10.) Use this result and Sylow's third theorem to prove again the 'only if' implication in Wilson's theorem (cf. Exercise II.4.16.)

∎ SOLUTION The exponent of p in the prime factorization of $p!$ is 1, so p-Sylow subgroups of S_p are cyclic groups C_p. Thus, to compute the number N_p of Sylow subgroups of S_p, we can find the number of elements of order p in S_p. By Exercise 4.3, a permutation has order p if and only if it has type $[p]$, that is, if and only if it is a p-cycle. By Exercise 4.10, it follows that there are $(p-1)!$ elements of order p in S_p. Since the p-Sylow subgroups can only meet at the identity (because they are cyclic groups of prime order) and each one has $p-1$ elements of order p, it follows that

$$N_p(p-1) = (p-1)! \implies N_p = (p-2)!$$

and so S_p has $(p-2)!$ p-Sylow subgroups.

The third Sylow theorem implies that $N_p = (p-2)! \equiv 1 \mod p$. Multiplying by $p-1$ we get that

$$(p-1)! \equiv p-1 \equiv -1 \mod p,$$

which proves the 'only if' implication in Wilson's theorem. ∎

EXERCISE 4.12 ▷ A subgroup G of S_n is *transitive* if the induced action of G on $\{1,\ldots,n\}$ is transitive.

- Prove that if $G \subseteq S_n$ is transitive, then $|G|$ is a multiple of n.

- List the transitive subgroups of S_3.
- Prove that the following subgroups of S_4 are all transitive:
  - $\langle (1234) \rangle \cong C_4$ and its conjugates,
  - $\langle (12)(34), (13)(24) \rangle \cong C_2 \times C_2$,
  - $\langle (12)(34), (1234) \rangle \cong D_8$ and its conjugates,
  - A_4, and S_4.

  With a bit of stamina, you can prove that there are the *only* transitive subgroups of S_4.

[§VII.7.5]

■ SOLUTION G ■

EXERCISE 4.13

■ SOLUTION T ■

EXERCISE 4.14

■ SOLUTION A ■

EXERCISE 4.15 Justify the 'pictorial' recipe given in §4.3 to decide whether a permutation is even.

■ SOLUTION Let $\sigma \in S_n$ be a permutation whose Young diagram has n_e rows of even size and n_o rows of odd size. Note that $n \equiv n_o \mod 2$ and that σ is even if and only if $n_e \equiv 0 \mod 2$, that is, if and only if there is an even number of rows of even size, which correspond to cycles of odd parity. Adding these congruences we obtain that σ is even if and only if n and the number $n_e + n_0$ of rows in the Young diagram of σ have the same parity. ■

EXERCISE 4.16 The number of conjugacy classes in A_n, $n \geq 2$, is (allegedly)

$$1, 3, 4, 5, 7, 9, 14, 18, 24, 31, 43, \ldots .$$

Check the first several numbers in this list by finding the class formulas for the corresponding alternating groups.

■ SOLUTION G ■

EXERCISE 4.17

■ SOLUTION T ■

EXERCISE 4.18

■ SOLUTION A ■

EXERCISE 4.19 Prove that for $n \geq 5$ there are no nontrivial actions of A_n on any set S with $|S| < n$. Construct a nontrivial action of A_4 on a set S, $|S| = 3$. Is there a nontrivial action of A_4 on a set S with $|S| = 2$?

■ SOLUTION Suppose that for some $n \geq 5$ there exists a nontrivial action of A_n on a set S with $m = |S| < n$. Thus, there exists a nontrivial group homomorphism $\varphi : A_n \to S_m$ and, since A_n is simple, φ is injective by Exercise 2.5. Hence, A_n is isomorphic to a subgroup of S_m and Lagrange's theorem implies that $|A_n| = \frac{n!}{2}$ divides $|S_m| = m!$. But this is impossible since $\frac{m!}{2} < \frac{n!}{2} \neq m!$. Therefore, for $n \geq 5$ there are no nontrivial actions of A_n on any set S with $|S| < n$.

We can construct a nontrivial action of A_4 on $S = \{1, 2, 3\}$ by realizing A_4 as the rotation group of the tetrahedron (see Exercise II.2.8), as Aluffi mentions. Identifying the pairs of opposite edges of the tetrahedron with the numbers 1, 2 and 3, we can define a nontrivial right-action where $x\sigma$ represents where the pair of opposite edges x goes after we apply the corresponding rotation of the even permutation σ to the tetrahedron. Algebraically, we can find an analogous action by knowing that $N = \{e, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of A_4. Since $A_4/N \cong C_3$ by order considerations and C_3 may be viewed as a subgroup of S_3, we can define a homomorphism $\varphi : A_4 \to S_3$ whose kernel is N, and this defines a left-action of A_4 on S. Note that the first action is a right-action and the second is a left-action, but they are closely related. By Exercise II.9.3 we can turn the first action into a left-action of A_4° on S. Applying the isomorphism between A_4 and A_4° given there, we get our second action. (Perhaps you will have to realize C_3 in S_3 in a different way to really get to the second action.)

Finally, note that there is no nontrivial action of A_4 on a set with two elements. Indeed, if it did exist, we would have a surjective group homomorphism $\varphi : A_4 \to S_2$ and it would follow from Corollary II.8.2 (first isomorphism theorem) and Lagrange's theorem that $|\ker \varphi| = 6$, which is impossible by Exercise 4.17. ■

EXERCISE 4.20 ¬ Find all fifteen elements of order 2 in A_5, and prove that A_5 has exactly five 2-Sylow subgroups. [4.22]

■ SOLUTION G ■

EXERCISE 4.21

■ SOLUTION T ■

EXERCISE 4.22

■ SOLUTION A ■

5 PRODUCTS OF GROUPS

EXERCISE 5.1 ▷ Let G be a finite group, and let $P_1, \dots, P_r$ be its nontrivial Sylow subgroups. Assume that all P_i are normal in G.

- Prove that $G \cong P_1 \times \cdots \times P_r$. (Induction of r; use Proposition 5.3.)
- Prove that G is nilpotent. (Hint: Mod out by the center, and work by induction of $|G|$. What is the center of a direct product of groups?)

Together with Exercise 3.10, this shows that a finite group is nilpotent if and only if each of its Sylow subgroups is normal. [3.12, §6.1]

■ SOLUTION G ■

EXERCISE 5.2

■ SOLUTION T ■

EXERCISE 5.3 Let

$$G = G_0 \supsetneq G_1 \supsetneq \cdots \supsetneq G_r = \{e\}$$

be a normal series. Show how to 'connect' $\{e\}$ to G by means of r exact sequences of groups using the groups G_i and the quotients $H_i = G_i/G_{i+1}$.

■ SOLUTION We can 'connect' $\{e\}$ to G by the short exact sequences that represent the quotients H_i:

$$1 \longrightarrow G_r = \{e\} \longrightarrow G_{r-1} \longrightarrow H_{r-1} \longrightarrow 1\,,$$

$$1 \longrightarrow G_{r-1} \longrightarrow G_{r-2} \longrightarrow H_{r-2} \longrightarrow 1\,,$$

$$\vdots$$

$$1 \longrightarrow G_1 \longrightarrow G_0 = G \longrightarrow H_0 \longrightarrow 1\,.$$

As in the example just before Definition 5.6, this tells us that G is an extension of H_0 by an extension of H_1 by an extension of H_2 ... by an extension of H_{r-1} by $\{e\}$. ■

EXERCISE 5.4

■ SOLUTION A ■

EXERCISE 5.5 In Proposition III.7.5 we have seen that is an exact sequence

$$0 \longrightarrow M \xrightarrow{\varphi} N \longrightarrow N/(\varphi(M)) \longrightarrow 0$$

of *abelian* groups splits, then φ has a left-inverse. Is this necessarily the case for split sequences of *groups*?

■ SOLUTION G ■

EXERCISE 5.6

■ SOLUTION T ■

EXERCISE 5.7 Let N be a group, and let $\alpha : N \to N$ be an automorphism of N. Prove that α may be realized as conjugation, in the sense that there exists a group G containing N as a normal subgroup and such that $\alpha(n) = gng^{-1}$ for some $g \in G$.

■ SOLUTION Let $\epsilon_\alpha : \mathbb{Z} \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ be the exponential map given by $\epsilon_\alpha(n) = \alpha^n$ for all $n \in \mathbb{Z}$ and take $G = N \rtimes_{\epsilon_\alpha} \mathbb{Z}$. By Proposition 5.10, N is contained in G as a normal subgroup and α can be realized as conjugation by $(e_N, 1)$ in G. ■

EXERCISE 5.8

■ SOLUTION A ■

EXERCISE 5.9 ▷ Prove that if $G = N \rtimes H$ is commutative, then $G \cong N \times H$. [§6.1]

■ SOLUTION G ■

EXERCISE 5.10

■ SOLUTION T ■

EXERCISE 5.11 ▷ For all $n > 0$ express D_{2n} as a semidirect product $C_n \rtimes_\theta C_2$, finding θ explicitly. [§5.3]]

■ SOLUTION By Exercise II.2.5, D_{2n} is generated by $x, y \in D_{2n}$ such that $x^2 = e$, $y^n = e$ and $yx = xy^{-1}$. Take the subgroups $N = \langle y \rangle$ and $H = \langle x \rangle$ of G. It is clear that $N \cap H = \{e\}$ and $D_{2n} = NH$. Moreover, since $[G : N] = 2$, we also know that N is normal in G. Thus, if $\gamma : H \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ is the homomorphism defined by

$$\gamma_h(n) = hnh^{-1}$$

for all $h \in H$, $n \in N$, Proposition 5.11 implies that $D_{2n} \cong N \rtimes_\gamma H$.

Since $N \cong C_n$ and $H \cong C_2$, we just have to figure it out how is γ when we change N and H by C_n and C_2 through the correspond-

ing isomorphisms. Let $\theta : C_2 \to \mathrm{Aut}_{\mathsf{Grp}}(C_n)$ be this homomorphism corresponding to γ. It is clear that $\theta_{[0]_2} = \mathrm{id}_{C_n}$. Now, note that

$$\gamma_x(y^k) = xy^kx^{-1} = xy^kx = xxy^{-k} = (y^k)^{-1}$$

for all $y^k \in N$. Thus, we must have

$$\theta_{[1]_2}(g) = g^{-1}$$

for all $g \in C_n$. This really is an automorphism of C_n since C_n is commutative. Therefore, we conclude that $D_{2n} \cong C_n \rtimes_\theta C_2$, where θ is given as above. ∎

EXERCISE 5.12

∎ SOLUTION A ∎

EXERCISE 5.13 ¬ Let $G = N \rtimes_\theta H$ be a semidirect product, and let K be the subgroup of G corresponding to $\ker\theta \subseteq H$. Prove that K is the kernel of the action of G on the set G/H of left-cosets of H. [5.14]

∎ SOLUTION G ∎

EXERCISE 5.14

∎ SOLUTION T ∎

EXERCISE 5.15 ▷ Let G be a group of order 28.

- Prove that G contains a normal subgroup N of order 7.
- Recall (or prove again) that, up to isomorphism, the only groups of order 4 are C_4 and $C_2 \times C_2$. Prove that there are two homomorphisms $C_4 \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ and two homomorphisms $C_2 \times C_2 \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ up to the choice of generators for the sources.
- Conclude that there are four groups of order 28 up to isomorphism: the two direct products $C_4 \times C_7$, $C_2 \times C_2 \times C_7$, and two noncommutative groups.
- Prove that $D_{28} \cong C_2 \times D_{14}$. The other noncommutative group of order 28 is a *generalized quaternionic group*.

[§5.3]

∎ SOLUTION

- Let N_7 be the number of 7-Sylow subgroups of G. By the third Sylow theorem, N_7 divides 4 and is congruent to 1 modulo 7, so we must have $N_7 = 1$. This implies that G contains a unique 7-Sylow subgroup N, which is of order 7 and must be normal.

- To recall that C_4 and $C_2 \times C_2$ are the only groups of order 4 up to isomorphism, see Exercise II.1.6.

  By Exercise II.4.15, $\mathrm{Aut}_{\mathsf{Grp}}(N) \cong C_6$, so $\mathrm{Aut}_{\mathsf{Grp}}(N)$ has only one element of order 2, which is the automorphism σ that sends each element to its inverse. Since a homomorphism $C_4 \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ is completely determined by the image of $[1]_4$ and its order must divide $|[1]_4| = 4$, there are only two such homomorphisms; the trivial one α_e and the homomorphism α_σ which sends $[1]_4$ to σ.

  The other case is similar to the previous one. A homomorphism $C_2 \times C_2 \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ is completely determined by the images of $([1]_2, [0]_2)$ and $([0]_2, [1]_2)$, which must have order 1 or 2. This tells us that there are actually four such homomorphisms, but the three that are not trivial are essentially the same and depend on the choice of generators for $C_2 \times C_2$. More formally, we mean that, if f_1 and f_2 are such homomorphisms, there is an automorphism φ of $C_2 \times C_2$ such that $f_1 \circ \varphi = f_2$. Thus, there are two homomorphisms $C_2 \times C_2 \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ up to choice of generators: the trivial one β_e and the homomorphism β_σ which sends $([1]_2, [0]_2)$ and $([0]_2, [1]_2)$ to σ.

- Let H be any 2-Sylow subgroup of G. By order constraints, we have that $N \cap H = \{e\}$. We claim that $G = NH$. To prove this, it suffices to show that $|NH| = 28$. Let $f : N \times H \to NH$ be the function given by

  $$f(n, h) = nh$$

  for all $n \in N$, $h \in H$, which is clearly surjective. Notice that f is also injective since

  $$\begin{aligned} f(n_1, h_1) = f(n_2, h_2) &\implies n_1 h_1 = n_2 h_2 \\ &\implies n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H = \{e\} \\ &\implies n_1 = n_2 \text{ and } h_1 = h_2 \\ &\implies (n_1, h_1) = (n_2, h_2). \end{aligned}$$

  Thus, f is a bijection and so $|NH| = |N \times H| = 28$, as desired. Since N is normal in G, it follows from Proposition 5.11 that $G \cong N \rtimes H$ for a suitable homomorphism $H \to \mathrm{Aut}_{\mathsf{Grp}}(N)$.

  Since $H \cong C_4$ or $H \cong C_2 \times C_2$, the previous item implies that G is isomorphic to one of the following groups: $G_1 = C_7 \rtimes_{\alpha_e} C_4$, $G_2 = C_7 \rtimes_{\alpha_\sigma} C_4$, $G_3 = C_7 \rtimes_{\beta_e} (C_2 \times C_2)$ or $G_4 = C_7 \rtimes_{\beta_\sigma} (C_2 \times C_2)$. We will prove that these groups are not isomorphic to each other. Firstly, since α_e and β_e are trivial, $G_1 \cong C_4 \times C_7$ and $G_3 \cong C_2 \times C_2 \times C_7$. Note that these two groups are abelian. On the other hand, since α_σ and β_σ are nontrivial, it follows from Exercise 5.9 that G_2 and G_4 are noncommutative. Hence, we just need to check that $G_1 \ncong G_3$ and $G_2 \ncong G_4$. Indeed, by the second Sylow theorem, p-Sylow subgroups are conjugate to each other

and, since conjugation preserves operation, they are isomorphic. Therefore, since $C_4 \ncong C_2 \times C_2$ and C_4 is a 2-Sylow subgroup of G_1 and G_2 and $C_2 \times C_2$ is a 2-Sylow subgroup of G_3 and G_4, the results follows. We conclude that there are four groups of order 28 up to isomophirsm: $C_4 \times C_7 \cong C_{28}$, $C_2 \times C_2 \times C_7$, and two noncommutative groups.

- Let x and y be the generators of D_{14} as in Exercise II.2.5 and take $X = (0, x) \in C_2 \times D_{14}$ and $Y = (1, y) \in C_2 \times D_{14}$. Note that $|X| = 2$, $|Y| = 14$ and

$$YX = (1, yx) = (1, xy^6) = XY^{13}.$$

We claim that X and Y generate $C_2 \times D_{14}$. Indeed, it is easy to check that the powers of Y are all elements of the form $(0, y^k)$ and $(1, y^k)$ for some $0 \leq k < 7$, so multiplying by X if needed we get all elements of $C_2 \times D_{14}$. Therefore, $D_{28} \cong C_2 \times D_{14}$ since they have the same presentation.

Just to mention, note that D_{28} is isomorphic to G_4, as defined in the last item, since the other noncommutative group has elements of order 4 and D_{28} do not. The group G_2 is isomorphic to Dic_7 (see the Remark in Exercise 2.15). ∎

If $p > 3$ is a prime number such that $p \equiv 3 \mod 4$, a similar argument shows that the groups of order $4p$ are C_{4p}, $C_2 \times C_2 \times C_p$, D_{4p} and Dic_p.

Remark. An important observation to be made is that we just need to consider two of the four homomorphisms $C_2 \times C_2 \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ when we take the semidirect products. We will show that we can do this in general.

Claim. Let N, H be groups and let $\alpha, \beta : H \to \mathrm{Aut}_{\mathsf{Grp}}(N)$ be group homomorphisms. If there exists $\varphi \in \mathrm{Aut}_{\mathsf{Grp}}(H)$ such that $\alpha \circ \varphi = \beta$ then $N \rtimes_\alpha H \cong N \rtimes_\beta H$.

Proof. Define $\sigma : N \rtimes_\beta H \to N \rtimes_\alpha H$ by

$$\sigma(n, h) = (n, \varphi(h))$$

for all $(n, h) \in N \rtimes_\beta H$. Since φ is an automorphism, it is clear that σ is a bijection. We just need to check that σ is a homomorphism. Indeed,

$$\begin{aligned}
\sigma((n_1, h_1) \bullet_\beta (n_2, h_2)) &= \sigma(n_1 \beta_{h_1}(n_2), h_1 h_2) \\
&= (n_1 (\alpha \circ \varphi)_{h_1}(n_2), \varphi(h_1 h_2)) \\
&= (n_1 \alpha_{\varphi(h_1)}(n_2), \varphi(h_1)\varphi(h_2)) \\
&= (n_1, \varphi(h_1)) \bullet_\alpha (n_2, \varphi(h_2)) \\
&= \sigma(n_1, h_1) \bullet_\alpha \sigma(n_2, h_2)
\end{aligned}$$

for all $(n_1, h_1), (n_2, h_2) \in N \rtimes_\beta H$. Thus, we have the desired isomorphism.

EXERCISE 5.16

■ SOLUTION A ■

EXERCISE 5.17 Prove that the multiplicative group $\mathbb{H}^*$ of nonzero quaternions (cf. Exercise III.2) is isomorphic to a semidirect product $\mathrm{SU}_2(\mathbb{C}) \rtimes \mathbb{R}^+$. (Hint: Exercise III.2.5.) Is this semidirect product in fact direct?

■ SOLUTION G ■

6 FINITE ABELIAN GROUPS

EXERCISE 6.1

■ SOLUTION T ■

EXERCISE 6.2

■ SOLUTION A ■

EXERCISE 6.3 Let G be a noncommutative group of order p^3, where p is a prime integer. Prove that $Z(G) \cong \mathbb{Z}/p\mathbb{Z}$ and $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

■ SOLUTION By Corollary 1.9 and Lemma 1.5, the center of G is nontrivial and $G/Z(G)$ is not cyclic. Thus, we must have $|Z(G)| = p$ and so $Z(G) \cong \mathbb{Z}/p\mathbb{Z}$. Since $G/Z(G)$ has order p^2, we know from Exercise 1.6 that $G/Z(G)$ is commutative and so Theorem 6.6 implies that it is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/p^2\mathbb{Z}$. But it cannot be cyclic and, hence, we conclude that $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. ■

EXERCISE 6.4 Classify abelian groups of order 400.

■ SOLUTION G ■

EXERCISE 6.5

■ SOLUTION T ■

EXERCISE 6.6

■ SOLUTION A ■

EXERCISE 6.7 ¬ Let $p > 0$ be a prime integer, G a finite abelian group, and denote by $\rho : G \to G$ the homomorphism defined by $\rho(g) = pg$.

- Let A be a finite abelian group such that $pA = 0$. Prove that $A \cong \mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}$.

- Prove that $p \ker \rho$ and $p(\operatorname{coker} \rho)$ are both 0.
- Prove that $\ker \rho \cong \operatorname{coker} \rho$.
- Prove that every subgroup of G of order p is contained in $\ker \rho$ and that every subgroup of G of index p contains $\operatorname{im} \rho$.
- Prove that the number of subgroups of G of order p equals the number of subgroups of G of index p.

[6.8]

■ SOLUTION

- Since $pA = 0$, the order of every element of A divides p and so, every element besides the identity is of order p. By Cauchy's theorem, A must be a p-group. By Theorem 6.6,

$$A \cong \bigoplus_{i=1}^{k} \frac{\mathbb{Z}}{p^{n_i}\mathbb{Z}}$$

where $n_1 \geq n_2 \geq \cdots \geq n_k$ are positive integers such that $|G| = p^{n_1+\cdots+n_k}$. If $n_1 > 1$, $(1, 0, \ldots, 0)$ would be an element of order greater than p, contradicting our first considerations. Therefore, $n_1 = 1$ and so $A \cong \mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}$.

- For all $g \in \ker \rho$, we have that $pg = \rho(g) = 0$, so $p \ker \rho = 0$. Now, for all $g + \operatorname{im} \rho \in \operatorname{coker} \rho$, $p(g + \operatorname{im} \rho) = pg + \operatorname{im} \rho = \rho(g) + \operatorname{im} \rho = 0$, so $p(\operatorname{coker} \rho) = 0$ too.
- By the first isomorphism theorem, we have that $G/\ker \rho \cong \operatorname{im} \rho$, so it follows from Lagrange's theorem that

$$\frac{|G|}{|\ker \rho|} = |\operatorname{im} \rho| \implies |\ker \rho| = \frac{|G|}{|\operatorname{im} \rho|} = \left|\frac{G}{\operatorname{im} \rho}\right| = |\operatorname{coker} \rho|.$$

We conclude from the first two items that

$$\ker \rho \cong \bigoplus_{i=1}^{n} \frac{\mathbb{Z}}{p\mathbb{Z}} \cong \operatorname{coker} \rho,$$

where n is such that $|\ker \rho| = |\operatorname{coker} \rho| = p^n$.

- Let H be a subgroup of G of order p. Since all elements besides the identity are of order p, it follows that $pH = 0$, that is, $\rho(H) = 0$ and so $H \subseteq \ker \rho$. Now, let K be a subgroup of G of index p. Thus, G/K is of order p and so

$$p(g + K) = \rho(g) + K = K \implies \rho(g) \in K$$

for all $g \in G$, that is, $\operatorname{im} \rho \subseteq K$.

- We will prove this by induction on the order of G. If $|G| = 1$, the result is immediate. Now, suppose that $|G| > 1$ and that the result is valid for all abelian groups of order less than $|G|$. We have two cases: either $|\operatorname{coker}\rho| = |G|$ or $|\operatorname{coker}\rho| < |G|$.

  In the first case, we must have $\operatorname{im}\rho = 0$ and so $\ker\rho = G$. From the first two items we get that $G \cong \mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}$. Note that every subgroup of $\mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}$ is of the form $H_1 \oplus \cdots \oplus H_k$, where $H_1, \ldots, H_k$ are subgroups of $\mathbb{Z}/p\mathbb{Z}$. Since the only subgroups of $\mathbb{Z}/p\mathbb{Z}$ are $\{0\}$ and $\mathbb{Z}/p\mathbb{Z}$ itself, it follows that the subgroups of order p are those such that only one H_i is $\mathbb{Z}/p\mathbb{Z}$ and the other are trivial, while subgroups of index p are those such that only one H_i is trivial and the other are $\mathbb{Z}/p\mathbb{Z}$. Thus, it is clear that there is the same number of subgroups of order p and of subgroups of index p.

  In the second case, by the inductive hypothesis there exists a bijection between subgroups of $\operatorname{coker}\rho$ of order p and subgroups of $\operatorname{coker}\rho$ of index p. Since every subgroup of G of order p is contained in $\ker\rho$ and $\ker\rho \cong \operatorname{coker}\rho$, there exists a bijection between subgroups of G of order p and subgroups of $\operatorname{coker}\rho$ of index p. Furthermore, Proposition II.8.9 implies that there is a bijection between the subgroups of $\operatorname{coker}\rho$ and the subgroups of G that contain $\operatorname{im}\rho$. By the third isomorphism theorem, it preserves indices and, since every subgroup of G of index p contains $\operatorname{im}\rho$, we get that the number of subgroups of G of order p equals the number of subgroups of G of index p. ∎

EXERCISE 6.8 ¬ Let G be a finite abelian p-group, with elementary divisors $p^{n_1}, \ldots, p^{n_r}$ $(n_1 \geq n_2 \geq \ldots)$. Prove that G has a subgroup H with invariant divisors $p^{m_1}, \ldots, p^{m_s}$ $(m_1 \geq m_2 \geq \ldots)$ if and only if $s \leq r$ and $m_i \leq n_i$ for $i = 1, \ldots, s$. (Hint: One direction is immediate. For the other, with notation as in Exercise 6.7, compare $\ker\rho$ for H and G to establish $s \leq r$; this also proves the statement if all $n_i = 1$. For the general case use induction, noting that if $G \cong \bigoplus_i \mathbb{Z}/p^{n_i}\mathbb{Z}$, then $\rho(G) \cong \bigoplus_i \mathbb{Z}/p^{n_i-1}\mathbb{Z}$.)

Prove that the same description holds for the homomorphic images of G. [6.9]

■ SOLUTION G ■

EXERCISE 6.9

■ SOLUTION T ■

EXERCISE 6.10

■ SOLUTION A ■

EXERCISE 6.11

- Use the classification theorem for finite abelian groups (Theorem 6.6) to classify all finite modules over the ring $\mathbb{Z}/n\mathbb{Z}$.
- Prove that if p is prime, all finite modules over $\mathbb{Z}/p\mathbb{Z}$ are free.

THEOREM 6.6 Let G be a finite nontrivial abelian group. Then

- there exist prime integers $p_1, \ldots, p_r$ and positive integers n_{ij} such that $|G| = \prod_{i,j} p_i^{n_{i,j}}$ and
$$G \cong \bigoplus_{i,j} \frac{\mathbb{Z}}{p_i^{n_{ij}}\mathbb{Z}};$$
- there exist positive integers $1 < d_1 \mid \cdots \mid d_s$ such that $|G| = d_1 \cdots d_s$ and
$$G \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_s\mathbb{Z}}.$$

Further, these decompositions are uniquely determined by G.

■ SOLUTION

- Let M be a finite module over $\mathbb{Z}/n\mathbb{Z}$. Thus, there exists a ring homomorphism $\sigma : \mathbb{Z}/n\mathbb{Z} \to \mathrm{End}_{\mathsf{Ab}}(M)$ that represents the action of $\mathbb{Z}/n\mathbb{Z}$ on M. Since $|\mathrm{id}_M| = |\sigma([1]_n)|$ divides $|[1]_n| = n$, we know that the order of every element of M divides n. If $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime factorization of n, the classification theorem for finite abelian groups implies that we must have the following isomorphism of abelian groups:
$$M \cong \bigoplus_{i,j} \frac{\mathbb{Z}}{p_i^{n_{ij}}\mathbb{Z}},$$
for some positive integers n_{ij} such that $|M| = \prod_{i,j} p_i^{n_{ij}}$ and $n_{ij} \leq \alpha_i$ for all indices i and j. Conversely, note that every abelian group of the form given above admits a unique $\mathbb{Z}/n\mathbb{Z}$-module structure, since every element has order dividing n and so we can define the homomorphism σ. Moreover, the isomorphism above also preserves the structure of the modules and so it is indeed an isomorphism of $\mathbb{Z}/n\mathbb{Z}$-modules.

  Putting all together, we have the following classification:

  Classification for finite modules over $\mathbb{Z}/n\mathbb{Z}$. Let M be a finite nontrivial $\mathbb{Z}/n\mathbb{Z}$-module and let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the prime factorization of n. Then

- there exist positive integers n_{ij} such that $|M| = \prod_{i,j} p_i^{n_{ij}}$, $n_{ij} \leq \alpha_i$ and
$$M \cong \bigoplus_{i,j} \frac{\mathbb{Z}}{p_i^{n_{ij}}\mathbb{Z}};$$
- there exist positive integers $1 < d_1 \mid \cdots \mid d_s \mid n$ such that $|M| = d_1 \cdots d_s$ and
$$M \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_s\mathbb{Z}}.$$

Further, these decompositions are uniquely determined by M.

- Since p is prime, the previous item implies that all finite $\mathbb{Z}/p\mathbb{Z}$-modules are of the form $\mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z}$. By Claim III.6.3 (see Exercise III.6.1), they are all free. ∎

EXERCISE 6.12 Let G, H, K be finite abelian groups such that $G \oplus H \cong G \oplus K$. Prove that $H \cong K$.

∎ SOLUTION G ∎

EXERCISE 6.13

∎ SOLUTION T ∎

EXERCISE 6.14

∎ SOLUTION A ∎

EXERCISE 6.15 Let G be a finite abelian group, and let $a \in G$ be an element of *maximal* order in G. Prove that the order of every $b \in G$ divides $|a|$. (This essentially reproduces the result of Exercise II.1.15.)

∎ SOLUTION By the classification theorem for finite abelian groups, there exist positive integers $1 < d_1 \mid \cdots \mid d_n$ such that $|G| = d_1 \cdots d_n$ and
$$G \cong \frac{\mathbb{Z}}{d_1\mathbb{Z}} \oplus \cdots \oplus \frac{\mathbb{Z}}{d_n\mathbb{Z}},$$
so we will simply assume that $G = \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_n\mathbb{Z}$. Let $x = (x_1, \ldots, x_n) \in G$. Note that, if $x^k = 0$, then $x_i^k = 0$ and so $|x_i|$ divides k for all $1 \leq i \leq n$. This implies that $\operatorname{lcm}(|x_1|, \ldots, |x_n|)$ divides k and, since $x^{\operatorname{lcm}(|x_1|,\ldots,|x_n|)} = 0$, we have that $|x| = \operatorname{lcm}(|x_1|, \ldots, |x_n|)$. Since $|x_i|$ divides d_i which divides d_n, for all $x_i \in \mathbb{Z}/d_i\mathbb{Z}$ and $1 \leq i \leq n$, it follows that $|x|$ divides d_n for all $x \in G$. Finally, note that G have at least one element of order d_n, which is $(0, \ldots, 0, 1)$. Therefore, we conclude that $|a| = d_n$ and that $|b|$ divides $|a|$ for all $b \in G$. ∎

We give a different proof from the one given in Exercise II.1.15 to illustrate one application of the results of this section.

EXERCISE 6.16 Let G be an abelian group of order n, and assume that G has at most one subgroup of order d for all $d|n$. Prove that G is cyclic.

■ SOLUTION G ■

V

IRREDUCIBILITY AND FACTORIZATION IN INTEGRAL DOMAINS

1 CHAIN CONDITIONS AND EXISTENCE OF FACTORIZATIONS

EXERCISE 1.1

■ SOLUTION T ■

EXERCISE 1.2

■ SOLUTION A ■

EXERCISE 1.3 Let k be a field, and let $f \in k[x]$, $f \notin k$. For every subring R of $k[x]$ contaning 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

- Firstly, recall that $p(t)g(x) = p(f) \cdot g(x)$ for all $p(t) \in k[t]$ and $g(x) \in k[x]$, that is, the action of $p(t)$ on $g(x)$ is to multiply $g(x)$ by the polynomial obtained by substituting t by f in $p(t)$ (see Example III.5.6). If $d = \deg f$, we claim that $k[t]$ is generated by $1, x, \ldots, x^{d-1}$ as a $k[t]$-module. Let $\alpha \in k[x]$ and suppose that $\deg \alpha \geq d$. Dividing α by f with remainder, we get that

$$\alpha = fh_1 + r_1$$

where $h_1, r_1 \in k[x]$ and $\deg r_1 < d$. Since $f \notin k$, $d > 0$ and so $\deg h_1 < \deg \alpha$. Now, divide h_1 by f and get h_2 and r_2 similar as before. Continue this procedure until $\deg h_k < d$ for some k. Thus,

$$\alpha = f^k h_k + f^{k-1} r_k + \cdots + f r_2 + r_1,$$

where $\deg h_k, \deg r_k, \ldots, \deg r_1 < d$. It follows immediately that there are $p_0(t), \ldots, p_{d-1}(t) \in k[t]$ such that

$$\alpha = p_{d-1}(t)x^{d-1} + \cdots + p_1(t)x + p_0(t)1,$$

as desired. Therefore, $k[x]$ is finitely generated as a $k[t]$-module.

- By Lemma 1.3, $k[t]$ is Noetherian and so Corollary III.6.8 implies that $k[x]$ is Noetherian as a $k[t]$-module. Since R is a submodule of $k[x]$, it follows that R is finitely generated as a $k[t]$-module.

- Let R be a subring of $k[x]$ containing k. If $R = k$ then R is immediately Noetherian since it is a field. Suppose that $R \neq k$ and let $f \in R \setminus k$. By the previous item, the corresponding homomorphism $\varphi : k[t] \to R$ turns R into a finitely generated $k[t]$-module. Since $k[t]$ is Noetherian by Lemma 1.3, Corollary III.6.8 implies that R is Noetherian as a $k[t]$-module.

  Now, let I be an ideal of R and let's prove that it is finitely generated. Note that I can also be viewed as a $k[t]$-module since the action of any element of $k[t]$ is the same as multiplication by some element of R. Thus, I is a submodule of R and so it is finitely generated as a $k[t]$-module. This means that there are $i_1, \ldots, i_k \in I$ such that every element i of I may be written as

  $$i = p_1(t)i_1 + \cdots + p_k(t)i_k = p_1(f) \cdot i_1 + \cdots + p_k(f) \cdot i_k$$

  for some $p_1(t), \cdots, p_k(t) \in k[t]$. It follows that $I = (i_1, \cdots, i_k)$ and so it is finitely generated as an ideal of R as well. We conclude that R is a Noetherian ring. ∎

EXERCISE 1.4

∎ SOLUTION G ∎

EXERCISE 1.5

∎ SOLUTION T ∎

EXERCISE 1.6

∎ SOLUTION A ∎

EXERCISE 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.)

Lemma 1.3 (Hilbert's basis theorem). R Noetherian $\implies$ $R[x]$ Noetherian.

∎ SOLUTION Let I be an ideal of $R[[x]]$ and let's prove that I is finitely generated. Let $A_i \subseteq R$ be the set of dominant coefficients of series of order i in I, together with 0. We claim that A_i is an ideal of R for all

$i \in \mathbb{N}$. Firstly, $A_i \neq \emptyset$ since it contains 0. Now, if $a, b \in A_i$, there are $p_a(x), p_b(x) \in I$ of order i whose dominant coefficients are a and b, respectively. Note that either $a - b = 0 \in A_i$ or $p_a(x) - p_b(x) \in I$ is a series of order i whose dominant coefficient is $a - b$ and so $a - b \in A_i$. Moreover, we have that either $ra = 0 \in A_i$ or $rp_a(x) \in I$ is of order i whose dominant coefficient is ra and so $ra \in A_i$ for all $r \in R$. This proves our claim.

Also notice that $A_i \subseteq A_{i+1}$ for all $i \in \mathbb{N}$. Indeed, if $a \in A_i$, $a \neq 0$, there is $p_a(x) \in I$ of order i whose dominant coefficient is a and, thus, $xp_a(x) \in I$ has order $i+1$ and a as dominant coefficient, so $a \in A_{a+1}$. Thus, we get the the sequence $A_0 \subseteq A_1 \subseteq A_2 \subseteq \cdots$ of ideals of R. Since R is Noetherian, all these ideals are finitely generated and there exists $k \in \mathbb{N}$ such that $A_i = A_k$ for all $i \geq k$. Let $f_1^i(x), \ldots, f_{r_i}^i(x) \in I$ be series of order i whose dominant coefficients $a_1^i, \ldots, a_{r_i}^i$ generate A_i as an ideal of R, for all $0 \leq i \leq k$. We will prove that all these series generate the ideal I.

Let $\alpha(x) \in I$ be an arbitrary series of I and suppose that it is of order $d < k$. If a is the dominant coefficient of $\alpha(x)$ then $a \in A_d$ and there are $b_1, \ldots, b_{r_d} \in R$ such that

$$a = b_1 a_1^d + \cdots + b_{r_d} a_{r_d}^d,$$

so

$$\alpha(x) - b_1 f_1^d(x) - \cdots - b_{r_d} f_{r_d}^d(x) \in I$$

has order strictly greater than d. Repeating this procedure, we get a series $\alpha^*(x)$ of order $e \geq k$. If its dominant coefficient is a^* then $a^* \in A_e = A_k$ and there are $c_1, \ldots, c_{r_k} \in R$ such that

$$a^* = c_1 a_1^k + \cdots + c_{r_k} a_{r_k}^k,$$

so

$$\alpha^* - x^{e-k}(c_1 f_1^k(x) + \cdots + c_{r_k} f_{r_k}^k(x)) \in I$$

has order strictly greater than e. Finally, iterating this new process, we obtain a finite list of (possibly infinite) series $\beta_1(x), \ldots, \beta_{r_k}(x) \in R[[x]]$ such that

$$\alpha^*(x) - \beta_1(x) f_1^k(x) - \beta_{r_k} f_{r_k}^k(x) = 0,$$

which implies that $\alpha(x)$ really is in the ideal generated by the series listed above. Therefore, I is finitely generated and so $R[[x]]$ is Noetherian. ∎

EXERCISE 1.8

∎ SOLUTION G ∎

EXERCISE 1.9

∎ SOLUTION T ∎

EXERCISE 1.10

■ SOLUTION A ■

EXERCISE 1.11 Prove that the 'associate' relation is an equivalence relation.

■ SOLUTION Let R be a commutative ring. Recall that $a, b \in R$ are associate if and only if $(a) = (b)$. It is straightforward that this 'associate' relation is an equivalence relation since the equality of sets is itself an equivalence relation. ■

EXERCISE 1.12

■ SOLUTION G ■

EXERCISE 1.13

■ SOLUTION T ■

EXERCISE 1.14

■ SOLUTION A ■

EXERCISE 1.15 ▷ Identify $S = \mathbb{Z}[x_1, \dots, x_n]$ in a natural way with a subring of the polynomial ring in countably infinitely many variables $R = \mathbb{Z}[x_1, x_2, x_3, \dots]$. 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. [§1.3, §4.3]

■ SOLUTION We can naturally identify S as the set of all polynomials in R only in the variables $x_1, \dots, x_n$. It is clear that this set is a subring of R isomorphic to S. Thus, we may assume that $S \subseteq R$.

The fact that $\mathbb{Z}$ is an integral domain is essential here. For example, if we take $f(x) = x_1^2 \in \mathbb{Z}/4\mathbb{Z}[x_1]$ and $g(x) = x_1 + 2x_2 \in \mathbb{Z}/4\mathbb{Z}[x_1, \dots]$, we have that $(f) \subseteq (g)$ since $f = (x_1 - 2x_2)g$, but $g \notin \mathbb{Z}/4\mathbb{Z}[x_1]$.

Now, let $f \in S$, $f \neq 0$ and $g \in R$ be such that $(f) \subseteq (g)$ in R. This implies that there exists $h \in R$ such that $f = gh$. We will show that $g, h \in S$. Let m be the largest index such that x_m appears as a variable in g or h, and suppose that $m > n$. Thus, we may identify g and h as polynomials of $\mathbb{Z}[x_1, \dots, x_n, \dots, x_m]$ as we did before. If we write g and h as polynomials in x_m with coefficients in $\mathbb{Z}[x_1, \dots, x_{m-1}]$ (recall that $\mathbb{Z}[x_1, \dots, x_m] = \mathbb{Z}[x_1, \dots, x_{m-1}][x_m]$), we conclude that x_m appears as a variable in $gh = f$ by the same argument given in Exercise III.1.15 since $\mathbb{Z}[x_1, \dots, x_{m-1}]$ is an integral domain. But this contradicts that $f \in S$. Therefore, we must have $m \leq n$ and so $g, h \in S$, as desired.

For the last part, let $(f_0) \subseteq (f_1) \subseteq (f_2) \subseteq \cdots$ be an ascending chain of principal ideals in R. We may assume without loss of generality that n is the largest index such that x_n appears as a variable in f_0, so we have that $f_0 \in S$. Therefore, $f_i \in S$ for all $i \in \mathbb{N}$. Since S is Noetherian by Theorem 1.2, the chain of ideals stabilizes if we consider them as ideals in S. Thus, there exists k such that $(f_i) = (f_k)$ in S for all $i \geq k$.

But this clearly implies that $(f_i) = (f_k)$ in R for all $i \geq k$ and so the chain of ideals stabilizes. By Proposition 1.11, R is a domain with factorizations. ∎

EXERCISE 1.16

∎ SOLUTION G ∎

EXERCISE 1.17

∎ SOLUTION T ∎

2 UFDS, PIDS, EUCLIDEAN DOMAINS

EXERCISE 2.1

∎ SOLUTION A ∎

EXERCISE 2.2

∎ SOLUTION G ∎

EXERCISE 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's find a composition series for $\mathbb{Z}/n\mathbb{Z}$. Since it is abelian, we need not worry about normality but only about the simplicity of the quotients. If $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime factorization of n, we can define the following normal series:

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \supsetneq \frac{p_1\mathbb{Z}}{n\mathbb{Z}} \supsetneq \cdots \supsetneq \frac{p_1^{\alpha_1}\mathbb{Z}}{n\mathbb{Z}} \supsetneq \frac{p_1^{\alpha_1}p_2\mathbb{Z}}{n\mathbb{Z}} \supsetneq \cdots \supsetneq \frac{p_1^{\alpha_1}p_2^{\alpha_2}\mathbb{Z}}{n\mathbb{Z}} \supsetneq \cdots \supsetneq \{0\}.$$

In this series we are adding one prime factor at each step until we get to $n\mathbb{Z}/n\mathbb{Z} = \{0\}$. By the third isomorphism theorem, each quotient is isomorphic to $\mathbb{Z}/p_i\mathbb{Z}$ for some i, which is simple. Therefore, this series is indeed a composition series for $\mathbb{Z}/n\mathbb{Z}$. It follows immediately that there is a one-to-one correspondence preserving multiplicities between the irreducible factors of n and the composition factors of $\mathbb{Z}/n\mathbb{Z}$. ∎

Remark. As pointed out in the statement of the exercise, the Jordan-Hölder theorem may be used to prove that $\mathbb{Z}$ is a UFD as follows. Let n be an integer greater than 1. Since $\mathbb{Z}/n\mathbb{Z}$ is finite, it admits a composition series (see Exercise IV.3.3), which is of the form

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \supsetneq \frac{n_1\mathbb{Z}}{n\mathbb{Z}} \supsetneq \cdots \supsetneq \frac{n_{k-1}\mathbb{Z}}{n\mathbb{Z}} \supsetneq \frac{n\mathbb{Z}}{n\mathbb{Z}} = \{0\}$$

where $n_1, \cdots, n_{k-1}$ are positive divisors of n. Let $n_0 = 1$ and $n_k = n$. By the inclusions, we must have that n_i divides n_{i+1} for all $0 \leq i < k$. Furthermore, since each quotient is simple and isomorphic to $\mathbb{Z}/(n_{i+1}/n_i)\mathbb{Z}$, we must have that n_{i+1}/n_i is a prime number. Thus, since

$$n = \frac{n_k}{n_{k-1}} \cdots \frac{n_1}{n_0},$$

it follows that n can be factorized as a product of irreducible elements in $\mathbb{Z}$, which are prime integers by definition. Finally, the Jordan-Hölder theorem guarantees the uniqueness of the factorization (as stated in Definition 1.8) because each factorization corresponds to a composition series for $\mathbb{Z}/n\mathbb{Z}$ (as shown in the exercise) and each composition factor corresponds to a prime number. Note that this property naturally extends to negative numbers and so we conclude that $\mathbb{Z}$ is indeed a UFD.

EXERCISE 2.4

■ SOLUTION T ■

EXERCISE 2.5

■ SOLUTION A ■

EXERCISE 2.6

■ SOLUTION G ■

EXERCISE 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. [§2.3]

■ SOLUTION Let I be an ideal of R. Since R is Noetherian, I is finitely generated, that is, there are $a_1, \ldots, a_n \in I$ such that $I = (a_1, \ldots, a_n)$. Let d be a gcd of a_1 and a_2. By the definition of R, there are $r, s \in R$ such that $d = ra_1 + sa_2$. Thus, it follows that $a_1, a_2 \in (d, a_3, \ldots, a_n)$ and $d \in (a_1, a_2, a_3, \ldots, a_n) = I$, so $I = (d, a_3, \ldots, a_n)$. Repeating this procedure of reducing the set of generators of I sometimes, we get that $I = (r)$ for some $r \in I$ and so I is principal. We conclude that R is a PID. ■

Note that r is a gcd of $a_1, \ldots, a_n$.

EXERCISE 2.8

■ SOLUTION T ■

EXERCISE 2.9

■ SOLUTION A ■

EXERCISE 2.10

■ SOLUTION G ■

EXERCISE 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 Let $I_1 \supseteq I_2 \supseteq \cdots$ be a descending chain of ideals in R/I. These ideals correspond to ideals of R containing I, so we have a corresponding descending chain of principal ideals in R. By Proposition 2.6, R is also a UFD, so Exercise 2.8 implies that this chain of principal ideals must stabilize since I is nonzero. It follows that our original chain also stabilizes and so R/I is Artinian. ■

EXERCISE 2.12

■ SOLUTION T ■

EXERCISE 2.13

■ SOLUTION A ■

EXERCISE 2.14

■ SOLUTION G ■

EXERCISE 2.15 Prove that if R is an Euclidean domain, then R admits a Euclidean valuation $\overline{v}$ such that $\overline{v}(ab) \geq \overline{v}(b)$ 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 $\overline{v}(a)$ 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 $\overline{v}$ 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 $\overline{v}(r) \geq \overline{v}(b)$, and get a contradiction.) [§2.4, 2.16]

■ SOLUTION Following the hint, let v be an Euclidean valuation on R and, for $a \neq 0$, define $\overline{v}(a)$ as the minimum of all $v(ab)$ as $b \in R, b \neq 0$. It follows that $\overline{v}(ab) \geq \overline{v}(b)$ for all nonzero $a, b \in R$. Let's prove that $\overline{v}$ is also an Euclidean valuation on R.

Let a, b be nonzero elements in R with $b \nmid a$ and choose $q, r \in R$ so that $a = bq + r$ with $v(r)$ minimal. Assume that $\overline{v}(r) \geq \overline{v}(b)$. Thus, there exists $c \in R$, $c \neq 0$ such that $v(bc) \leq v(r)$. Since v is an Euclidean valuation on R, there are $q', r' \in R$ such that $a = bcq' + r'$ with either $r' = 0$ or $v(r') < v(bc) \leq v(r)$. But we cannot have $r = 0$ because it would imply that $b|a$, and it is also impossible that $v(r') < v(r)$ by the definition of r. Therefore, we have a contradiction and it follows that $\overline{v}(r) < \overline{v}(b)$. This proves that $\overline{v}$ is indeed an Euclidean evaluation on R, as desired. ■

EXERCISE 2.16

■ SOLUTION T ■

EXERCISE 2.17

■ SOLUTION A ■

EXERCISE 2.18

■ SOLUTION G ■

EXERCISE 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.

[2.20, VIII.1.19]

■ SOLUTION

- Firstly, R is nonempty since $0 \in R$. Moreover, note that $v(1) = 0$ since v preserves identities, so $1 \in R$. Thus, we also have that $2v(-1) = v(1) = 0$ and so $v(-1) = 0$ and $-1 \in R$. This implies that $v(-r) = v(r)$ and $-r \in R$ for all $r \in R$, $r \neq 0$. Now, let $a, b \in R$ be nonzero elements. It is clear that $ab \in R$ since $v(ab) = v(a) + v(b) \geq 0$. Further, either $a + b = 0$ or $v(a+b) \geq \min(v(a), v(b)) \geq 0$, which implies that $a + b \in R$. From all these considerations, we conclude that R is a subring of k.
- We claim that v restricted to R is an Euclidean valuation. Let $a, b \in R$ with $b \neq 0$. If $a = 0$, it is immediate that $a = b \cdot 0 + 0$, so we may assume that $a \neq 0$. If $v(a) < v(b)$, we can take $q = 0$ and $r = a$, obtaining $a = bq + r$ with $v(r) < v(b)$. Otherwise, $v(ab^{-1}) = v(a) - v(b) \geq 0$, so $ab^{-1} \in R$ and we can take $q = ab^{-1}$ and $r = 0$, following that $a = bq + r$. In any case, there are $q, r \in R$ such that $a = bq + r$ with $r = 0$ or $v(r) < v(b)$. Therefore, we conclude that R is indeed a Euclidean domain with v as a Euclidean valuation.

- Let's define a discrete valuation v on $\mathbb{Q}$ as follows. Given $r \in \mathbb{Q}^*$, there are $a, b \in \mathbb{Z}$ not divisible by p and a unique $x \in \mathbb{Z}$ such that
$$r = p^x \frac{a'}{b'}.$$
Define $v(r) = x$. This function v is clearly surjective and note that, if $a, b, c, d \in \mathbb{Z}$ are not divisible by p and $x, y \in \mathbb{Z}$, then
$$v\left(p^x \frac{a}{b} \cdot p^y \frac{c}{d}\right) = v\left(p^{x+y} \frac{ac}{bd}\right) = x + y = v\left(p^x \frac{a}{b}\right) + v\left(p^y \frac{c}{d}\right),$$
so v is a group homomorphism between $(\mathbb{Q}^*, \cdot)$ and $(\mathbb{Z}, +)$. Finally, if $p^x a/b + p^y c/d \neq 0$ and $m = \min(x, y)$, then
$$v\left(p^x \frac{a}{b} + p^y \frac{c}{d}\right) = v\left(p^m \frac{p^{x-m} ad + p^{y-m} bc}{bd}\right) \geq m$$
since bd is not divisible by p. Therefore, v is indeed a discrete valuation on $\mathbb{Q}$ and it is easy to see that the ring of rational numbers a/b with b not divisible by p is given by $R = \{r \in \mathbb{Q}^* \mid v(r) \geq 0\} \cup \{0\}$. ■

EXERCISE 2.20

■ SOLUTION T ■

EXERCISE 2.21

■ SOLUTION A ■

EXERCISE 2.22

■ SOLUTION G ■

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

■ SOLUTION Executing the Euclidean algorithm, we get the following equations:

$$\begin{aligned}
5504227617645696 &= 2922476045110123 \cdot 1 + 2581751572535573 \\
2922476045110123 &= 2581751572535573 \cdot 1 + 340724472574550 \\
2581751572535573 &= 340724472574550 \cdot 7 + 196680264513723 \\
340724472574550 &= 196680264513723 \cdot 1 + 144044208060827 \\
196680264513723 &= 144044208060827 \cdot 1 + 52636056452896 \\
144044208060827 &= 52636056452896 \cdot 2 + 38772095155035 \\
52636056452896 &= 38772095155035 \cdot 1 + 13863961297861 \\
38772095155035 &= 13863961297861 \cdot 2 + 11044172559313 \\
13863961297861 &= 11044172559313 \cdot 1 + 2819788738548 \\
11044172559313 &= 2819788738548 \cdot 3 + 2584806343669 \\
2819788738548 &= 2584806343669 \cdot 1 + 234982394879 \\
2584806343669 &= 234982394879 \cdot 11.
\end{aligned}$$

Therefore, $d = 234982394879$. To find a and b, we can use substitute each of these equations into the previous one, starting from the penultimate one. By doing so, we find that possible values for a and b are $a = 1055$ and $b = -1987$. ■

EXERCISE 2.24

■ SOLUTION T ■

EXERCISE 2.25

■ SOLUTION A ■

3 INTERMEZZO: ZORN'S LEMMA

EXERCISE 3.1

■ SOLUTION G ■

EXERCISE 3.2

■ SOLUTION T ■

EXERCISE 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 By Exercise I.2.2, we know that the axiom of choice implies that a set-function is surjective if and only if it has a right-inverse. Let's show that the converse also holds. Assume that a set-

function is surjective if and only if it has a right-inverse. Let $\mathscr{F}$ be a family of disjoint nonempty subsets of a set Z. Define a function

$$f : \bigcup_{S \in \mathscr{F}} S \to \mathscr{F}$$

by letting $f(x)$ be the subset of Z in $\mathscr{F}$ that contains x, for all $x \in \bigcup_{S \in \mathscr{F}} S$. Since the subsets in $\mathscr{F}$ are disjoint, f is well-defined. Moreover, since they are nonempty, we also know that f is surjective. Therefore, f admits a right-inverse g. Since $f \circ g = \mathrm{id}_{\mathscr{F}}$, it follows that $g(S) \in S$ for all $S \in \mathscr{F}$. Thus, $\operatorname{im} g$ is a set formed by selecting one element of each $S \in \mathscr{F}$. We conclude that the axiom of choice is true, stablishing the equivalence in the exercise. ∎

EXERCISE 3.4

∎ SOLUTION A ∎

EXERCISE 3.5

∎ SOLUTION G ∎

EXERCISE 3.6

∎ SOLUTION T ∎

EXERCISE 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.

THEOREM 3.3 (Well-ordering theorem). Every set admits a well-ordering.

■ SOLUTION

- To construct a γ-woset $(S, \leq)$, we need to define a least element a in S. By the definition of a γ-woset, we are forced to define $a = \gamma(\emptyset)$, since there will not be any element preceding a with respect to $\leq$. It is clear that any γ-woset must have it least element as $\gamma(\emptyset)$ by the same reason.

- Since $(U, \leq'') \prec (T, \leq')$, we know that $U \subsetneq T$. Thus, $T \setminus U$ is nonempty and has a least element x with respect to $\leq'$ because $\leq'$ is a well-ordering on T. It follows that the set $X = \{b \in T, b <' x\}$ is contained in U. In fact, we claim that $X = U$. We will prove this by contradiction. Suppose that $X \subsetneq U$. Hence, $U \setminus X$ is nonempty and has a least element y with respect to $\leq''$ because $\leq''$ is a well-ordering on U. Let $Y = \{b \in U, b <'' y\}$ and let's prove that $X = Y$. If $b \in Y$, then b must be in X since $b <'' y$, so we have the inclusion $Y \subseteq X$. For the other inclusion, firstly note that $x <' y$. Indeed, by Exercise 3.1, we can compare x and y and certainly $x \leq' y$ since $y \notin X$. On the other hand $x \neq y$ since $x \notin U$ and $y \in U$, and so $x <' y$. Thus, if $b \in X$ then $b \in U$ and

$$b <' x \implies b <' y \implies b <'' y \implies b \in Y,$$

as desired. By the definition of a γ-woset,

$$x = \gamma(X) = \gamma(Y) = y,$$

but this contradicts that $x \neq y$. Therefore, we must have $X = U$ and so $\gamma(U) = x \in T$.

- Ainda não sei.

- Suppose that $(U, \leq'')$ is different from $(S, \leq)$ and $(T, \leq')$. By the second item, $\gamma(U) \in S$ and $\gamma(U) \in T$. Define $V = U \cup \{\gamma(U)\}$ and extend $\leq''$ to $\leq'''$ by setting $u <''' \gamma(U)$ for all $u \in U$ and $\gamma(U) \leq''' \gamma(U)$. It is clear that $(V, \leq''')$ is a γ-woset and that $V \subseteq S$ and $V \subseteq T$. Let's prove that $\leq'''$ is the restriction of $\leq$ and $\leq'$ to V. We just need to verify this between every element of U and $\gamma(U)$. As in the proof of the second item, there are $x \in S$ and $y \in T$ such that $b \in U \iff b < x$ and $b \in U \iff b <' y$. Since $\gamma(U) \notin U$, $x \leq \gamma(U)$ and $y \leq' \gamma(U)$ and so it follows by transitivity that $u < \gamma(U)$ and $u <' \gamma(U)$ for all $u \in U$.

It follows that $(V, \leq''')$ precedes both $(S, \leq)$ and $(T, \leq')$ with respect to $\preceq$. But this contradicts the definition of $(U, \leq'')$ since $(U, \leq'') \prec (V, \leq''')$. Therefore, we conclude that $(U, \leq'')$ must equal $(S, \leq)$ or $(T, \leq')$.

- Não tenho certeza
- Suppose that $M \neq Z$. As in the fourth item, we can define $M' = M \cup \{\gamma(M)\}$ and $\leq'$ such that $(M', \leq')$ is a γ-woset. It follows that $(M, \leq) \prec (M', \leq')$, contradicting that $(M, \leq)$ is maximal. Therefore, we must have $M = Z$ and so Z admits a well-ordering. ∎

EXERCISE 3.8

∎ SOLUTION A ∎

EXERCISE 3.9

∎ SOLUTION G ∎

EXERCISE 3.10

∎ SOLUTION T ∎

EXERCISE 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.)

PROPOSITION 3.13 Let R be a PID, and let I be a nonzero ideal in R. Then I is prime if and only if it is maximal.

PROPOSITION 3.5 Let $I \neq (1)$ be a proper ideal of a commutative ring R. Then there exists a maximal ideal $\mathfrak{m}$ of R containing I.

∎ SOLUTION If R is a PID, Proposition III.4.13 implies that every nonzero prime ideal in R is maximal. To prove the converse, we will follow the hint.

Suppose that every nonzero prime ideal in R is maximal. Let M be a maximal ideal of R. If $m \in M$, we can factorize m into irreducible factors since R is an UFD. It follows that one of these factors, say p, is in M since M is, in particular, a prime ideal. By Lemma 2.4, p is prime and so (p) is a prime ideal. By hypothesis, (p) is maximal and, since $(p) \subseteq M$, we have that $M = (p)$, following that M is principal.

Let I be any nontrivial and proper ideal of R. Denote by $n(I)$ the minimum number of irreducible factors that every nonzero element

in I must have. We will prove that I is principal by induction in $n(I)$. If $n(I) = 1$, there exists $q \in I$ irreducible, which is prime and so (q) is maximal, implying that $I = (q)$ since $(q) \subseteq I$. Now, suppose that $n(I) > 1$ and that every nontrivial and proper ideal J of R with $n(J) < n(I)$ is principal. By Proposition 3.5, there exists a maximal ideal (p) of R containing I, where $p \in R$ is irreducible. Thus, every element of I has p as an irreducible factor. Let

$$J = \{x \in R \mid px \in I\}.$$

It is clear that J is a nontrivial and proper ideal of R and that $n(J) < n(I)$. By the inductive hypothesis, $J = (a)$ for some $a \in R$ and, since every element of I is divisible by p,

$$I = pJ = p(a) = (pa),$$

that is, I is principal, as desired. We conclude that R is a PID. ∎

EXERCISE 3.12

∎ SOLUTION A ∎

EXERCISE 3.13

∎ SOLUTION G ∎

EXERCISE 3.14

∎ SOLUTION T ∎

EXERCISE 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 $\mathscr{F} \neq \emptyset$, 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_1J_2 and J_1/J_1J_2.
- Prove that I/J_1J_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

- Let $\mathscr{C}$ be a chain of ideals in $\mathscr{F}$ and consider
$$U := \bigcup_{J \in \mathscr{C}} J.$$
It is clear that U is an ideal since $\mathscr{C}$ is a chain (see the proof of Proposition 3.5). Now, assume that U is finitely generated, that is, $U = (a_1, \ldots, a_n)$ for some $a_1, \ldots, a_n \in U$. Thus, there are ideals $J_1, \ldots, J_n \in \mathscr{C}$ such that $a_i \in J_i$ for all i. It is easy to check that any finite subset of $\mathscr{C}$ has a greatest element with respect to inclusion, so $a_1, \ldots, a_n \in J_i$ for some i. This implies that $J_i = U$, which contradicts the fact that J_i is not finitely generated. Therefore, U cannot be finitely generated and hence it is an upper bound for $\mathscr{C}$ in $\mathscr{F}$. This proves that every chain in $\mathscr{F}$ has an upper bound, and it follows that $\mathscr{F}$ has a maximal element I, by Zorn's lemma.

- Let A be a nontrivial ideal of R/I. Thus, there exists an ideal J of R properly containing I such that $A = J/I$. Since I is a maximal element in $\mathscr{F}$, J must be finitely generated and it follows that A is also finitely generated. Therefore, every ideal of R/I is finitely generated and so R/I is Noetherian.

- Since I is not finitely generated, I is not a prime ideal of R. This implies that there are $a, b \in R$ such that $a, b \notin I$ but $ab \in I$. Define
$$J_1 := I + (a) \text{ and } J_2 := I + (b).$$
It is clear that J_1, J_2 are ideals of R properly containing I. To prove that $J_1 J_2 \subseteq I$, it suffices to show that every element of the form $j_1 j_2$ with $j_1 \in J_1$ and $j_2 \in J_2$ is in I. Indeed, if $j_1 \in J_1$ and $j_2 \in J_2$, there are $i_1, i_2 \in I$ and $r_1, r_2 \in R$ such that
$$j_1 = i_1 + r_1 a \text{ and } j_2 = i_2 + r_2 b.$$
Therefore,
$$j_1 j_2 = i_1 i_2 + (r_1 a) i_2 + (r_2 b) i_1 + (r_1 r_2)(ab) \in I$$
since $ab \in I$, so $J_1 J_2 \subseteq I$, as desired.

- A natural way to define this structure is to set
$$(r + I)(i + J_1 J_2) := (ri + J_1 J_2)$$
for all $r \in R$ and $i \in I$. If this action is well-defined, it follows easily that it turns $I/J_1 J_2$ into an R/I-module. To see that it is really well-defined, let $i \in I$ and $r, r' \in R$ be such that $r + I = r' + I$, that is, $r - r' \in I$. Since $I \subseteq J_1, J_2$, we have that
$$(r - r')i \in J_1 J_2 \implies ri - r'i \in J_1 J_2 \implies ri + J_1 J_2 = r'i + J_1 J_2,$$
which tells us that this action is really well-defined. Note that we can give a structure of R/I-module to $J_1/J_1 J_2$ in the same fashion.

- We just need to prove that J_1/J_1J_2 is a finitely generated R/I-module. Indeed, if this is the case, Corollary III.6.8 implies that J_1/J_1J_2 is a Noetherian module because R/I is Noetherian by the second item. Since $I \subseteq J_1$, we have that I/J_1J_2 is contained in J_1/J_1J_2 as a submodule and so I/J_1J_2 is a finitely generated R/I-module.

  Since J_1 properly contains I, J_1 must be a finitely generated ideal of R and so there are $x_1, \dots, x_n \in J_1$ such that $J_1 = (x_1, \dots, x_n)$. We claim that J_1/J_1J_2 is generated by $x_1 + J_1J_2, \dots, x_n + J_1J_2$ as an R/I-module. Indeed, if $j_1 + J_1J_2 \in J_1/J_1J_2$, there are $r_1, \dots, r_n \in R$ such that

  $$j_1 = r_1x_1 + \cdots + r_nx_n$$

  and so

  $$j_1 + J_1J_2 = (r_1 + I)(x_1 + J_1J_2) + \cdots + (r_n + I)(x_n + J_1J_2).$$

  Therefore, J_1/J_1J_2 is a finitely generated R/I-module, as desired.

- By the previous item, I/J_1J_2 is generated (as an R/I-module) by some $i_1 + J_1J_2, \dots, i_k + J_1J_2 \in I/J_1J_2$. Moreover, since J_1 and J_2 properly contain I, they are finitely generated ideals of R and so $J_1J_2 = (j_1, \dots, j_l)$ for some $j_1, \dots, j_l \in J_1J_2 \subseteq I$. Let's prove that $I = (i_1, \dots, i_k, j_1, \dots, j_l)$. If $i \in I$, there are $r_1, \dots, r_k \in R$ such that

  $$\begin{aligned} i + J_1J_2 &= (r_1 + I)(i_1 + J_1J_2) + \cdots + (r_k + I)(i_k + J_1J_2) \\ &= (r_1i_1 + \cdots + r_ki_k) + J_1J_2. \end{aligned}$$

  Therefore,

  $$i - (r_1i_1 + \cdots + r_ki_k) \in J_1J_2,$$

  which implies that there are $s_1, \dots, s_l \in R$ such that

  $$i = r_1i_1 + \cdots + r_ki_k + s_1j_1 + \cdots + s_lj_l.$$

  This proves our claim and we reach a contradiction since I is not finitely generated by definition. We conclude that we must have $\mathscr{F} = \emptyset$, that is, R is Noetherian. ∎

4 UNIQUE FACTORIZATION IN POLYNOMIAL RINGS

EXERCISE 4.1

∎ SOLUTION A ∎

EXERCISE 4.2

∎ SOLUTION G ∎

EXERCISE 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. [§4.1]

■ SOLUTION For any ring R, a polynomial $f \in R[x]$ is primitive if it is very primitive, by definition. Now, if R is PID, the converse also holds since every prime ideal of R is principal. However, it may not be true in an arbitrary UFD. For instance, take $R = \mathbb{Z}[x]$ (which is a UFD by Theorem 4.14) and $f = x + (x+2)y \in R[y]$. It is easy to check that $\gcd(x, x+2) = 1$ and so f is primitive by Lemma 4.5. On the other hand, $(x, x+2) = (2, x)$ do not equal (1) by Exercise III.4.3 and it follows (again by Lemma 4.5) that f is not very primitive. ■

EXERCISE 4.4

■ SOLUTION T ■

EXERCISE 4.5

■ SOLUTION A ■

EXERCISE 4.6

■ SOLUTION G ■

EXERCISE 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 $l : R \to S^{-1}R$.
- Prove that $l(s)$ 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 $0 \in S$.

[4.8, 4.9, 4.11, 4.15, VII.2.16, VIII.1.4, VIII.2.5, VIII.2.6, VIII.2.12, §IX.9.1]

■ SOLUTION

- Firstly, we have that $(a,s) \sim (a,s)$ for all $(a,s) \in R \times S$ since $1 \cdot (sa - sa) = 0$ and $1 \in S$. Also note that, if $(a,s) \sim (a',s')$, then there exists $t \in S$ such that $t(s'a - sa') = 0$, so $t(sa' - s'a) = 0$ and $(a',s') \sim (a,s)$. Now, if $(a,s) \sim (a',s')$ and $(a',s') \sim (a'',s'')$, there are $t_1, t_2 \in S$ such that $t_1(s'a - sa') = t_2(s''a' - s'a'') = 0$. Thus,

$$\begin{aligned}(s't_1t_2)(s''a - sa'') &= (t_1s'a)(t_2s'') - (t_2s'a'')(t_1s)\\ &= (t_1sa')(t_2s'') - (t_2s''a')(t_1s)\\ &= t_1t_2sa's'' - t_1t_2sa's'' = 0\end{aligned}$$

  and, since $s't_1t_2 \in S$, $(a,s) \sim (a'',s'')$. We conclude that $\sim$ is an equivalence relation.

- As in §4.2, we define operations on such 'fractions' as follows:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1s_2 + a_2s_1}{s_1s_2},$$
$$\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1a_2}{s_1s_2}.$$

  Let's verify that they are well-defined. Firstly, note that the fractions on the right are indeed valid fractions since $s_1s_2 \in S$ because S is multiplicatively closed.Now, let $\frac{a_1}{s_1}, \frac{a_1'}{s_1'}, \frac{a_2}{s_2}, \frac{a_2'}{s_2'}$ be such that

$$\frac{a_1}{s_1} = \frac{a_1'}{s_1'} \text{ and } \frac{a_2}{s_2} = \frac{a_2'}{s_2'},$$

  that is, there are $t_1, t_2 \in S$ such that

$$t_1(s_1'a_1 - s_1a_1') = t_2(s_2'a_2 - s_2a_2') = 0.$$

  Thus, $t_1t_2 \in S$ and note that

$$(t_1t_2)((a_1s_2 + a_2s_1)(s_1's_2') - (a_1's_2' + a_2's_1')(s_1s_2)) = 0$$

  and

$$(t_1t_2)(a_1a_2s_1's_2' - a_1'a_2's_1s_2) = 0,$$

  so

$$\frac{a_1s_2 + a_2s_1}{s_1s_2} = \frac{a_1's_2' + a_2's_1'}{s_1's_2'} \text{ and } \frac{a_1a_2}{s_1s_2} = \frac{a_1'a_2'}{s_1's_2'}.$$

  We conclude that these operations are indeed well-defined.

- Let's prove that $S^{-1}R$ is a commutative ring. The associative property for $+$ and $\cdot$ follows from associativity and distributivity in R. It also follows immediately that $+$ and $\cdot$ are commutative since commutativity holds in R both for sum and for multiplication. Further, $\frac{0}{1}$ and $\frac{1}{1}$ are the additive and multiplicative identities, respectively, and for all $a \in R$ and $s \in S$ we have that

$$-\left(\frac{a}{s}\right) = \frac{(-a)}{s}.$$

Finally, the computation done just after Definition 4.10 also proves the distributive property in $S^{-1}R$. Thus, $S^{-1}R$ is indeed a commutative ring.

Now, define $l : R \to S^{-1}R$ by $l(a) = \frac{a}{1}$ for every $a \in R$. This function is a ring homomorphism because $l(1) = \frac{1}{1}$, which is the multiplicative identity of $S^{-1}R$, and

$$l(a+b) = \frac{a+b}{1} = \frac{a \cdot 1 + b \cdot 1}{1 \cdot 1} = \frac{a}{1} + \frac{b}{1} = l(a) + l(b)$$

$$l(a \cdot b) = \frac{ab}{1} = \frac{ab}{1 \cdot 1} = \frac{a}{1} \cdot \frac{b}{1} = l(a) \cdot l(b)$$

for all $a, b \in R$.

- We have that

$$l(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1}$$

and so $l(s)$ is invertible for every $s \in S$. Note that $\frac{1}{s}$ is well-defined since $s \in S$.

- Let $f : R \to R'$ be a ring homomorphism from R to a ring R' such that $f(s)$ is invertible in R' for every $s \in S$. As in Claim 4.11, we need to define an induced homomorphism $\varphi : S^{-1}R \to R'$ so that the diagram

$$\begin{array}{ccc} S^{-1}R & \xrightarrow{\varphi} & R' \\ & {\scriptstyle l}\nwarrow \quad \nearrow{\scriptstyle f} & \\ & R & \end{array}$$

commutes, and we must show that φ is unique. Now, the definition of φ is in fact forced upon us: if φ exists as a homomorphism, then necessarily

$$\begin{aligned} \varphi\left(\frac{a}{s}\right) &= \varphi\left(\frac{a}{1}\right)\varphi\left(\left(\frac{s}{1}\right)^{-1}\right) \\ &= \varphi\left(\frac{a}{1}\right)\varphi\left(\frac{s}{1}\right)^{-1} \\ &= ((\varphi \circ l)(a))((\varphi \circ l)(s))^{-1} \\ &= f(a)f(s)^{-1}. \end{aligned}$$

Thus φ is indeed unique, if it exists. On the other hand, the prescription

$$\varphi\left(\frac{a}{s}\right) \coloneqq f(a)f(s)^{-1}$$

does define a function $S^{-1}R \to R'$. Indeed, firstly note that $f(s)$ is invertible since $s \in S$. Moreover, if $\frac{a}{s} = \frac{a'}{s'}$, there exists $t \in S$ such that

$$tas' = ta's$$

in R, hence

$$f(t)f(a)f(s') = f(t)f(a')f(s')$$

in R', and

$$f(a)f(s)^{-1} = f(a')f(s')^{-1}$$

since $f(t)$, $f(s)$ and $f(s')$ are invertible in R'. This shows that φ is well-defined. Finally, it is a ring homomorphism because

$$\begin{aligned}\varphi\left(\frac{a}{s} + \frac{a'}{s'}\right) &= f(as' + a's)f(ss')^{-1} \\ &= (f(a)f(s') + f(a')f(s))(f(s)^{-1}f(s')^{-1}) \\ &= f(a)f(s)^{-1} + f(a')f(s')^{-1} \\ &= \varphi\left(\frac{a}{s}\right) + \varphi\left(\frac{a'}{s'}\right)\end{aligned}$$

and

$$\begin{aligned}\varphi\left(\frac{a}{s} \cdot \frac{a'}{s'}\right) &= f(aa')f(ss')^{-1} \\ &= (f(a)f(s)^{-1}) \cdot (f(a')f(s')^{-1}) \\ &= \varphi\left(\frac{a}{s}\right) \cdot \varphi\left(\frac{a'}{s'}\right)\end{aligned}$$

for all $\frac{a}{s}, \frac{a'}{s'} \in S^{-1}R$, and $f(\frac{1}{1}) = 1_{R'}$. Therefore, it follows that l is initial among ring homomorphisms $f : R \to R'$ such that $f(s)$ is invertible in R' for every $s \in S$.

- We will suppose that $0 \notin S$ because, otherwise, $S^{-1}R$ would be the zero-ring by the next item. Thus, we just need to show that, if $\frac{a}{s}, \frac{a'}{s'} \in S^{-1}R$ are nonzero fractions, then $\frac{a}{s} \cdot \frac{a'}{s'} \neq \frac{0}{1}$. Indeed, if this product were equal to $\frac{0}{1}$, there would exist $t \in S$ such that

  $$t(aa' \cdot 1 - ss' \cdot 0) = taa' = 0.$$

  Since R is an integral domain and $t \neq 0$, $a = 0$ or $a' = 0$. But this implies that $\frac{a}{s}$ or $\frac{a'}{s'}$ would be equal to zero, a contradiction. Therefore, the product is nonzero, as desired.

- Note that $\frac{0}{1} = \frac{1}{1}$ if and only if there exists $t \in S$ such that

  $$t(1 \cdot 0 - 1 \cdot 1) = -t = 0$$

  and so if and only if $0 \in S$. By Exercise III.1.1, $S^{-1}R$ is the zero-ring if and only if $0 \in S$. ∎

EXERCISE 4.8

■ SOLUTION T ■

EXERCISE 4.9

■ SOLUTION A ■

EXERCISE 4.10

■ SOLUTION G ■

EXERCISE 4.11 ¬ (Notation as in Exercise 4.7 and 4.8) 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 localizations $S^{-1}R$, $S^{-1}M$ 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. [4.12, 4.13, VI.5.5, VII.2.17, VIII.2.21]

■ SOLUTION Let's prove that $S = R \setminus \mathfrak{p}$ is a multiplicative subset of R. Since $\mathfrak{p} \neq (1)$, we have that $1 \in S$. Moreover, since $\mathfrak{p}$ is prime,

$$st \in \mathfrak{p} \implies s \in \mathfrak{p} \text{ or } t \in \mathfrak{p}$$

and so

$$s, t \in S \implies st \in S,$$

by contraposition. Hence S is multiplicatively closed as desired.

For the second part, Exercise 4.10 tells us that there is an inclusion-preserving bijection between the prime ideals of R_p and the prime ideals of R disjoint from S. But an ideal is disjoint from S if and only if it is contained in $\mathfrak{p}$ and so the result follows. Furthermore, Proposition 3.5 implies that $R_{\mathfrak{p}}$ contains a maximal ideal, which is in particular prime and, thus, is contained in the corresponding prime ideal of $\mathfrak{p}$. It follows that $R_{\mathfrak{p}}$ have only one maximal ideal (the one corresponding to $\mathfrak{p}$), that is, $R_{\mathfrak{p}}$ is a local ring. ■

EXERCISE 4.12

■ SOLUTION T ■

EXERCISE 4.13

■ SOLUTION A ■

EXERCISE 4.14

■ SOLUTION G ■

EXERCISE 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.

[4.16]

■ SOLUTION

- We will suppose that $0 \notin S$ so that $S^{-1}R$ is an integral domain by Exercise 4.7. In this case, we just need to check that

$$\frac{q}{1} = \frac{a}{s} \cdot \frac{a'}{s'} \implies \left(\frac{a}{s} \text{ is a unit or } \frac{a'}{s'} \text{ is a unit} \right).$$

  Indeed, this equality means that there exists $t \in S$ such that

$$tqss' = taa'$$

  and so

$$qss' = aa'$$

  since R is an integral domain and $t \neq 0$. By Lemma 2.4, q is prime and so q divides a or q divides a'. Without loss of generality, we may suppose that $a = qb$ for some $b \in R$. Thus,

$$\frac{q}{1} = \frac{a}{s} \cdot \frac{a'}{s'} = \frac{q}{1} \cdot \frac{b}{s} \cdot \frac{a'}{s'} \implies \frac{b}{s} \cdot \frac{a'}{s'} = \frac{1}{1} \implies \frac{a'}{s'} \text{ is a unit,}$$

  as desired.

- Since R is a UFD, there are irreducible elements $q_1, \ldots, q_n \in R$ such that $a = q_1 \cdots q_n$ and we may write

$$\frac{a}{s} = \frac{1}{s} \cdot \frac{q_1}{1} \cdots \frac{q_n}{1}.$$

  By the previous item, each of the factors on the right is either irreducible or a unit. Since $\frac{a}{s}$ is itself irreducible, we have that only one $\frac{q_i}{1}$ can be irreducible and the other factors must be units. Thus, $\frac{a}{s}$ is associate to $\frac{q_i}{1}$, where q_i is an irreducible element of R.

- As in the proof of Theorem 2.5, it suffices to show that factorizations exist in $S^{-1}R$ and that every irreducible element of $S^{-1}R$ is prime. For the first part, let $\frac{a}{s} \in S^{-1}R$ be an arbitrary element. Since R is a UFD, $a = q_1 \cdots q_n$ where $q_1, \ldots, q_n \in R$ are irreducible elements. Thus, we may write

$$\frac{a}{s} = \frac{1}{s} \cdot \frac{q_1}{1} \cdots \frac{q_n}{1}$$

and, after grouping $\frac{1}{s}$ with other possible units, we get a factorization of $\frac{a}{s}$ by the first item.

For the second part, let $x \in S^{-1}R$ be an irreducible element. By the second item we may assume that $x = \frac{q}{1}$ for some irreducible element q of R. We claim that (q) is disjoint from S. Indeed, if it existed $r \in R$ such that $qr = s \in S$, then

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

and $\frac{q}{1}$ would be a unit, which is impossible since it is irreducible. Moreover, since R is a UFD, q is prime and so the ideal $S^{-1}(q)$ is a prime ideal of $S^{-1}R$ by Exercise 4.10. Finally, note that

$$S^{-1}(q) = \left(\frac{q}{1}\right)$$

and so we conclude that $\frac{q}{1}$ is prime, as desired.

Therefore, $S^{-1}R$ is indeed a UFD. ∎

EXERCISE 4.16

∎ SOLUTION T ∎

EXERCISE 4.17

∎ SOLUTION A ∎

EXERCISE 4.18

∎ SOLUTION G ∎

EXERCISE 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. [VI.7.11, §VII.2.3]

∎ SOLUTION Let $a \in R$ be nilpotent and let $n \geq 0$ be such that $a^n = 0$. If $n = 0$, then R must be the zero-ring and it follows immediately that $1 + a$ is invertible. If $n > 0$, we can use a famous identity. Notice that

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

for all $x, y \in R$ such that $xy = yx$. Thus, taking $x = 1$ and $y = a$, we get that $1 + a$ is a unit in R and

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

is its inverse. ∎

Remark. Recall that the Taylor series for the function $\frac{1}{1+x}$ is

$$\frac{1}{1+x} = 1 - x + x^2 - x^3 + \cdots.$$

Note that the inverse for $1+a$ that we found in the exercise can be reached by replacing x by a and using the fact that a is nilpotent. In this sense, the Taylor series can help us guessing what may be the inverse for a certain element.

EXERCISE 4.20

■ SOLUTION T ■

EXERCISE 4.21

■ SOLUTION A ■

EXERCISE 4.22

■ SOLUTION G ■

EXERCISE 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. [§4.3, 4.24, §VII.5.2]

■ SOLUTION Write $\alpha(x) = \frac{a_1}{a_2}\alpha'(x)$ and $\beta(x) = \frac{b_1}{b_2}\beta'(x)$, where a_1, a_2, b_1, $b_2 \in R$ and $\alpha'(x), \beta'(x) \in R[x]$ are primitive polynomials. Thus,

$$a_2 b_2 f(x) = a_1 b_1 \alpha'(x)\beta'(x)$$

and, by Gauss's lemma and Lemma 4.7,

$$(a_2 b_2 (\mathrm{cont}_{f(x)})) = (a_1 b_1).$$

If $d \in R$ is a content of $f(x)$ then there exists a unit $u \in R$ such that

$$a_2 b_2 d u = a_1 b_1$$

and we may take

$$c = \frac{a_2 d u}{a_1} \in K.$$

It is immediate that $c^{-1} = \frac{b_2}{b_1}$ and so both $c\alpha(x)$ and $c^{-1}\beta(x)$ are in $R[x]$.

For the second part, note that the leading coefficients of $c\alpha(x)$ and $c^{-1}\beta(x)$ must be inverses for each other since $f(x)$ is monic. This implies that c is in R and is a unit because α is also monic. Therefore, it follows that $\alpha(x)$ and $\beta(x)$ are in $R[x]$ and, since $f(x) = \alpha(x)\beta(x)$, $\beta(x)$ is also monic. ■

EXERCISE 4.24

■ SOLUTION T ■

EXERCISE 4.25

■ SOLUTION A ■

5 IRREDUCIBILITY OF POLYNOMIALS

EXERCISE 5.1

■ SOLUTION G ■

EXERCISE 5.2

■ SOLUTION T ■

EXERCISE 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 Consider the 'evaluation map' $\varphi : R[x] \to R[x]$ that sends x to $-x$, which is a homomorphism by Example III.2.3 and Exercise III.2.6. Since $g(x)$ is a factor of $f(x)$, there exists $h(x) \in R[x]$ such that

$$f(x) = g(x)h(x).$$

The fact that $f(x)$ is a polynomial only involving even powers of x implies that

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

and so $g(-x)$ is also a factor of $f(x)$. ■

EXERCISE 5.4

■ SOLUTION A ■

EXERCISE 5.5

■ SOLUTION G ■

EXERCISE 5.6

■ SOLUTION T ■

EXERCISE 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 The proof is analogous to the one given for Corollary 5.2. Indeed, let $r_1, \ldots, r_{d+1}$ be distinct elements of R. If there were a

polynomial $g(x) \in R[x]$ different from $f(x)$ such that $f(r_i) = g(r_i)$ for all $1 \leq i \leq d+1$, the polynomial $f(x) - g(x) \neq 0$ would have more than n distinct roots, which contradicts Lemma 5.1. Therefore, $f(x)$ is uniquely determined by its value at any $d+1$ distinct elements of R. ■

EXERCISE 5.8

■ SOLUTION A ■

EXERCISE 5.9

■ SOLUTION G ■

EXERCISE 5.10

■ SOLUTION T ■

EXERCISE 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.) [§5.3]

■ SOLUTION Fix $n > 0$ and let's show that there is an irreducible polynomial in F of degree at least n. For this, let $p_1, \ldots, p_k \in F$ be all irreducible polynomials in F of degree at most $n-1$. Since F is finite, this list is indeed finite as well. Consider the polynomial

$$f = p_1 \cdots p_k + 1.$$

We can take F as any finite UFD and the argument will still hold due to Theorem 4.14.

Note that, if f were divisible by p_i for some i then 1 would be divisible by p_i, contradicting that p_i is irreducible. Therefore, f is not divisible by any irreducible polynomial of degree at most $n-1$. Since F is a field, $F[x]$ is a UFD and so f is divisible by some irreducible polynomial, which must be of degree at least n, as desired. ■

EXERCISE 5.12

■ SOLUTION A ■

EXERCISE 5.13

■ SOLUTION G ■

EXERCISE 5.14

■ SOLUTION T ■

EXERCISE 5.15 Prove Lemma 5.10.

Lemma 5.10 A field k is algebraically closed if and only if every nonconstant 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 Let's deal with each equivalence one at a time. For the first one, suppose that k is algebraically closed. Then, since $k[x]$ is a UFD, every nonconstant polynomial in $k[x]$ is not a unit and factors completely as a product of irreducible polynomials, which must be linear. Conversely, if every nonconstant polynomial of $k[x]$ factors as a product of linear factors, then any polynomial of degree higher than 1 is reducible, which implies that k is algebraically closed.

For the second equivalence, if every nonconstant polynomial $f \in k[x]$ factors as a product of linear factors, Example III.4.7 implies that f has a root in k. Reciprocally, if every nonconstant polynomial $f \in k[x]$ has a root in k, we can repeatedly apply Example III.4.7 to get that

$$f = a(x - r_1)^{l_1} \cdots (x - r_n)^{l_n}$$

for some $a, r_1, \ldots, r_n \in k$ and positive integers $l_1, \ldots, l_n$, that is, f factors completely as a product of linear factors. ■

EXERCISE 5.16

■ SOLUTION A ■

EXERCISE 5.17

■ SOLUTION G ■

EXERCISE 5.18

■ SOLUTION T ■

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

■ SOLUTION Applying Eisenstein's criterion with $R = \mathbb{Z}$ and $\mathfrak{p} = (2)$ to the polynomial $f(x) = x^2 - 2 \in \mathbb{Z}[x]$, we get that $f(x)$ is not the product of polynomials of degree less than 2. It follows that $f(x)$ is irreducible in $\mathbb{Q}[x]$ and so Proposition 5.3 implies that $f(x)$ has no rational roots. Since $\sqrt{2}$ is a root of $f(x)$, we conclude that $\sqrt{2}$ is not rational. ■

A similar argument shows that $\sqrt[n]{p}$ is irrational for every $n > 1$ and p prime.

EXERCISE 5.20

■ SOLUTION A ■

EXERCISE 5.21

■ SOLUTION G ■

EXERCISE 5.22

■ SOLUTION T ■

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

■ SOLUTION Firstly, by Exercise 5.12 we have that

$$\frac{\mathbb{C}[x]}{(x)} \cong \mathbb{C}$$

and so (x) is a prime (even maximal) ideal of $\mathbb{C}[x]$. Thus, we may apply Eisenstein's criterion with $R = \mathbb{C}[x]$ and $\mathfrak{p} = (x)$ to the polynomial $y^5 + x^2y^3 + x^3y^2 + x \in \mathbb{C}[x, y] = \mathbb{C}[x][y]$, obtaining that it is not a product of polynomials of degree less than 5 (if they are viewed as polynomials in y). Since it is monic (as a polynomial in y), we conclude that $y^5 + x^2y^3 + x^3y^2 + x$ is irreducible in $\mathbb{C}[x, y]$. ■

EXERCISE 5.24

■ SOLUTION A ■

6 FURTHER REMARKS AND EXAMPLES

EXERCISE 6.1

■ SOLUTION G ■

EXERCISE 6.2

■ SOLUTION T ■

EXERCISE 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 We will prove this exercise by induction on the order of R. If $|R| = 1$, then R is the zero-ring, which may be considered as the 'empty' product of $\mathbb{Z}/2\mathbb{Z}$'s rings. If $|R| = 2$, then $R \cong \mathbb{Z}/2\mathbb{Z}$ since this is the only ring (up to isomorphism) with two elements. Now, let $|R| = n > 2$ and suppose that all finite Boolean rings with less than n elements are of the form $\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$. Take $a \in R$ different from 0 and 1. By Exercise III.3.15, R is commutative and so Exercise 6.2 implies that $R \cong R/(a) \times R/(1-a)$. Since (a) and $(1-a)$ are nontrivial ideals, $R/(a)$ and $R/(1-a)$ have less than n elements. These quotients are clearly Boolean rings, so it follows from the inductive hypothesis that they are of the form $\mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$. We conclude that $R \cong \mathbb{Z}/2\mathbb{Z} \times \cdots \times \mathbb{Z}/2\mathbb{Z}$ for a suitable number of factors $\mathbb{Z}/2\mathbb{Z}$. ■

EXERCISE 6.4

■ SOLUTION A ■

EXERCISE 6.5

■ SOLUTION G ■

EXERCISE 6.6

■ SOLUTION T ■

EXERCISE 6.7 ▷ Find a polynomial $f \in \mathbb{Q}[x]$ such that $f \equiv 1 \mod (x^2+1)$ and $f \equiv x \mod x^{100}$. [§6.1]

■ SOLUTION We will execute the procedure shown in §6.1. Firstly, note that the gcd between x^2+1 and x^{100} is 1 since x^2+1 is irreducible and does not divide x^{100}. We have to find polynomials $\alpha(x), \beta(x) \in \mathbb{Q}[x]$ such that $\alpha(x)(x^2+1)+\beta(x)(x^{100}) = 1$ and, to do so, notice that

Here we are actually using the Euclidean algorithm, as described in the procedure

$$x^{100} = (x^2+1)(x^{98} - x^{96} + \cdots + x^2 - 1) + 1.$$

Thus, we may take $\alpha(x) = -x^{98} + x^{96} - \cdots - x^2 + 1$ and $\beta(x) = 1$. As described in the procedure, one solution to the given system of congruences is

$$f = 1 \cdot \beta(x) \cdot x^{100} + x \cdot \alpha(x) \cdot (x^2+1) = -x^{101} + x^{100} + x.$$

We can also find the other solutions to this system of congruences. Indeed, every solution must be congruent to f modulo x^2+1 and modulo x^{100}. Since $\gcd(x^2+1, x^{100}) = 1$, any other solution is congruent to f modulo $x^{100}(x^2+1)$ and so is of the form

$$f + p \cdot x^{100}(x^2+1)$$

for some $p \in \mathbb{Q}[x]$. ■

EXERCISE 6.8

■ SOLUTION A ■

EXERCISE 6.9

■ SOLUTION G ■

EXERCISE 6.10

■ SOLUTION T ■

EXERCISE 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 Firstly, note that the numbers described in the exercise are irreducible elements in $\mathbb{Z}[i]$. Indeed, Lemma 6.10 assures that any integer prime congruent to 3 mod 4 is irreducible in $\mathbb{Z}[i]$. Furthermore, a number q in one of the other cases is also irreducible because its

norm is a prime integer: since the norm is multiplicative and the units in $\mathbb{Z}[i]$ are exactly the elements of norm 1, it follows that

$$q = ab \implies N(p) = N(a)N(b) \implies N(a) = 1 \text{ or } N(b) = 1,$$

that is, a or b is a unit, which implies that q is irreducible.

Now, let's prove that the numbers mentioned in the exercise encompass all irreducible elements in $\mathbb{Z}[i]$. Let $q \in \mathbb{Z}[i]$ be irreducible. Since $\mathbb{Z}[i]$ is a UFD, q is prime and Lemma 6.7 implies that $N(q) = p$ or $N(q) = p^2$ for some prime integer p. We will deal with each case separately.

Notice that $a + bi$ and $a - bi$ are not associates since $a^2 + b^2$ is odd and so a and b are different.

If $N(q)$ is a prime integer, Theorem 6.11 implies that either $N(q) = 2$ or $N(q)$ is congruent to 1 modulo 4 since $N(q)$ is a sum of two squares. In the first case, $N(q) = \pm 1 \pm i$ and all these numbers are associates to $1 + i$. In the other case, it is immediate that $q = a \pm bi$ with $a^2 + b^2$ an integer prime congruent to 1 mod 4.

If $N(q) = p^2$ for some prime integer p, we have that q divides p^2 and, since q is prime, q divides p. By Exercise 6.10, q is associate to p. Finally, this implies that p is irreducible and so p is congruent to 3 mod 4 by Lemma 6.10. ∎

EXERCISE 6.12

∎ SOLUTION A ∎

EXERCISE 6.13

∎ SOLUTION G ∎

EXERCISE 6.14

∎ SOLUTION T ∎

EXERCISE 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 Notice that the square of any integer is congruent to 0 or 1 modulo 4. This can be easily proved by testing the square of each element of $\mathbb{Z}/4\mathbb{Z}$. Therefore, a sum of two squares can only be congruent to 0, 1 or 2 modulo 4, and we conclude that n is not the sum of two squares. ∎

EXERCISE 6.16

∎ SOLUTION A ∎

EXERCISE 6.17

∎ SOLUTION G ∎

EXERCISE 6.18

■ SOLUTION T ■

EXERCISE 6.19 ¬ Let $\mathbb{I} \subseteq \mathbb{H}$ be the set of quaternions (cf. Exercise III.2) 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 $N(w_1w_2) = N(w_1)N(w_2)$.
- Prove that $\mathbb{I}$ has exactly 24 units in $\mathbb{I}$: ± 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*. [6.20, 6.21]

■ SOLUTION

- It is straightforward that $(\mathbb{I},+)$ is a subgroup of $(\mathbb{H},+)$ since it is clearly nonempty and $x-y \in \mathbb{I}$ for all $x,y \in \mathbb{I}$. Moreover, with some computation one can check that the product of two elements of $\mathbb{I}$ is also in $\mathbb{I}$, so this set is multiplicatively closed. Finally, since $1 = \frac{2}{2}(1+i+j+k) - i - j - k \in \mathbb{I}$, we conclude that $\mathbb{I}$ is a subring of the ring of quaternions.

- If $w = \frac{a}{2}(1+i+j+k)+bi+cj+dk$, we can rewrite it as

$$w = \frac{a}{2} + \left(\frac{a}{2}+b\right)i + \left(\frac{a}{2}+c\right)i + \left(\frac{a}{2}+d\right)k$$

and it follows that

$$\begin{aligned} N(w) &= \left(\frac{a}{2}\right)^2 + \left(\frac{a}{2}+b\right)^2 + \left(\frac{a}{2}+c\right)^2 + \left(\frac{a}{2}+d\right)^2 \\ &= a^2+b^2+c^2+d^2+a(b+c+d), \end{aligned}$$

which is an integer. By Exercise III.2.5, we know that $N(w_1w_2) = N(w_1)N(w_2)$ for all $w_1, w_2 \in \mathbb{I}$, since the norm defines a group homomorphism from the multiplicative group $\mathbb{H}^*$ of nonzero quaternions to the multiplicative group $\mathbb{R}^+$ of positive real numbers.

- We claim that $w \in \mathbb{I}$ is a unit if and only if $N(w) = 1$. Indeed, if w is a unit then

$$N(w)N(w^{-1}) = N(ww^{-1}) = N(1) = 1,$$

which implies that $N(w) = 1$ since it is an integer. Conversely, by the item (ii) in Exercise III.2, we know that $N(w) = w\overline{w} = \overline{w}w$,

where $\overline{w}$ is the *conjugate* of w, obtained by changing the signal of the coefficients of i, j and k. A quick verification shows that $\overline{w} \in \mathbb{I}$ and, if $N(w) = 1$, it follows that w is a unit and $w^{-1} = \overline{w}$.

Thus, we only need to find what are the integral quaternions of norm 1. By the previous item, any element $w \in \mathbb{I}$ may be written as

$$w = \frac{a}{2} + \left(\frac{a}{2} + b\right) i + \left(\frac{a}{2} + c\right) i + \left(\frac{a}{2} + d\right) k$$

where $a, b, c, d \in \mathbb{Z}$, and we have that

$$N(w) = \left(\frac{a}{2}\right)^2 + \left(\frac{a}{2} + b\right)^2 + \left(\frac{a}{2} + c\right)^2 + \left(\frac{a}{2} + d\right)^2.$$

If $N(w) = 1$, the squares on the right must be between 0 and 1. Also note that each one is the square of a reduced fraction whose denominator is 1 or 2. This implies that these squares can only be 0, $\frac{1}{4}$ or 1. Hence, there are two options: either one of the squares is 1 and the other are 0, which gives us the quaternions ± 1, $\pm i$, $\pm j$ and $\pm k$; or every square equals to $\frac{1}{4}$, which results in the quaternions $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$. Therefore, we conclude that these are the only units in $\mathbb{I}$.

- Write $w = \frac{a}{2}(1 + i + j + k) + bi + cj + dk$, where $a, b, c, d \in \mathbb{Z}$. If a is even, w is already in the desired form. Thus, suppose that a is an odd integer. We claim that w can be written as

$$w = \frac{a}{2}(1 \pm i \pm j \pm k) + 2(b'i + c'j + d'k)$$

where $b', c', d' \in \mathbb{Z}$. This representation depends on the parity of b, c and d. If one of these coefficients is odd, we may add a to it (which turns it even since a is odd) and change the signal of the corresponding imaginary number in the leftmost part. For example, if b and d are odd and c is even, note that

$$w = \frac{a}{2}(1 - i + j - k) + (b + a)i + cj + (d + a)k$$

and $b + a$, c and $d + a$ are even. Let u be the quaternion multiplying a in the expression above (in the example we gave, u would be $\frac{1}{2}(1 - i + j - k)$). By the previous item, we know that $u \in \mathbb{I}$ and is a unit. It follows that wu^{-1} can be written as $a'' + b''i + c''j + d''k$ with $a'', b'', c'', d'' \in \mathbb{Z}$. Indeed,

$$wu^{-1} = auu^{-1} + 2(b'i + c'j + d'k)u^{-1} = a + 2(b'i + c'j + d'k)u^{-1}$$

and the factor 2 will cancel with the factor 2 that appears in the denominators of the coefficients in u^{-1}, so only integers remain. Since u^{-1} is a unit, we conclude that w is an associate of an element in the desired form. ∎

EXERCISE 6.20

■ SOLUTION A ■

EXERCISE 6.21

■ SOLUTION G ■

VI

LINEAR ALGEBRA

1 FREE MODULES REVISITED

EXERCISE 1.1

■ SOLUTION T ■

EXERCISE 1.2 ¬ Prove that the sets listed in Exercise III.1.4 are all $\mathbb{R}$-vector spaces, and compute their dimensions. [1.3]

■ SOLUTION We can define an action of $\mathbb{R}$ on $\mathfrak{gl}_n(\mathbb{R})$ and $\mathfrak{gl}_n(\mathbb{C})$ by componentwise multiplication. Together with componentwise addition, we naturally identify them with $\mathbb{R}^{n^2}$ and $\mathbb{C}^{n^2}$ and so, $\mathfrak{gl}_n(\mathbb{R})$ and $\mathfrak{gl}_n(\mathbb{C})$ are $\mathbb{R}$-vector spaces. Moreover, it is easy to check that the functions

$$\begin{aligned} T_1 : \mathfrak{gl}_n(\mathbb{R}) &\to \mathbb{R} \\ M &\mapsto \operatorname{tr}(M) \end{aligned}$$

and

$$\begin{aligned} T_2 : \mathfrak{gl}_n(\mathbb{C}) &\to \mathbb{C} \\ M &\mapsto \operatorname{tr}(M) \end{aligned}$$

are homomorphisms of $\mathbb{R}$-vector spaces and $\ker T_1 = \mathfrak{sl}_n(\mathbb{R})$ and $\ker T_2 = \mathfrak{sl}_n(\mathbb{C})$, thus, these sets are also $\mathbb{R}$-vector spaces. Finally, $\mathfrak{so}_n(\mathbb{R})$ and $\mathfrak{su}(n)$ also admit a structure of vector space over $\mathbb{R}$ because they are the kernels of the $\mathbb{R}$-vector space homomorphisms

$$\begin{aligned} T_3 : \mathfrak{sl}_n(\mathbb{R}) &\to \mathfrak{sl}_n(\mathbb{R}) \\ M &\mapsto M + M^t \end{aligned}$$

and

$$\begin{aligned} T_4 : \mathfrak{sl}_n(\mathbb{C}) &\to \mathfrak{sl}_n(\mathbb{C}) \\ M &\mapsto M + M^\dagger, \end{aligned}$$

respectively.

Let's compute their dimensions. To do so, denote by E_{xy} the $n \times n$ matrix which is 1 in the x-th row and the y-th column, and 0 in the other entries. Also denote by E^*_{xy} the matrix E_{xy} but with the imaginary number i instead of 1. Therefore, the following sets are basis for the indicated $\mathbb{R}$-vector spaces:

$$B_{\mathfrak{gl}_n(\mathbb{R})} = \{E_{xy} \mid 1 \leq x, y \leq n\}$$

$$B_{\mathfrak{gl}_n(\mathbb{C})} = B_{\mathfrak{gl}_n(\mathbb{R})} \cup \{E^*_{xy} \mid 1 \leq x, y \leq n\}$$
$$B_{\mathfrak{sl}_n(\mathbb{R})} = \{E_{xy} \mid 1 \leq x, y \leq n, x \neq y\} \cup \{E_{xx} - E_{nn} \mid 1 \leq x < n\}$$
$$B_{\mathfrak{sl}_n(\mathbb{C})} = B_{\mathfrak{sl}_n(\mathbb{R})} \cup \{E^*_{xy} \mid 1 \leq x, y \leq n, x \neq y\} \cup \{E^*_{xx} - E^*_{nn} \mid 1 \leq x < n\}$$
$$B_{\mathfrak{so}_n(\mathbb{R})} = \{E_{xy} - E_{yx} \mid 1 \leq x < y \leq n\}$$
$$B_{\mathfrak{su}(n)} = B_{\mathfrak{so}_n(\mathbb{R})} \cup \{E^*_{xy} + E^*_{yx} \mid 1 \leq x < y \leq n\} \cup \{E^*_{xx} - E^*_{nn} \mid 1 \leq x < n\}$$

As an illustration, we will show that $B_{\mathfrak{so}_n(\mathbb{R})}$ really is a basis for $\mathfrak{so}_n(\mathbb{R})$. Firstly, a quick computation proves that this set is linear independent. We just need to check that it generates $\mathfrak{so}_n(\mathbb{R})$. If $M = (a_{xy}) \in \mathfrak{so}_n(\mathbb{R})$ then $M = -M^t$, that is, $a_{xy} = -a_{yx}$ for all $x, y \in \{1, \ldots, n\}$. In particular, we have that $a_{xx} = 0$. Thus,

$$\begin{aligned} M &= \sum_{1 \leq x,y \leq n} a_{xy} E_{xy} \\ &= \sum_{1 \leq x < y \leq n} a_{xy} E_{xy} + \sum_{1 \leq y < x \leq n} a_{xy} E_{xy} \\ &= \sum_{1 \leq x < y \leq n} a_{xy} E_{xy} + \sum_{1 \leq x < y \leq n} a_{yx} E_{yx} \\ &= \sum_{1 \leq x < y \leq n} a_{xy} E_{xy} - \sum_{1 \leq x < y \leq n} a_{xy} E_{yx} \\ &= \sum_{1 \leq x < y \leq n} a_{xy} (E_{xy} - E_{yx}), \end{aligned}$$

We could have computed these dimensions by other methods. For example, Claim 3.10 (also known as the *rank-nullity theorem)* allows us to calculate the last four dimensions since these vector spaces are the kernels of T_1, T_2, T_3 and T_4.

so $B_{\mathfrak{so}_n(\mathbb{R})}$ really generates $\mathfrak{so}_n(\mathbb{R})$, as desired.

We conclude that

$$\dim_{\mathbb{R}}(\mathfrak{gl}_n(\mathbb{R})) = n^2 \qquad \dim_{\mathbb{R}}(\mathfrak{gl}_n(\mathbb{C})) = 2n^2$$
$$\dim_{\mathbb{R}}(\mathfrak{sl}_n(\mathbb{R})) = n^2 - 1 \qquad \dim_{\mathbb{R}}(\mathfrak{sl}_n(\mathbb{C})) = 2n^2 - 2$$
$$\dim_{\mathbb{R}}(\mathfrak{so}_n(\mathbb{R})) = \frac{n(n-1)}{2} \qquad \dim_{\mathbb{R}}(\mathfrak{su}(n)) = n^2 - 1$$

are the desired dimensions. ∎

EXERCISE 1.3

∎ SOLUTION A ∎

EXERCISE 1.4

∎ SOLUTION G ∎

EXERCISE 1.5

∎ SOLUTION T ∎

EXERCISE 1.6 ▷ Prove Lemma 1.8. [§1.3]

■ SOLUTION To prove that B is a basis of V, it suffices to show that B is linear independent. Suppose that it is not, that is, there exist $b_1, \dots, b_n \in B$ and $c_1, \dots, c_n \in k$ such that

$$c_1 b_1 + \cdots + c_n b_n = 0$$

with not all $c_1, \dots, c_n$ equal to 0. Without loss of generality, we can assume that $c_1 \neq 0$. Since k is a field, c_1 is a unit and

$$b_1 = (-c_1^{-1} c_2) b_2 + \cdots + (-c_1^{-1} c_n) b_n.$$

It follows that $B \setminus \{b_1\}$ is a generating set for V because B is a generating set and b_1 is a linear combination of elements of $B \setminus \{b_1\}$. However, this contradicts that B is minimal and, therefore, we must have that B is linear independent and so is a basis for V.

The second part of Lemma 1.8 is covered by Proposition 1.15. ■

EXERCISE 1.7

■ SOLUTION A ■

EXERCISE 1.8

■ SOLUTION G ■

EXERCISE 1.9

■ SOLUTION T ■

EXERCISE 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. [1.11]

■ SOLUTION Firstly, note that $\mathfrak{m}(F/\mathfrak{m}F) = 0$ by definition of $\mathfrak{m}F$. By the previous exercise, we can define a vector space structure over k on $F/\mathfrak{m}F$ by setting

$$(r + \mathfrak{m})(f + \mathfrak{m}F) := rf + \mathfrak{m}F$$

for all $r \in R$ and $f \in F$.

Given $\alpha \in k^{\oplus B}$, we can define $f_\alpha : B \to R$ as follows: for every $b \in B$, set $f_\alpha(b) \in R$ such that $\alpha(b) = f_\alpha(b) + \mathfrak{m}$ and $f_\alpha(b) = 0$ if $\alpha(b) = \mathfrak{m}$. It is clear that $f_\alpha \in F$. Therefore, we can define the function

$$\begin{aligned} \varphi : k^{\oplus B} &\to F/\mathfrak{m}F \\ \alpha &\mapsto f_\alpha + \mathfrak{m}F. \end{aligned}$$

It is easy to check that φ is well-defined and that it is a homomorphism of k-vector spaces. We claim that φ is indeed a isomorphism.

If $\varphi(\alpha) = 0$, we have that $f_\alpha \in \mathfrak{m}F$. This implies that $f_\alpha(b) \in \mathfrak{m}$ and so $\alpha(b) = f_\alpha(b) + \mathfrak{m} = 0$ for all $b \in B$. Therefore, $\alpha = 0$ and $\ker \psi = 0$. It follows the φ is injective.

More generally, if I is any ideal of R then $F/IF \cong (R/I)^{\oplus B}$ as R/I-modules. The proof is analogous.

Moreover, if $x \in F/\mathfrak{m}F$ then there exists $f : B \to R$ such that $x = f + \mathfrak{m}F$. Define $\alpha : B \to k$ by $\alpha(b) = f(b) + \mathfrak{m}$ for all $b \in B$. We have that $\alpha \in k^{\oplus B}$ and $\varphi(\alpha) = x$, so φ is also surjective.

We conclude that φ is indeed an isomorphism and so $F/\mathfrak{m}F \cong k^{\oplus B}$.

■

EXERCISE 1.11

■ SOLUTION A ■

EXERCISE 1.12

■ SOLUTION G ■

EXERCISE 1.13

■ SOLUTION T ■

EXERCISE 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 $\operatorname{im} \varphi^{n+1} = \operatorname{im} \varphi^n$.

Show that both claims may fail if V has infinite dimension. [1.15]

■ SOLUTION An important observation here is that any subspace U of V is finite-dimensional and $\dim U \leq \dim V$. This follows from Propositions 1.7 and 1.9. Moreover, Corollary 1.11 implies that $U = V$ if and only if $\dim U = \dim V$.

Note that we have the following chains:

$$\ker \varphi \subseteq \ker \varphi^2 \subseteq \ker \varphi^3 \subseteq \cdots$$

$$\operatorname{im} \varphi \supseteq \operatorname{im} \varphi^2 \supseteq \operatorname{im} \varphi^3 \supseteq \cdots .$$

By our initial observation, every one of these vectors spaces is finite-dimensional and we have that

$$\dim(\ker \varphi) \leq \dim(\ker \varphi^2) \leq \dim(\ker \varphi^3) \leq \cdots \leq \dim V$$

and

$$\dim V \geq \dim(\operatorname{im} \varphi) \geq \dim(\operatorname{im} \varphi^2) \geq \dim(\operatorname{im} \varphi^3) \geq \cdots .$$

Since all these dimensions are positive integers limited by $\dim V$, they will have to stabilize and so $\ker \varphi^{m+1} = \ker \varphi^m$ and $\operatorname{im} \varphi^{n+1} = \operatorname{im} \varphi^n$ for sufficiently large integers m and n. Finally, it follows by induction that

$$\ker \varphi^{m+1} = \ker \varphi^m \implies (\forall k \geq m) \ker \varphi^{k+1} = \ker \varphi^k$$

and

$$\operatorname{im} \varphi^{n+1} = \operatorname{im} \varphi^n \implies (\forall k \geq n) \operatorname{im} \varphi^{k+1} = \operatorname{im} \varphi^k,$$

thus, we may assume that $m = n$, which proves the exercise.

To see that both claims may fail if V is infinite-dimensional, take $V = \mathbb{R}^{\oplus\mathbb{N}}$, which has infinite dimension. If $\varphi : V \to V$ is the left-shift homomorphism given by

$$(a_0, a_1, a_2, \dots) \mapsto (a_1, a_2, a_3, \dots),$$

it is clear that $\ker \varphi^n$ is the subspace of all sequences $(a_0, a_1, a_2, \dots) \in V$ where $a_i = 0$ for all $i \geq n$, following that $\ker \varphi^{n+1} \neq \ker \varphi^n$ for all $n \geq 1$. Similarly, if $\psi : V \to V$ is the right-shift homomorphism defined by

$$(a_0, a_1, a_2, \dots) \mapsto (0, a_0, a_1, \dots),$$

we have that $\operatorname{im} \varphi^n$ is the subspace of all sequences $(a_0, a_1, a_2, \dots) \in V$ such that $a_i = 0$ for all $i < n$, which implies that $\operatorname{im} \varphi^{n+1} \neq \operatorname{im} \varphi^n$ for all $n \geq 1$. ∎

EXERCISE 1.15

∎ SOLUTION A ∎

EXERCISE 1.16

∎ SOLUTION G ∎

EXERCISE 1.17

∎ SOLUTION T ∎

EXERCISE 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

- Let
$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_m = \langle 0 \rangle$$
be a composition series for G. Intersecting it with N gives a sequence of submodules of M:
$$N = M \cap N \supseteq M_1 \cap N \supseteq \cdots \supseteq \langle 0 \rangle \cap N = \langle 0 \rangle.$$
We claim that this becomes a composition series for N once repetitions are eliminated, which implies that N has finite length $n \leq m$. Indeed, this follows once we establish that
$$\frac{M_i \cap N}{M_{i+1} \cap N}$$

is either trivial (so that $M_{i+1} \cap N = M_i \cap N$, and the corresponding inclusion may be omitted) or isomorphic to M_i/M_{i+1} (hence simple). To see this, consider the homomorphism

$$M_i \cap N \hookrightarrow M_i \twoheadrightarrow \frac{M_i}{M_{i+1}} :$$

the kernel is clearly $M_{i+1} \cap N$; therefore (by the first isomorphism theorem) we have an injective homomorphism

$$\frac{M_i \cap N}{M_{i+1} \cap N} \hookrightarrow \frac{M_i}{M_{i+1}}$$

identifying $(M_i \cap N)/(M_{i+1} \cap N)$ with a submodule of M_i/M_{i+1}. Since M_i/M_{i+1} is simple, our claim follows.

The remaining part of the proof of Proposition IV.3.4 can also be easily adapted for R-modules.

- By the version of Proposition IV.3.4 for R-modules, we get that M/N has also finite length $n' \leq m$ and that $m = n + n'$. It follows that, if N is proper, then $n' > 0$ and so $n < m$. This fact will be important for us.

  Let

  $$N_0 \supseteq N_1 \supseteq N_2 \supseteq N_3 \supseteq \cdots$$

  be a descending chain of submodules of M. As suggested in the hint, we will prove by induction on m that this chain stabilizes. If $m = 0$, then M is the 0-module and so the chain stabilizes because all the submodules are equal to M. Now, suppose that $m > 0$ and that the d.c.c. for submodules holds for every R-module of finite length $n < m$. If all the submodules in the chain are equal to M, we are done, so we may suppose that there exists a submodule N_i properly contained in M. By our previous observation, N_i is of finite length $n < m$ and, by the inductive hypothesis, the d.c.c. for submodules holds in N_i. But the chain starting from N_i is a descending chain of submodules of N_i and, therefore, it stabilizes. We conclude that the d.c.c. for submodules holds in M.

- One implication is trivial since the 0-module clearly has finite length. Let's prove the converse. Suppose that F is not the 0-module. Since it is free, we may assume that

  $$F = R^{\oplus B}$$

  for some $B \neq \emptyset$. Let $x \in R$ be any nonzero element that is not a unit and let $I = (x)$. We have that

  $$(1) \supsetneq I \supsetneq I^2 \supsetneq I^3 \supsetneq \cdots .$$

  Indeed, if $I^n = I^{n+1}$ for some $n \geq 1$, there would be $r \in R$ such that

  $$x^n = rx^{n+1}$$

and, since R is an integral domain, it would follow that x is a unit, a contradiction. Now, we will show that

$$F \supsetneq IF \supsetneq I^2F \supsetneq I^3F \supsetneq \cdots .$$

Let $f \in F$ be the function defined by $f(b) = 1$ for all $b \in B$. If $I^nF = I^{n+1}F$ for some n, we would have that

$$r \in I^n \iff rf \in I^nF \iff rf \in I^{n+1}F \iff r \in I^{n+1}$$

and so $I^n = I^{n+1}$, contradicting what we proved earlier. Therefore, we have a descending chain of submodules of F that does not stabilize. By the second item, F is not of finite length. ∎

EXERCISE 1.19

■ SOLUTION A ∎

EXERCISE 1.20

■ SOLUTION G ∎

2 HOMOMORPHISMS OF FREE MODULES, I

EXERCISE 2.1

■ SOLUTION T ∎

EXERCISE 2.2 ▷ Prove that matrix multiplication is associative. [§2.1]

■ SOLUTION Let $A = (a_{ik})$ be a $m \times p$ matrix, $B = (b_{kl})$ be a $p \times q$ matrix and $C = (c_{lj})$ be a $q \times n$ matrix, all of them with entries in some ring R. Denote $(A \cdot B) \cdot C = (d_{ij})$ and $A \cdot (B \cdot C) = (e_{ij})$. It follows that

$$\begin{aligned} d_{ij} &= \sum_{l=1}^{q} \left(\sum_{k=1}^{p} a_{ik} b_{kl} \right) c_{lj} = \sum_{l=1}^{q} \sum_{k=1}^{p} a_{ik} b_{kl} c_{lj} \\ &= \sum_{k=1}^{p} \sum_{l=1}^{q} a_{ik} b_{kl} c_{lj} = \sum_{k=1}^{p} a_{ik} \left(\sum_{l=1}^{q} b_{kl} c_{lj} \right) = e_{ij} \end{aligned}$$

The swap of the summation signs represents a change in the order of the sum of the terms $a_{ik}b_{kl}c_{lj}$. Since addition is commutative, these sums must be equal.

for all indices i, j. Therefore, we have that $(A \cdot B) \cdot C = A \cdot (B \cdot C)$, proving that matrix multiplication is associative. ∎

EXERCISE 2.3

■ SOLUTION A ∎

EXERCISE 2.4

■ SOLUTION G ∎

EXERCISE 2.5

■ SOLUTION T ■

EXERCISE 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*.) [2.7, 2.9]

■ SOLUTION Let k be a field. The proof will be divided into two steps. We will firstly show that any matrix in $\mathcal{M}_{m,n}(k)$ can be brought into row echelon form by a sequence of elementary operations on rows. Secondly, we will deduce that matrices in row echelon form in $\mathcal{M}_{m,n}(k)$ can be turned into reduced row echelon form by a sequence of elementary operations on rows as well. Both steps will be proved by induction on the number $m + n$, which we will call as the *extent* of the matrix.

Let $M = (a_{ij}) \in \mathcal{M}_{m,n}(k)$ be a nonzero matrix. If $m = 1$, we just multiply the unique row of M by the inverse of the leftmost nonzero entry, turning it into row echelon form. Now, suppose that the extent of M is strictly greater than 2 and that every other matrix with extent less than the extent of M can be brought into row echelon form by a sequence of elementary operations on rows. As shown before, we may suppose that M is not a row n-vector. Moreover, we may also assume without loss of generality that the first column of M has a nonzero entry. After a row switch if necessary, we may assume that a_{11} is nonzero. Multiplying the first row by a_{11}^{-1}, we may consider that $a_{11} = 1$:

$$M = \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

Adding the first row multiplied by $-a_{21}$ to the second row clears the $(2,1)$ entry. After an analogous operation on all rows, we may reach the row echelon form (especially if $n = 1$), or we get a matrix of the form:

$$\left(\begin{array}{c|c} 1 & A \\ \hline 0 & M' \end{array}\right),$$

for some matrices A and M' of size $1 \times n$ and $(m-1) \times (n-1)$, respectively. The extent of M' is less than the extent of M, thus the inductive hypothesis implies that M' can be brought to row echelon form by a sequence of elementary operations on rows. Applying this sequence to the matrix above, the first column will not change and we will surely get to row echelon form, as desired.

For the second part, assume that M is already in row echelon form. If $m = 1$ or $n = 1$ then M is clearly in the reduced form. Now, suppose that the extent of M is strictly greater than 2 and that every other matrix in row echelon form with extent less than the extent of M can be turned into the reduced form by a sequence of elementary operations on rows. Suppose that M is neither a row n-vector nor a column m-vector. Ignoring the zero rows and the columns after the last pivot, we may also assume that $a_{mn} = 1$:

$$M = \begin{pmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 0 & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Similarly to the previous part, we may add the last row multiplied by $-a_{in}$ to the i-th row for all $0 \leq i < m$, obtaining a matrix of the form:

$$\left(\begin{array}{c|c} M' & 0 \\ \hline 0 & 1 \end{array}\right),$$

where M' is a $(m-1) \times (n-1)$ matrix. Note that M' is in row echelon form and so we can apply the inductive hypothesis since its extent is smaller than the extent of M. The resulting sequence of elementary operations on rows can be applied to M and it will not change the last column of the matrix above. Therefore, the final matrix will be in reduced row echelon form, as needed. ∎

The algorithm that arises from the proof is known as *Gaussian elimination*.

EXERCISE 2.7

∎ SOLUTION A ∎

EXERCISE 2.8

∎ SOLUTION G ∎

EXERCISE 2.9

■ SOLUTION T ■

EXERCISE 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 column. Prove that row-equivalent matrices have the same row space and isomorphic column spaces. [2.12, §3.3]

■ SOLUTION Let R be a ring and let $M, N \in \mathcal{M}_{m,n}(R)$ be two row-equivalent matrices, that is, $M = PN$ for some invertible matrix $P \in \mathcal{M}_m(R)$. Further, let $M_1, \ldots, M_m$ and $N_1, \ldots, N_m$ be the rows of M and N respectively. To prove that M and N have the same row space, it suffices to show that $M_1, \ldots, M_m$ are in the span of $N_1, \ldots, N_m$ and vice versa. Indeed, if $P = (p_{ij})$, it follows that

$$\begin{aligned} M &= P \cdot N \\ &= \begin{pmatrix} p_{11} & \cdots & p_{1m} \\ \vdots & \ddots & \vdots \\ p_{m1} & \cdots & p_{mm} \end{pmatrix} \cdot \begin{pmatrix} N_1 \\ \vdots \\ N_m \end{pmatrix} \\ &= \begin{pmatrix} p_{11}N_1 + p_{12}N_2 + \cdots p_{1m}N_m \\ \vdots \\ p_{m1}N_1 + p_{m2}N_2 + \cdots p_{mm}N_m \end{pmatrix}, \end{aligned}$$

that is, $M_1, \ldots, M_m$ really are in the span of $N_1, \ldots, N_m$. Since $N = P^{-1}M$, we similarly get the converse, as desired.

If R is a field, Proposition 3.7 implies that the row space and the column space of a matrix are isomorphic. In this particular case, the first half of the proof would already be sufficient.

For the second part, let $\mu, \nu : R^n \to R^m$ and $\rho : R^m \to R^m$ be the corresponding R-module homomorphisms to M, N and P, respectively, accordingly to Corollary 2.2. Since $\mu(\mathbf{e}_i)$ is the i-th column of M and $\nu(\mathbf{e}_i)$ s the i-th column of N, for all i, it follows that the column spaces of M and N are, respectively, the image of μ and the image of ν. Moreover, $M = PN$ implies that $\mu = \rho \circ \nu$ by Lemma 2.3. Thus, we may take $\rho' : \mathrm{im}(\nu) \to \mathrm{im}(\mu)$ as the restriction of ρ, which is also a homomorphism of R-modules. It is clear that ρ' is surjective, and, since ρ is an isomorphism (Exercise 2.3), ρ' is also injective. Hence, we conclude that ρ' is an isomorphism and so M and N have isomorphic column spaces. ■

EXERCISE 2.11

■ SOLUTION A ■

EXERCISE 2.12

■ SOLUTION G ■

EXERCISE 2.13

■ SOLUTION T ■

EXERCISE 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.) [VIII.4.8]

■ SOLUTION As in the previous exercise, we need to list all the possible reduced echelon forms. In this case, since we are dealing with $\mathrm{Gr}_k(2,4)$, we will consider reduced row echelon matrices of size 4×4 with 2 nonzero rows, which naturally correspond to those of size 2×4 with no zero rows.

The reduced echelon forms may be divided into subsets accordingly to the position of their pivots. We have six of them:

$$\begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix},$$

$$\begin{pmatrix} 1 & a & 0 & b \\ 0 & 0 & 1 & c \end{pmatrix},$$

$$\begin{pmatrix} 1 & a & b & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & 0 & a \\ 0 & 0 & 1 & b \end{pmatrix},$$

$$\begin{pmatrix} 0 & 1 & a & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

and

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where $a, b, c, d \in k$. These subsets are in a natural bijection with k^4, k^3, k^2, k^2, k^1 and k^0, respectively. Since they partition $\mathrm{Gr}_k(2,4)$, we conclude that $\mathrm{Gr}_k(2,4)$ is the union of 6 Schubert cells: $k^4 \cup k^3 \cup k^2 \cup k^2 \cup k^1 \cup k^0$. ■

EXERCISE 2.15

■ SOLUTION A ■

EXERCISE 2.16

■ SOLUTION G ■

EXERCISE 2.17

■ SOLUTION T ■

EXERCISE 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 Let P be the matrix above and let A and C be the standard bases for $\mathbb{Z}^3$ and $\mathbb{Z}^2$, respectively. By the discussion preceding Proposition 2.5, we need to find bases B and D for $\mathbb{Z}^3$ and $\mathbb{Z}^2$ such that

$$Q = (M_D^C)^{-1} \cdot P \cdot N_B^A$$

is a matrix in the form obtained in Proposition 2.11, where N_B^A and M_D^C are the corresponding matrices of change of basis. To do so, we will firstly find N_B^A and M_D^C by executing the algorithm in §2.4.

We are taking these matrices instead of N_A^B and M_C^D to facilitate the recovering of B and D from the corresponding matrices of change of basis, as we will see soon.

We will first clear the $(2,1)$ entry (and other entries will vanish too as we will see). Add to the second row the (-3)-multiple of the first, producing the matrix

$$\begin{pmatrix} -6 & 12 & 18 \\ 3 & 0 & 0 \end{pmatrix}.$$

Swapping the rows and adding to the second one the 2-multiple of the first, we get the matrix

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 12 & 18 \end{pmatrix}.$$

Now, we will clear the $(2,3)$ entry. Adding to the third column the opposite of the second results in the matrix

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 12 & 6 \end{pmatrix}.$$

Finally, swapping the last two columns and adding to the third one the (-2)-multiple of the second, we end with the matrix

$$\begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 0 \end{pmatrix},$$

which is already in the form desired.

The matrix N_B^A is obtained by applying the elementary operations on *columns* that we did above to the 3×3 identity matrix. Thus,

$$N_B^A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 3 \\ 0 & 1 & -2 \end{pmatrix}.$$

Similarly, $(M_D^C)^{-1}$ is obtained by applying the elementary operations on *rows* that we did above to the 2×2 identity matrix. This is equivalent to the product of elementary matrices

$$(M_D^C)^{-1} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}$$

by Exercise 2.5. Hence,

$$\begin{aligned} M_D^C &= \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^{-1} \\ &= \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} -2 & 1 \\ -5 & 3 \end{pmatrix}. \end{aligned}$$

Recall that the inverse of an elementary matrix M is the elementary matrix that undoes the operation done by M.

Finally, the desired (ordered) bases are given by the columns of N_B^A and M_D^C, so

$$B = \{(1,0,0), (0,-1,1), (0,3,-2)\}$$

and

$$D = \{(-2,-5), (1,3)\}$$

are bases of $\mathbb{Z}^3$ and $\mathbb{Z}^2$ with respect to which α is given by a matrix of the form obtained in Proposition 2.11. ∎

Exercise 2.19

∎ Solution A ∎

3 HOMOMORPHISMS OF FREE MODULES, II

Exercise 3.1

∎ Solution G ∎

Exercise 3.2

∎ Solution T ∎

Exercise 3.3 Redo Exercise II.8.8.

■ Solution See the solution of Exercise II.8.8 given in Chapter II. ■

Exercise 3.4

■ Solution A ■

Exercise 3.5

■ Solution G ■

Exercise 3.6

■ Solution T ■

Exercise 3.7 ¬ Let R be a commutative ring, M a finitely generated R-module, and let J be an ideal of R. Assume that $JM = M$. 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.) [3.8, VIII.1.18]

■ Solution Let $m_1, \ldots, m_r$ be generators for M. Since $m_i \in M = JM$, there are $b_{i1}, \ldots, b_{ir} \in J$ such that

$$m_i = b_{i1}m_1 + \cdots + b_{ir}m_r$$

for all $1 \leq i \leq r$. Let $B = (b_{ij})$ be the $r \times r$ matrix formed by these elements of J. Note that

$$B \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = \begin{pmatrix} b_{11}m_1 + b_{12}m_2 + \cdots b_{ir}m_r \\ \vdots \\ b_{r1}m_1 + b_{r2}m_2 + \cdots b_{rr}m_r \end{pmatrix} = \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix}$$

and so

$$(I_r - B) \cdot \begin{pmatrix} m_1 \\ \vdots \\ m_r \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

This congruence is valid since the determinant may be expressed as a sum of products of elements of the matrix.

By Exercise 3.6, $\det(I_r - B)M = 0$. Finally, we have that

$$\det(I_r - B) \equiv \det(I_r) = 1 \mod J$$

and so $\det(I_r - B) - 1 \in J$, that is, there exists $b \in J$ such that $\det(I_r - B) = 1 + b$. We conclude that $(1+b)M = 0$. ■

EXERCISE 3.8

■ SOLUTION A ■

EXERCISE 3.9

■ SOLUTION G ■

EXERCISE 3.10

■ SOLUTION T ■

EXERCISE 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 Let M be a matrix over a field. By Exercise 2.6, M can be brought into a matrix N in reduced echelon form by Gaussian elimination. Thus, Exercise 2.8 implies that M and N are row-equivalent and so they have the same row space by Exercise 2.10. Finally, it follows from Exercise 2.7 that the nonzero rows of N form a basis for the row space of M. To find a basis for the column space, apply the same procedure to the transpose of M. ■

EXERCISE 3.12

■ SOLUTION A ■

EXERCISE 3.13

■ SOLUTION G ■

EXERCISE 3.14

■ SOLUTION T ■

EXERCISE 3.15 ▷ Prove Proposition 3.13 for the case $N = 1$. [§3.4]

■ SOLUTION Consider the following complex of finite-dimensional vector spaces and linear maps:

$$V_\bullet : \ 0 \longrightarrow V_1 \xrightarrow{\alpha_1} V_0 \longrightarrow 0 .$$

If $\chi_H(V_\bullet)$ denotes

$$\chi_H(V_\bullet) = \dim(H_0(V_\bullet)) - \dim(H_1(V_\bullet)),$$

we need to prove that $\chi(V_\bullet) = \chi_H(V_\bullet)$. Since

$$H_0(V_\bullet) = \frac{V_0}{\operatorname{im} \alpha_1} \text{ and } H_1(V_\bullet) = \ker \alpha_1,$$

it follows by Proposition 3.11 (cf. Claim 3.10) that

$$\begin{aligned}\chi_H(V_\bullet) &= \dim(H_0(V_\bullet)) - \dim(H_1(V_\bullet)) \\ &= (\dim(V_0) - \dim(\operatorname{im}\alpha_1)) - \dim(\ker\alpha_1) \\ &= \dim(V_0) - (\dim(\operatorname{im}\alpha_1) + \dim(\ker\alpha_1)) \\ &= \dim(V_0) - \dim(V_1) \\ &= \chi(V_\bullet),\end{aligned}$$

as desired. ∎

EXERCISE 3.16

∎ SOLUTION A ∎

EXERCISE 3.17

∎ SOLUTION G ∎

EXERCISE 3.18

∎ SOLUTION T ∎

EXERCISE 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 $(\mathbb{Q}^*, \cdot)$. [3.20]

∎ SOLUTION Let X be the set of all isomorphism classes in Ab^f. Since all groups of a isomorphism class have the same order, we can define the function $f : X \to \mathbb{Q}^*$ that sends $[G]$ to $|G|$ for all $G \in \mathrm{Obj}(\mathsf{Ab}^f)$. By the universal property of free abelian groups, there exists a unique group homomorphism $\varphi : F^{ab}(X) \to (\mathbb{Q}^*, \cdot)$ such that the diagram

$$\begin{array}{ccc} F^{ab}(X) & \xrightarrow{\varphi} & \mathbb{Q}^* \\ {\scriptstyle j}\uparrow & \nearrow_{f} & \\ X & & \end{array}$$

commutes, where j denotes the natural inclusion of X in $F^{ab}(X)$. Now, let E be the subgroup of $F^{ab}(X)$ generated by the elements

$$[H] - [G] - [K]$$

for all short exact sequences

$$1 \longrightarrow G \longrightarrow H \longrightarrow K \longrightarrow 1$$

in Ab^f. In this case, we have that

$$\begin{aligned}\frac{H}{G} \cong K &\implies |H| = |G| \cdot |K| \\ &\implies |H| \cdot |G|^{-1} \cdot |K|^{-1} = 1 \\ &\implies \varphi([H] - [G] - [K]) = 1 \\ &\implies [H] - [G] - [K] \in \ker\varphi\end{aligned}$$

and so $E \subseteq \ker \varphi$. Recalling that

$$K(\mathsf{Ab}^f) = \frac{F^{ab}(X)}{E},$$

Theorem II.7.12 implies that there exists a unique group homomorphism $\tilde{\varphi} : K(\mathsf{Ab}^f) \to (\mathbb{Q}^*, \cdot)$ such that $\tilde{\varphi} \circ \pi = \varphi$, where $\pi : F^{ab}(X) \to K(\mathsf{Ab}^f)$ is the canonical projection. Note that $\tilde{\varphi}$ naturally extends f in the sense that $\tilde{\varphi}([G]) = |G|$ for all finite abelian group G. ∎

EXERCISE 3.20

∎ SOLUTION A ∎

4 PRESENTATIONS AND RESOLUTIONS

EXERCISE 4.1

∎ SOLUTION G ∎

EXERCISE 4.2

∎ SOLUTION T ∎

EXERCISE 4.3 ▷ Prove that an integral domain R is a PID if and only if every submodule of R itself is free. [§4.1, 5.13]

∎ SOLUTION ($\Longrightarrow$) Suppose that R is a PID and let's prove that every ideal of I is free as an R-module. Since I is principal, it is generated by some $a \in I$. If $a = 0$, I is the 0-module and so it is free. If $a \neq 0$, $\{a\}$ is linear independent since R is an integral domain, so $\{a\}$ is a basis for I and I is free.

($\Longleftarrow$) Suppose that every submodule of R is free and let I be an ideal (that is, a submodule) of R. Since R is an integral domain and has rank 1, it follows from Proposition 1.9 that I has rank at most 1, which implies that I is generated by one of its elements. Therefore, I is principal and we conclude that R is a PID. ∎

EXERCISE 4.4

∎ SOLUTION A ∎

EXERCISE 4.5

∎ SOLUTION G ∎

EXERCISE 4.6

∎ SOLUTION T ∎

EXERCISE 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 $M'' \supseteq M'$ such that $M''/M' \cong R/\mathfrak{p}_2$ for some prime $\mathfrak{p}_2$. Why must this process stop after finitely many steps?) [4.8]

■ SOLUTION Since R is Noetherian, Exercise 4.6 implies that $\mathrm{Ass}_R(M)$ is nonempty and so there exists a prime ideal $\mathfrak{p}_1$ of R which is the annihilator of some element of M. By Exercise 4.5, M contains an isomorphic copy M' of $R/\mathfrak{p}_1$. Now, it follows from Proposition III.6.7 that M/M' is Noetherian and, by the same reasoning as before, M/M' contains an isomorphic copy of $R/\mathfrak{p}_2$ for some prime ideal $\mathfrak{p}_2$ of R. This copy corresponds to a submodule M'' of M containing M' such that $M''/M' \cong R/\mathfrak{p}_2$. Note that $M' \subsetneq M''$ because $R/\mathfrak{p}_2$ is not the 0-module. Continuing this process, we get an ascending chain of submodules of M:

$$\langle 0 \rangle \subsetneq M' \subsetneq M'' \subsetneq \cdots .$$

Since R is Noetherian and M is finitely generated, we have from Corollary III.6.8 that M is Noetherian and so the chain above stabilizes. Finally, by construction, the chain can only stabilize when we reach M. Therefore, after a renaming of the submodules, we get 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. ■

EXERCISE 4.8

■ SOLUTION A ■

EXERCISE 4.9

■ SOLUTION G ■

EXERCISE 4.10

■ SOLUTION T ■

EXERCISE 4.11 Review the notion of presentation *of a group*, (§II.8.2), and relate it to the notion of presentation introduced in §4.2.

■ SOLUTION Recall from §II.8.2 that a presentation of a group G is an explicit group homomorphism $\rho : F(A) \to G$ for some set A which is

surjective and has a specified kernel R, the subgroup of 'relations'. If G is finitely presented, we can rewrite this definition so that it resembles the notion of presentation introduced in §4.2. If A is finite, Exercise II.9.16 implies that R is free, that is, there exists a set B (not necessarily finite) such that $R \cong F(B)$. If $\varphi : F(B) \to F(A)$ denotes the inclusion homomorphism (after a natural identification), we have the following exact sequence of groups:

$$F(B) \xrightarrow{\varphi} F(A) \xrightarrow{\rho} G \longrightarrow 1,$$

which is similar to Definition 4.7, but for groups. Conversely, note that an exact sequence as the one above naturally determines a presentation of G as defined in §II.8.2. ∎

The *Nielsen-Schreier theorem* states the every subgroup of a free group is free (even for free groups on infinite sets). In this sense, we need not suppose that A is finite.

EXERCISE 4.12

∎ SOLUTION A ∎

EXERCISE 4.13

∎ SOLUTION G ∎

EXERCISE 4.14

∎ SOLUTION T ∎

EXERCISE 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. [VIII.4.21]

∎ SOLUTION Since R is Noetherian (by Hilbert's basis theorem), we can iterate the argument proving Lemma 4.8 to find a free resolution of $\mathbb{Z}$ over R. Firstly, since $\mathbb{Z}$ is generated by 1, there exists a surjective R-module homomorphism $\varphi_1 : R \to \mathbb{Z}$ such that $f(1) = 1$. Note that $\ker \varphi_1$ consists of all polynomials in R with constant term equal to 0 and so $\ker \varphi_1$ is generated by x and y. This gives us an R-module homomorphism $\varphi_2 : R^2 \to R$ which sends $(1, 0)$ to x and $(0, 1)$ to y. Let's compute $\ker \varphi_2$. If $(p_1, p_2) \in \ker \varphi_2$, we have that

$$p_1 x + p_2 y = 0 \implies p_1 x = -p_2 y.$$

Since y is prime in R (note that $R/(y)$ is isomorphic to $\mathbb{Z}[x]$, which is an integral domain) and does not divide x, it follows that y divides p_1, that is, there exists $p \in R$ such that $p_1 = py$. Thus, we have that $p_2 = -px$ and so

$$(p_1, p_2) = p(y, -x)$$

and $\ker \varphi_2$ is generated by $(-y, x)$. Finally, we have an injective R-module homomorphism $\varphi_3 : R \to R^2$ sending 1 to $(y, -x)$. Therefore, we have the following exact sequence:

$$0 \longrightarrow R \xrightarrow{\varphi_3} R^2 \xrightarrow{\varphi_2} R \xrightarrow{\varphi_1} \mathbb{Z} \longrightarrow 0,$$

which is a free resolution of $\mathbb{Z}$ over R. ∎

EXERCISE 4.16

■ SOLUTION A ■

EXERCISE 4.17

■ SOLUTION G ■

5 CLASSIFICATION OF FINITELY GENERATED MODULES OVER PIDS

EXERCISE 5.1

■ SOLUTION T ■

EXERCISE 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 Note that $\operatorname{rk} M = 0$ if and only if $\{m\}$ is linearly dependent for all $m \in M$, that is, if and only if every element of M is a torsion element. It follows that $\operatorname{rk} M = 0$ if and only if M is torsion. ■

EXERCISE 5.3

■ SOLUTION A ■

EXERCISE 5.4

■ SOLUTION G ■

EXERCISE 5.5

■ SOLUTION T ■

EXERCISE 5.6 ▷ Let R be an integral domain, and let $M = \langle m_1, \dots, m_r \rangle$ be a finitely generated module. Prove that $\operatorname{rk} M \leq r$. (Use Exercise 3.12.) [§5.3]

■ SOLUTION Let $v_1, v_2, \dots, v_n \in M$ be any finite collection of elements of M and suppose that $n > r$. We will prove that $\{v_1, \dots, v_n\}$ is linearly dependent (as an indexed set, since we may have repeated elements), which implies that $\operatorname{rk} M \leq r$. Since $M = \langle m_1, \dots, m_r \rangle$, there are $a_{ij} \in R$, with $1 \leq i \leq r$ and $1 \leq j \leq n$ such that

$$v_j = \sum_{i=1}^{r} a_{ij} m_i$$

for all $1 \leq j \leq n$. Let $A \in \mathcal{M}_{r,n}(R)$ be the matrix $A = (a_{ij})$. By Exercise 3.12, the columns of A are linearly dependent and so there are $r_1, \dots, r_n \in R$ not all zero such that

$$\sum_{j=1}^{n} r_j a_{ij} = 0$$

for all $1 \leq i \leq r$. Therefore,

$$\sum_{j=1}^{n} r_j v_j = \sum_{j=1}^{n} \sum_{i=1}^{r} r_j a_{ij} m_i = \sum_{i=1}^{r} \sum_{j=1}^{n} r_j a_{ij} m_i$$
$$= \sum_{i=1}^{r} \left(\sum_{j=1}^{n} r_j a_{ij} \right) m_i = \sum_{i=1}^{r} 0 \cdot m_i = 0$$

and $\{v_1, \ldots, v_n\}$ is linearly dependent, as desired. ∎

EXERCISE 5.7

∎ SOLUTION A ∎

EXERCISE 5.8

∎ SOLUTION G ∎

EXERCISE 5.9

∎ SOLUTION T ∎

EXERCISE 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 $T \cong \operatorname{Tor}_R(M)$. [§5.3]

∎ SOLUTION For simplicity, we will assume that $M = R^r \oplus T$ due to the given isomorphism. Firstly, let's prove that $T \cong \operatorname{Tor}_R(M)$. If $(s, t) \in \operatorname{Tor}_R(M)$, where $s \in R^r$ and $t \in T$, then $s = 0$ since $s \in \operatorname{Tor}_R R^r$ and free modules over integral domains are torsion-free (Lemma 4.2). Thus,

$$\operatorname{Tor}_R(M) = \{(0, t) \in M \mid t \in T\},$$

which is clearly isomorphic to T.

For the other part, note that $r \leq \operatorname{rk} M$ since any basis for R^r naturally corresponds to a linearly independent subset of M. Now, let $m_1, \ldots, m_n \in M$ be any finite collection of elements of M and suppose that $n > r$. We will show that the indexed set $\{m_1, \ldots, m_n\}$ is linearly dependent. Let $s_i \in R^r$ and $t_i \in T$ be such that

If M is finitely generated, Exercise 5.7 readily implies that $r = \operatorname{rk} M$ because $M/\operatorname{Tor}_R(M)$ is isomorphic to R^r.

$$m_i = (s_i, t_i)$$

for all $1 \leq i \leq n$. Since R^r is of rank $r < n$, the indexed set $\{s_1, \ldots, s_n\}$ is linearly dependent and so there are $a_1, \ldots, a_n \in R$ not all zero such that

$$a_1 s_1 + \cdots + a_n s_n = 0.$$

On the other hand, since T is torsion, there are $r_1, \ldots, r_n \in R$ such that

$$r_i t_i = 0 \text{ and } r_i \neq 0$$

for all $1 \leq i \leq n$. The product $P = r_1 \cdots r_n$ is nonzero because R is an integral domain, and note that $Pt_i = 0$ for all $1 \leq i \leq n$. Finally, at least one of the elements $Pa_1, \ldots, Pa_n$ of R is nonzero and we have that

$$\begin{aligned} Pa_1m_1 + \cdots + Pa_nm_n &= Pa_1(s_1, t_1) + \cdots + Pa_n(s_n, t_n) \\ &= (P(a_1s_1 + \cdots + a_ns_n), a_1Pt_1 + \cdots + a_nPt_n) \\ &= 0, \end{aligned}$$

which proves that $\{m_1, \ldots, m_n\}$ is linearly dependent, as desired. Therefore, we get the other inequality $r \geq \operatorname{rk} M$ and we conclude that $r = \operatorname{rk} M$. ∎

EXERCISE 5.11

∎ SOLUTION A ∎

EXERCISE 5.12

∎ SOLUTION G ∎

EXERCISE 5.13

∎ SOLUTION T ∎

EXERCISE 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.

More generally, we could have taken R as any Noetherian integral domain which is not a PID, and I as any nonprincipal ideal of R.

∎ SOLUTION Let $R = \mathbb{Z}[x]$ and let $I = (2, x)$. It is clear that I is finitely generated as a module over R. Now, suppose that I is isomorphic to a direct sum of cyclic modules. Our first observation is that only finitely many of these cyclic modules is nonzero because, otherwise, I would not be finitely generated. Thus, we may suppose that

$$I \cong M_1 \oplus M_2 \oplus \cdots \oplus M_n$$

where M_i is a cyclic R-module for all i. By Definition 4.4 (see Exercise III.6.16), there are ideals $I_1, \ldots, I_n$ of R such that

$$M_i \cong R/I_i$$

for all indices i. If the ideal I_i is nonzero, it follows that M_i is not torsion-free and, consequently, I is not torsion-free, which contradicts Lemma 4.2 since R is clearly torsion-free and I is a submodule of R. Thus, $I_1 = \cdots = I_n = 0$ and so

$$I \cong R^n$$

and I is free. However, Example 4.3 shows that I is not free, a contradiction. Therefore, we conclude that I is not isomorphic to a direct sum of cyclic modules. ∎

EXERCISE 5.15

■ SOLUTION A ■

EXERCISE 5.16

■ SOLUTION G ■

EXERCISE 5.17

■ SOLUTION T ■

6 LINEAR TRANSFORMATIONS OF A FREE MODULE

EXERCISE 6.1 Let k be an infinite field, and let n be any positive integer.

- Prove that there are finitely many *equivalence* classes of matrices in $\mathcal{M}_n(k)$.
- Prove that there are infinitely many *similarity* classes of matrices in $\mathcal{M}_n(k)$.

■ SOLUTION

- By Proposition 2.10, every matrix in $\mathcal{M}_n(k)$ is equivalent to a matrix of the form
$$\left(\begin{array}{c|c} I_r & 0 \\ \hline 0 & 0 \end{array}\right),$$
for some $1 \leq r \leq n$. Therefore, there are exactly n equivalence classes of matrices in $\mathcal{M}_n(k)$.
- As shown in §6.2, similar matrices have the same trace. Thus, since k is infinite, it suffices to show that any $c \in k$ is the trace of some matrix in $\mathcal{M}_n(k)$. Indeed, it is straightfoward that the trace of the matrix
$$\begin{pmatrix} c & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$
is c, as desired. ■

Remark. There is a more general statement than the one given in the second item: any monic polynomial $f(t)$ in $k[t]$ is the characteristic polynomial of some linear transformation in $\mathrm{End}_k(k^n)$, where n is the degree of $f(t)$. Indeed, if
$$f(t) = t^n + r_{n-1}t^{n-1} + \cdots + r_0,$$

then Exercise 7.2 implies that $f(t)$ is the characteristic polynomial of the linear transformation given by the matrix

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -r_0 \\ 1 & 0 & 0 & \cdots & 0 & -r_1 \\ 0 & 1 & 0 & \cdots & 0 & -r_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -r_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -r_{n-1} \end{pmatrix}.$$

This is called the *companion matrix* of the polynomial $f(t)$. Companion matrices will be further studied in the next section.

EXERCISE 6.2

■ SOLUTION A ■

EXERCISE 6.3

■ SOLUTION G ■

EXERCISE 6.4

■ SOLUTION T ■

EXERCISE 6.5 ▷ Let k be a field, and view $k[t]$ as a vector space over k in the evident way. Give an example of a k-linear transformation $k[t] \to k[t]$ which is injective but not surjective; give an example of a linear transformation which is surjective but not injective. [§6.2, §VII.4.1]

■ SOLUTION Define the 'shift' functions

$$\begin{aligned} \varphi_l : k[t] &\to k[t] \\ \sum_{i\geq 0} a_i x^i &\mapsto \sum_{i\geq 0} a_{i+1} x^i \end{aligned}$$

These linear transformations are analogous to the ones defined in Exercise 1.14 since $k[t] \cong k^{\oplus \mathbb{N}}$ as k-vector spaces.

and

$$\begin{aligned} \varphi_l : k[t] &\to k[t] \\ \sum_{i\geq 0} a_i x^i &\mapsto \sum_{i\geq 1} a_{i-1} x^i. \end{aligned}$$

It is straightfoward that φ_l and φ_r are k-linear transformations. Furthermore, since $\varphi_l \circ \varphi_r = \mathrm{id}_{k[t]}$, we have that φ_l is surjective and φ_r is injective. However, φ_l is not injective since $\varphi_l(c) = 0$ for all $c \in k$, and φ_r is not surjective because $\operatorname{im} \varphi_r$ does not contain any constant polynomial. ■

EXERCISE 6.6

■ SOLUTION A ■

EXERCISE 6.7

■ SOLUTION G ■

EXERCISE 6.8

■ SOLUTION T ■

EXERCISE 6.9 ▷ Prove the Cayley-Hamilton theorem, as follows. Recall that every square matrix M has an *adjoint* matrix, which we will denote $\text{adj}(M)$, and that we proved (Corollary 3.5) that $\text{adj}(M) \cdot M = \det(M) \cdot I$. Applying this to $M = tI - A$ (with A a matrix realization of $\alpha \in \text{End}_R(F)$) gives

$$\text{adj}(tI - A) \cdot (tI - A) = P_\alpha(t) \cdot I. \tag{*}$$

Prove that there exist matrices $B_k \in \mathcal{M}_n(R)$ such that $\text{adj}(tI - A) = \sum_{k=0}^{n-1} B_k t^k$; then use (*) to obtain $P_\alpha(A) = 0$, proving the Cayley-Hamilton theorem. [§6.2]

■ SOLUTION By the definition of the adjoint matrix, each entry of $\text{adj}(tI - A)$ is the determinant of a $(n-1) \times (n-1)$ matrix and so is a polynomial in t of degree at most $n-1$. Thus, we can break $\text{adj}(tI - A)$ into $n-1$ matrices, each one containing only monomials of the same degree on t, and we then factor the powers of t out, obtaining that

$$\text{adj}(tI - A) = \sum_{k=0}^{n-1} B_k t^k$$

for some matrices $B_k \in \mathcal{M}_n(R)$. Now, let

$$P_\alpha(t) = c_n x^n + c_{n-1} x^{n-1} + \cdots c_1 x + c_0$$

be the characteristic polynomial of α. From (*), we have that

$$\left(\sum_{k=0}^{n-1} B_k t^k \right) \cdot (tI - A) = \sum_{k=0}^{n} (c_k I) t^k$$

and so

$$B_{n-1} t^n + \sum_{k=1}^{n-1} (B_{k-1} - B_k A) t^k - B_0 A = \sum_{k=0}^{n} (c_k I) t^k.$$

Although we know that $c_n = 1$, we will denote it this way to facilitate writing the following sums.

Comparing the entries of the matrices above and the coefficients of the corresponding polynomials, it follows that

$$\begin{aligned} B_{n-1} &= c_n I \\ B_{n-2} - B_{n-1}A &= c_{n-1} I \\ B_{n-3} - B_{n-2}A &= c_{n-2} I \\ &\vdots \\ B_0 - B_1 A &= c_1 I \\ -B_0 A &= c_0 I. \end{aligned}$$

Finally, multiplying the first equation by A^n on the right, the second by A^{n-1}, the third by A^{n-2}, and so on, and adding them, we conclude that

$$0 = c_n A^n + c_{n-1} A^{n-1} + \cdots + c_1 A + c_0 I,$$

that is,

$$P_\alpha(A) = 0,$$

proving the Cayley-Hamilton theorem. ∎

EXERCISE 6.10

∎ SOLUTION A ∎

EXERCISE 6.11

∎ SOLUTION G ∎

EXERCISE 6.12

∎ SOLUTION T ∎

EXERCISE 6.13 Let A be a square matrix with integer entries. Prove that if λ is a *rational* eigenvalue of A, then in fact $\lambda \in \mathbb{Z}$. (Hint: Proposition V.5.5.)

∎ SOLUTION By Lemma 6.14, λ is a rational root of the characteristic polynomial of A, which is monic and has integer coefficients. By Proposition V.5.5, it follows that $\lambda \in \mathbb{Z}$. ∎

EXERCISE 6.14

∎ SOLUTION A ∎

EXERCISE 6.15

∎ SOLUTION G ∎

EXERCISE 6.16

∎ SOLUTION T ∎

EXERCISE 6.17 ¬ We say that two vectors $\mathbf{v}, \mathbf{w}$ of $\mathbb{R}^n$ or $\mathbb{C}^n$ are *orthogonal* if $(\mathbf{v}, \mathbf{w}) = 0$. The *orthogonal complement* $\mathbf{v}^\perp$ of $\mathbf{v}$ is the set of vectors $\mathbf{w}$ that are orthogonal to $\mathbf{v}$. Prove that if $\mathbf{v} \neq 0$ in $V = \mathbb{R}^n$ or $\mathbb{C}^n$, then $\mathbf{v}^\perp$ is a subspace of V of dimension $n - 1$. [7.16, VIII.5.15]

■ SOLUTION We will suppose that $V = \mathbb{R}^n$ (the other case is analogous). Let $\varphi : V \to \mathbb{R}$ be the function defined by

$$\varphi(\mathbf{w}) = (\mathbf{v}, \mathbf{w})$$

for all $\mathbf{w} \in V$. By the properties of the standard inner product on V, it is easy to check that φ is a homomorphism of $\mathbb{R}$-vector spaces. Note that $\mathbf{v}^\perp = \ker \varphi$ and so the orthogonal complement of $\mathbf{v}$ is a subspace of V. Moreover, since $\mathbf{v} \neq 0$, $\varphi(\mathbf{v})$ is not zero, which implies that φ is surjective because $\dim \mathbb{R} = 1$. We conclude from Claim 3.10 that

$$\dim \mathbf{v}^\perp = \dim(\ker \varphi) = \dim V - \dim(\operatorname{im} \varphi) = n - 1,$$

as desired. ■

Remark. More generally, we can define the notion of orthogonal complement for any subset S of $V = \mathbb{R}^n$ or $\mathbb{C}^n$ by setting

$$S^\perp = \{\mathbf{v} \in V \mid (\forall \mathbf{s} \in S)(\mathbf{s}, \mathbf{v}) = 0\}.$$

We have that $S^\perp$ is always a subspace of V. Furthermore, if $U \subseteq V$ is a subspace, then

$$V \cong U \oplus U^\perp$$

and so $\dim U^\perp = n - \dim U$.

EXERCISE 6.18

■ SOLUTION A ■

EXERCISE 6.19

■ SOLUTION G ■

EXERCISE 6.20

■ SOLUTION T ■

EXERCISE 6.21 ¬ A matrix $M \in \mathcal{M}_n(\mathbb{R})$ is *symmetric* if $M^t = M$. Prove that M is symmetric if and only if $(\forall \mathbf{v}, \mathbf{w} \in \mathbb{R}^n)$, $(M\mathbf{v}, \mathbf{w}) = (\mathbf{v}, M\mathbf{w})$.

A matrix $M \in \mathcal{M}_n(\mathbb{C})$ is *hermitian* if $M^\dagger = M$. Prove that M is hermitian if and only if $(\forall \mathbf{v}, \mathbf{w} \in \mathbb{C}^n)$, $(M\mathbf{v}, \mathbf{w}) = (\mathbf{v}, M\mathbf{w})$.

In both cases, one may say that M is *self-adjoint*; this means that shuttling it from one side of the product to the other does not change the result of the operation.

A hermitian matrix with real entries is symmetric. It is in fact useful to think of real symmetric matrices as particular cases of hermitian matrices. [6.22]

■ SOLUTION Let $M = (m_{ij}) \in \mathcal{M}_n(\mathbb{R})$. If M is symmetric, it follows that

Recall that $(AB)^t = B^t A^t$ for all $A \in \mathcal{M}_{m,p}(R)$ and $B \in \mathcal{M}_{p,n}(R)$ and any ring R.

$$(M\mathbf{v}, \mathbf{w}) = (M \cdot \mathbf{v})^t \cdot \mathbf{w} = \mathbf{v}^t \cdot M^t \cdot \mathbf{w} = \mathbf{v}^t \cdot M \cdot \mathbf{w} = (\mathbf{v}, M\mathbf{w})$$

for all $\mathbf{v}, \mathbf{w} \in \mathbb{R}^n$. Conversely, if this last equality holds, replacing $\mathbf{v} = \mathbf{e_i}$ and $\mathbf{w} = \mathbf{e_j}$ gives

$$m_{ij} = m_{ji}$$

for all $1 \leq i, j \leq n$, that is, $M^t = M$ and M is symmetric. Finally, since $(AB)^\dagger = B^\dagger A^\dagger$ for all $A \in \mathcal{M}_{m,p}(\mathbb{C})$ and $B \in \mathcal{M}_{p,n}(\mathbb{C})$, a similar argument proves the analogous result for hermitian matrices. ■

EXERCISE 6.22

■ SOLUTION A ■

7 CANONICAL FORMS

EXERCISE 7.1

■ SOLUTION G ■

EXERCISE 7.2

■ SOLUTION T ■

EXERCISE 7.3 ▷ Prove that two linear transformations of a vector space of dimension ≤ 3 are similar if and only if they have the same characteristic and minimal polynomials. Is this true in dimension 4? [§6.2]

■ SOLUTION Independently of the dimension of the vector space, similar linear transformations have the same characteristic and minimal polynomials. This follows, for example, from Corollary 7.7 and Proposition 7.9. Now, let α, β be two linear transformations of a vector space V of dimension ≤ 3 and suppose that they have the same characteristic and minimal polynomials. We will show that α and β are similar by comparing their rational canonical forms.

Let $f_1(t) \mid \cdots \mid f_m(t)$ and $g_1(t) \mid \cdots \mid g_n(t)$ be the invariant factors of α and β, respectively. Note that $f_m(t) = g_n(t) = p(t)$ by Proposition 7.9 because α and β have the same minimal polynomials. Since $m, n \leq \dim V$, if $\dim V = 1$ or $\dim V = 2$, the same Proposition will imply

that the other invariant factors are also the same since α and β have the same characteristic polynomial too. Now, assume that $\dim V = 3$. If $\deg p(t) = 3$, then we must have $m = n = 1$ and, thus, the invariant factors coincide. If $\deg p(t) = 2$, then $m = n = 2$ and there is only one more invariant factor for α and β to compare; they will be the same again by Proposition 7.9 and because the linear transformations have the same characteristic polynomial. Finally, if $\deg p(t) = 1$, the condition of divisibility of the invariant factors and the fact that they are monic will imply that they are all equal to $p(t)$, as desired.

In any case, α and β have the same invariant factors and, therefore, the same rational canonical form. We conclude that they are similar.

Notice that this result is not true if V is of dimension 4. For example, take α as a linear transformation whose invariant factors are t, t and t^2, and β as a linear transformation whose invariant factors are t^2 and t^2. Proposition 7.9 implies that α and β have the same characteristic and minimal polynomials. However, the rational canonical forms of α and β are respectively

$$\left(\begin{array}{c|c|cc} 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right) \quad \text{and} \quad \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array}\right),$$

These matrices are also the Jordan canonical forms of α and β.

which are different and, thus, α and β are not similar. ∎

EXERCISE 7.4

∎ SOLUTION A ∎

EXERCISE 7.5

∎ SOLUTION G ∎

EXERCISE 7.6

∎ SOLUTION T ∎

EXERCISE 7.7 Let V be a k-vector space of dimension n, and let $\alpha \in \mathrm{End}_k(V)$. Prove that the minimal and characteristic polynomials of α coincide if and only if there is a vector $\mathbf{v} \in V$ such that

$$\mathbf{v},\ \alpha(\mathbf{v}),\ \cdots,\ \alpha^{n-1}(\mathbf{v})$$

is a basis of V.

■ SOLUTION The minimal and characteristic polynomials of α coincide if and only if the rational canonical form of α is a companion matrix:

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -r_0 \\ 1 & 0 & 0 & \cdots & 0 & -r_1 \\ 0 & 1 & 0 & \cdots & 0 & -r_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -r_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -r_{n-1} \end{pmatrix}.$$

This happens if and only if there exists a basis $B = \{v_1, \cdots, v_n\}$ of V such that the matrix of α with respect to B is the one above. Finally, looking to the columns of this matrix, we must have

$$v_2 = \alpha(v_1),\ v_3 = \alpha^2(v_1),\ \ldots,\ v_n = \alpha^{n-1}(v_1),$$

that is, if we take $\mathbf{v} := v_1$, then

$$B = \{\mathbf{v}, \alpha(\mathbf{v}), \ldots, \alpha^{n-1}(\mathbf{v})\},$$

as desired. ■

EXERCISE 7.8

■ SOLUTION A ■

EXERCISE 7.9

■ SOLUTION G ■

EXERCISE 7.10

■ SOLUTION T ■

EXERCISE 7.11 A square matrix $A \in \mathcal{M}_n(k)$ is *nilpotent* (cf. Exercise V.4.19) if $A^k = 0$ for some integer k.

- Characterize nilpotent matrices in terms of their Jordan canonical form.
- Prove that if $A^k = 0$ for some integer k, then $A^k = 0$ for some integer k no larger than n (= the size of the matrix).
- Prove that the trace of a nilpotent matrix is 0.

■ SOLUTION

- Let's prove that $A \in \mathcal{M}_n(k)$ is nilpotent if and only if the main diagonal of its Jordan canonical form has only zeroes.

  If A is a nilpotent, then the minimal polynomial of A is of the form t^k for some integer k. By Proposition 7.9, all the other

invariant factors divide the minimal polynomial and so the characteristic polynomial of A is t^n. Thus, the only eigenvalue of A is 0, so the main diagonal of its Jordan canonical form has only zeroes.

Conversely, if the Jordan canonical form of A has only zeroes in the main diagonal, its characteristic polynomial must be t^n. By the Cayley-Hamilton theorem, A is nilpotent.

- If $A^k = 0$, then the minimal polynomial of A divides t^k and so it is t^l for some positive integer l. Since the minimal polynomial always has degree at most n, $l \leq n$ and the result follows.
- Since similar matrices have the same trace, it follows from the first item that the trace of any nilpotent matrix is 0. ∎

EXERCISE 7.12

∎ SOLUTION A ∎

EXERCISE 7.13

∎ SOLUTION G ∎

EXERCISE 7.14

∎ SOLUTION T ∎

EXERCISE 7.15 A *complete flag* of subspaces of a vector space V of dimension n is a sequence of nested subspaces

$$0 = V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{n-1} \subsetneq V_n = V$$

with $\dim V_i = i$. In other words, a complete flag is a composition series in the sense of Exercise 1.16.

Let V be a finite-dimensional vector space over an algebraically closed field. Prove that every linear transformation α of V preserves a complete flag: that is, there is a complete flag as above and such that $\alpha(V_i) \subseteq V_i$.

Find a linear transformation of $\mathbb{R}^2$ that does not preserve a complete flag.

∎ SOLUTION Let α be a linear transformation of V. Since V is a finite-dimensional vector space over an algebraically closed field, α admits a Jordan canonical form. Let $B = \{v_1, \ldots, v_n\}$ be a basis of V such that the matrix of α with respect to B is in Jordan canonical form. Define $V_0 = 0$ and

$$V_i = \langle v_1, v_2, \ldots, v_i \rangle$$

for all $1 \leq i \leq n$. It is clear that

$$V_0 \subsetneq V_1 \subsetneq \cdots \subsetneq V_{n-1} \subsetneq V_n$$

is a complete flag and $\alpha(V_i) \subseteq V_i$ for all $0 \leq i \leq n$ by the definition of B and the subspaces V_i. Therefore, α preserves a complete flag.

For the second part, let β be the linear transformation of $\mathbb{R}^2$ given by the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Geometrically, since β represents a rotation of the plane by 90° degrees about the origin, it cannot preserve any line passing through the point $(0,0)$.

and let's prove that β does not preserve a complete flag. To show this, it suffices to prove that, for any subspace $U \subseteq V$ of dimension 1, $\beta(U) \not\subseteq U$. Indeed, such subspace would be generated by a single nonzero vector $(a,b) \in U$. However, if $\beta((a,b)) = (-b,a) \in U$, this vector would be a multiple of (a,b) and so

$$\det \begin{pmatrix} a & -b \\ b & a \end{pmatrix} = 0 \implies a^2 + b^2 = 0 \implies a = b = 0,$$

contradicting the fact that (a,b) is nonzero. Thus, $(-b,a) \notin U$ and $\beta(U) \not\subseteq U$, as desired. ∎

Exercise 7.16

∎ Solution A ∎

Exercise 7.17

∎ Solution G ∎

Exercise 7.18

∎ Solution T ∎

Exercise 7.19 Prove that a matrix $M \in \mathcal{M}_n(\mathbb{C})$ is normal *if and only if* it admits an orthonormal basis of eigenvectors. (Exercise 7.18 gives one direction; prove the converse.)

∎ Solution If M admits an orthonormal basis of eigenvectors, there exists a matrix P whose columns are orthonormal vectors and such that

$$D = P^{-1}MP$$

is a diagonal matrix. By Exercise 6.18, $P \in \mathrm{U}(n)$ and so $P^{-1} = P^\dagger$. Since

$$M = PDP^{-1} = PDP^\dagger$$

and diagonal matrices commute with each other, we have that

$$\begin{aligned} MM^\dagger &= (PDP^\dagger)(PDP^\dagger)^\dagger = PDP^\dagger PD^\dagger P^\dagger \\ &= PDD^\dagger P^\dagger = PD^\dagger DP^\dagger \\ &= PD^\dagger P^\dagger PDP^\dagger = (PDP^\dagger)^\dagger (PDP^\dagger) \\ &= M^\dagger M. \end{aligned}$$

Therefore, M is normal and so the converse of Exercise 7.18 holds. ∎

EXERCISE 7.20

■ SOLUTION A ■

VII

FIELDS

1 FIELD EXTENSIONS, I

EXERCISE 1.1

■ SOLUTION G ■

EXERCISE 1.2

■ SOLUTION T ■

EXERCISE 1.3 ▷ Let $k \subseteq F$ be a field extension, and let $\alpha \in F$. Prove that the field $k(\alpha)$ consists of all elements of F which may be written as a rational function in α, with coefficients in k. Why does this *not* give (in general) an onto homomorphism $k(t) \to k(\alpha)$? [§1.2, §1.3]

■ SOLUTION Let E be the set of all elements of F which may be written as a rational function in α, with coefficients in k. It is clear that E is a subfield of F that contains k and α, so $k(\alpha) \subseteq E$ by the definition of $k(\alpha)$. On the other hand, since $k(\alpha)$ contains both k and α and is a field, it must also contain any rational function in α, with coefficients in k. Therefore, the other inclusion holds and so $k(\alpha) = E$.

Note that this does not necessarily give an onto homomorphism $k(t) \to k(\alpha)$. Indeed, since field homomorphisms are always injective, such homomorphism would be in fact an isomorphism. However, note that $k \subseteq k(t)$ is always an infinite extension, while $k \subseteq k(\alpha)$ can be finite if α is algebraic over k. By Proposition 1.3, we conclude that this onto homomorphism arises if and only if α is transcendental over k. ■

EXERCISE 1.4

■ SOLUTION A ■

EXERCISE 1.5

■ SOLUTION G ■

EXERCISE 1.6

■ SOLUTION T ■

EXERCISE 1.7 Let $k \subseteq F$ be a field extension, and let $\alpha \in F$ be algebraic over k.

- Suppose $p(x) \in k[x]$ is an irreducible monic polynomial such that $p(\alpha) = 0$; prove that $p(x)$ is the minimal polynomial of α over k, in the sense of Proposition 1.3.
- Let $f(x) \in k[x]$. Prove that $f(\alpha) = 0$ if and only if $p(x) \mid f(x)$.
- Show that the minimal polynomial of α is the minimal polynomial of a certain k-linear transformation of F, in the sense of Definition VI.6.12.

■ SOLUTION

- By Proposition 1.3, $p(x)$ must be divisible by the minimal polynomial of α since its image through the isomorphism given there is $p(\alpha) = 0$. It follows that $p(x)$ is associate to the minimal polynomial of α because $p(x)$ is irreducible. But since both polynomials are monic, they must be the same, as desired.
- Let $\varphi : k[x]/(p(x)) \to k(\alpha)$ be the isomorphism given in Proposition 1.3. It follows that

$$\begin{aligned} f(\alpha) = 0 &\iff \varphi(f(x) + (p(x))) = 0 \\ &\iff f(x) + (p(x)) = 0 \\ &\iff p(x) \mid f(x), \end{aligned}$$

  as needed.
- Let $T : F \to F$ be the k-linear transformation on F given by multiplication by α. It is easy to check that, if $f(x) \in k[x]$ then

$$f(T)(c) = f(\alpha) \cdot c$$

  for all $c \in F$. Therefore, $f(T) = 0$ if and only if $f(\alpha) = 0$ and, by the previous item, this happens if and only if $p(x)$ divides $f(x)$. We conclude that $m_T(x) = p(x)$ by the definition of minimal polynomial of a linear transformation. ■

EXERCISE 1.8

■ SOLUTION A ■

EXERCISE 1.9

■ SOLUTION G ■

EXERCISE 1.10

■ SOLUTION T ■

EXERCISE 1.11 ¬ Let $k \subseteq F$ be a finite field extension, and let $p(x)$ be the characteristic polynomial of the k-linear transformation of F given by multiplication by α. Prove that $p(\alpha) = 0$.

This gives an effective way to find a polynomial satisfied by an element of an extension. Use it to find a polynomial satisfied by $\sqrt{2}+\sqrt{3}$ over $\mathbb{Q}$, and compare this method with the one used in Example 1.19. [1.12]

■ SOLUTION By Exercise 1.7, the minimal polynomial of α is the minimal polynomial of the k-linear transformation of F given by multiplication by α. By the Cayley-Hamilton theorem, we conclude that $p(\alpha) = 0$.

If we consider the composition of extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

the proof of Proposition 1.10 implies that

$$(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$$

is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$ because $(1, \sqrt{2})$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ and $(1, \sqrt{3})$ is a basis for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}(\sqrt{2})$. With this basis, the $\mathbb{Q}$-linear transformation of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ given by multiplication by $\sqrt{2}+\sqrt{3}$ has the following matrix representation:

$$\begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

A quick computation shows that the characteristic polynomial of this matrix is $p(x) = x^4 - 10x^2 + 1$. As we proved before, it follows that $p(\sqrt{2}+\sqrt{3}) = 0$.

Note that this method does not require solving a system of equations or guessing values, as done in Example 1.19. However, it is necessary that we have a basis for the extension in order to compute the characteristic polynomial of the linear transformation. ■

EXERCISE 1.12

■ SOLUTION A ■

EXERCISE 1.13

■ SOLUTION G ■

EXERCISE 1.14

■ SOLUTION T ■

EXERCISE 1.15 ¬ Let $k \subseteq F$ be a finite extension, and let $\alpha \in F$. Assume $[F : k(\alpha)] = r$. Prove that

$$\mathrm{tr}_{k\subseteq F}(\alpha) = r\,\mathrm{tr}_{k\subseteq k(\alpha)}(\alpha) \text{ and } N_{k\subseteq F}(\alpha) = N_{k\subseteq k(\alpha)}(\alpha)^r.$$

(Cf. Exercises 1.12 and 1.13.) (Hint: If $f_1, \dots, f_r$ is a basis of F over $k(\alpha)$ and α has degree d over k, then $(f_i\alpha^j)_{\substack{i=1,\cdots,r \\ j=1,\cdots,d-1}}$ is a basis of F over k. The matrix corresponding to multiplication by α with respect to this basis consists of r identical square blocks.) [4.19, 4.21]

■ SOLUTION Let B be the basis given in the hint, ordered as

$$B = (f_1, f_1\alpha, \dots, f_1\alpha^{d-1}, f_2, f_2\alpha, \dots, f_2\alpha^{d-1}, \dots, f_r\alpha^{d-1}).$$

For a given index i, note that the α-multiples of $f_i, \dots, f_i\alpha^{d-1}$ can also be written as linear combinations of these elements. Indeed, we essentially need to check this for $\alpha \cdot (f_i\alpha^{d-1})$: if

$$p(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_1x + x_0$$

is the minimal polynomial of α over k, then

$$\alpha \cdot (f_i\alpha^{d-1}) = f_i\alpha^d = (-c_0)f_i + (-c_1)f_i\alpha + \cdots + (-c_{d-1})f_i\alpha^{d-1},$$

Each block will be the companion matrix of the minimal polynomial $p(x)$ of α over k.

as desired. Therefore, the matrix of the linear transformation of F given by multiplication by α will consist of r square blocks of size d over the main diagonal. Furthermore, since $(1, \alpha, \dots, \alpha^{d-1})$ is a basis for $k(\alpha)$ over k, these blocks will be identical to the matrix of the linear transformation of $k(\alpha)$ given by multiplication by α. Thus, it follows immediately that

$$\operatorname{tr}_{k\subseteq F}(\alpha) = r \operatorname{tr}_{k\subseteq k(\alpha)}(\alpha)$$

and, by the Remark below, we also have that

$$N_{k\subseteq F}(\alpha) = N_{k\subseteq k(\alpha)}(\alpha)^r,$$

proving the exercise. ■

Remark. A remarkable property of determinants is that, if M is a matrix of the form

$$M = \left(\begin{array}{c|c|c|c|c} M_1 & * & * & \cdots & * \\ \hline 0 & M_2 & * & \cdots & * \\ \hline 0 & 0 & M_3 & \cdots & * \\ \hline \vdots & \vdots & \vdots & \ddots & \vdots \\ \hline 0 & 0 & 0 & \cdots & M_n \end{array}\right),$$

where $M_1, M_2, \dots, M_n$ are square blocks (not necessarily of the same size), then

$$\det M = \det M_1 \det M_2 \cdots \det M_n.$$

Another interesting property is that, if M is a matrix of the form

$$M = \left(\begin{array}{c|c} A & B \\ \hline C & D \end{array}\right),$$

where the block D is invertible, then

$$\det M = \det(AD - BD^{-1}CD).$$

In particular, if $CD = DC$, we have that

$$\det M = \det(AD - BC)$$

and we can compute this determinant almost as if M were a 2×2 matrix. (In this last case, the hyptohesis that D is invertible can be dispensed.)

EXERCISE 1.16

■ SOLUTION A ■

EXERCISE 1.17

■ SOLUTION G ■

EXERCISE 1.18

■ SOLUTION T ■

EXERCISE 1.19 Let $k \subseteq F$ be a field extension of degree p, a prime integer. Prove that there are no subrings of F properly containing k and properly contained in F. (Use Exercise 1.18.)

■ SOLUTION Let R be a subring of F containing k. Since $k \subseteq F$ is a finite extension, Lemma 1.9 implies that it is algebraic and so R is a field by Exercise 1.18. Now, Proposition 1.10 tells us that the extensions $k \subseteq R$ and $R \subseteq F$ are finite, and

$$[F : R] \cdot [R : k] = [F : k] = p.$$

Since p is prime, either $[F : R] = 1$ or $[R : k] = 1$, that is, either $R = F$ or $R = k$. Therefore, there are no subrings of F properly containing k and properly contained in F. ■

EXERCISE 1.20

■ SOLUTION A ■

EXERCISE 1.21

■ SOLUTION G ■

EXERCISE 1.22

■ SOLUTION T ■

EXERCISE 1.23 Express $\sqrt{2}$ explicitly as a polynomial function in $\sqrt{2}+\sqrt{3}$ with rational coefficients.

■ SOLUTION By Example 1.19, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}+\sqrt{3})$ is an extension of degree 4. Thus,

$$(1,\ \sqrt{2}+\sqrt{3},\ (\sqrt{2}+\sqrt{3})^2,\ (\sqrt{2}+\sqrt{3})^3)$$

is a basis for $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ over $\mathbb{Q}$ and so there are unique $q_0, q_1, q_2, q_3 \in \mathbb{Q}$ such that

$$\sqrt{2} = q_0 + q_1(\sqrt{2}+\sqrt{3}) + q_2(\sqrt{2}+\sqrt{3})^2 + q_3(\sqrt{2}+\sqrt{3})^3.$$

Computing the powers above we get that

$$\sqrt{2} = (q_0 + 5q_2) + (q_1 + 11q_3)\sqrt{2} + (q_1 + 9q_3)\sqrt{3} + (2q_2)\sqrt{6}.$$

As argued in Exercise 1.11, $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ is also a basis for $\mathbb{Q}(\sqrt{2}+\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$. Therefore, we must have

$$\begin{cases} q_0 + 5q_2 = 0 \\ q_1 + 11q_3 = 1 \\ q_1 + 9q_3 = 0 \\ 2q_2 = 0 \end{cases} \implies \begin{cases} q_0 = 0 \\ q_1 = -\frac{9}{2} \\ q_2 = 0 \\ q_3 = \frac{1}{2} \end{cases}$$

and so

$$\sqrt{2} = -\frac{9}{2}(\sqrt{2}+\sqrt{3}) + \frac{1}{2}(\sqrt{2}+\sqrt{3})^3$$

expresses $\sqrt{2}$ as a polynomial function in $\sqrt{2}+\sqrt{3}$ with rational coefficients. ■

EXERCISE 1.24

■ SOLUTION A ■

EXERCISE 1.25

■ SOLUTION G ■

EXERCISE 1.26

■ SOLUTION T ■

EXERCISE 1.27 ¬ With notation and terminology as in Exercise 1.26, the indexed set $\{\alpha_i\}_{i\in I}$ is a *transcendence basis* for F over k if it is a maximal algebraically independent set in F.

- Prove that $\{\alpha_i\}_{i\in I}$ is a transcendence basis for F over k if and only if it is algebraically independent and F is algebraic over $k(\{\alpha_i\}_{i\in I})$.
- Prove that transcendence bases exist. (Zorn)
- Prove that any two transcendence bases for F over k have the same cardinality. (Mimic the proof of Proposition VI.1.9. Don't feel too bad if you prefer to deal only with the case of finite transcendence bases.)

The cardinality of a transcendence basis is called the *transcendence degree* of F over k, denoted $\mathrm{tr}.\deg_{k\subseteq F}$. [1.28, 1.29, 2.19]

■ SOLUTION

- Let $S = \{\alpha_i\}_{i\in I}$ be an algebraically independent set in F. We will prove the equivalent statement that S is not a transcendental basis for F over k if and only if F is transcendental over $k(S)$. Indeed, this last condition happens if and only if there exists $\beta \in F$ that does not satisfy any polynomial function with coefficients in $k(S)$. Since S is already algebraically independent over k, this occurs if and only if $S \cup \{\beta\} \supsetneq S$ is also algebraically independent over k and, therefore, if and only if S is not a transcendental basis for F over k.

- The proof is very similar to the proof of Lemma VI.1.2. Consider the family $\mathscr{F}$ of all algebraically independent sets in F over k, ordered by inclusion. If the extension $k \subseteq F$ is algebraic, then we may consider the empty set as a transcendence basis for F over k. Thus, we may suppose that $k \subseteq F$ is a transcendental extension and so $\mathscr{F} \neq \emptyset$. By Zorn's lemma, to show that transcendence bases exist, it suffices to verify that every chain in $\mathscr{F}$ has an upper bound. Indeed, the union of a chain of algebraically independent sets in F over k is also algebraically independent over k because, since polynomials are only finite sums of monomials, any relation of 'algebraic dependence' only involves finitely many elements and these elements would all belong to one subset in the chain.

  The same argument shows that any algebraically independent set may be extended to a transcendence basis.

- Mimicking Proposition VI.1.9, we will prove that, if $S \subseteq F$ is algebraically independent over k and $B \subseteq F$ is a transcendence basis for F over k, then $|S| \leq |B|$. It will follows that any two transcendence bases for F over k have the same cardinality.

  We have to prove that there is an injective map $j : S \hookrightarrow B$, and this can be done by an inductive process, replacing the elements of B by elements of S 'one-by-one'. For this, let $\leq$ be a well-ordering on S, let $\alpha \in S$, and assume we have defined j for all $\beta \in S$ with $\beta < \alpha$. Let B' be the set obtained from B by

replacing all $j(\beta)$ by β, for all $\beta < \alpha$, and assume (inductively) that B' is still a transcendence basis for F over k. Then we claim that $j(\alpha) \in B$ may be defined so that $j(\alpha) \neq j(\beta)$ for all $\beta < \alpha$ and the set B'' obtained from B' by replacing $j(\alpha)$ by α is still a transcendence basis for F over k. Transfinite induction (Claim V.3.2) then shows that j is defined and injective on S, as needed.

To verify our claim, since B' is a transcendence basis for F over k, $B' \cup \{\alpha\}$ is not algebraically independent as an indexed set, so that there exists a nonzero polynomial $f \in k[x_0, x_1, \ldots, x_n]$ and distinct $\beta_1, \ldots, \beta_n \in B'$ such that

$$f(\alpha, \beta_1, \ldots, \beta_n) = 0.$$

We may assume that each one of the variables $x_0, x_1, \ldots, x_n$ appears in f with a nonzero coefficient at least one time. Moreover, since S is algebraically independent over k, at least one of the elements $\beta_1, \ldots, \beta_n$ is not in S. Without loss of generality, suppose that $\beta_1 \in B' \setminus S$. This guarantees that $\beta_1 \neq j(\beta)$ for all $\beta < \alpha$; we set $j(\alpha) = \beta_1$.

All that is left now is the verification that the set B'' obtained by replacing β_1 by α in B' is a transcendence basis for F over k. First, consider the composition of extensions:

$$k(B'') \subseteq k(B'' \cup \{\beta_1\}) = k(B' \cup \{\alpha\}) \subseteq F.$$

By the first item, the last extension above is algebraic and, since $f(\alpha, \beta_1, \ldots, \beta_n) = 0$, β_1 is algebraic over $k(B'')$ and so the first extension is also algebraic. By Corollary 1.18, $k(B'') \subseteq F$ is an algebraic extension. Now, if B'' were not algebraically independent over k, α would be algebraic over $k(B'' \setminus \{\alpha\})$ and, since we have the extensions

$$k(B'' \setminus \{\alpha\}) \subseteq k(B'') \subseteq F,$$

the extension $k(B'' \setminus \{\alpha\}) \subseteq F$ would be algebraic, again by Corollary 1.18. But this would imply that β_1 is algebraic over $k(B'' \setminus \{\alpha\})$, contradicting that B' is algebraically independent. Therefore, B'' must be algebraically independent and we conclude by the first item that B'' is a transcendence basis for F over k, as desired. ∎

EXERCISE 1.28

∎ SOLUTION A ∎

EXERCISE 1.29

∎ SOLUTION G ∎

EXERCISE 1.30

■ SOLUTION T ■

2 ALGEBRAIC CLOSURE, NULLSTELLENSATZ, AND A LITTLE ALGEBRAIC GEOMETRY

EXERCISE 2.1 ▷ Prove Lemma 2.1. [§2.1]

■ SOLUTION We will enumerate the statements in Lemma 2.1 as follows:

(1) K is algebraically closed.

(2) K has no nontrivial algebraic extensions.

(3) If $K \subseteq L$ is any extension $\alpha \in L$ is algebraic over K, then $\alpha \in K$.

Let's prove that (1) $\implies$ (2) $\implies$ (3) $\implies$ (1).

(1) $\implies$ (2). Suppose that $K \subseteq L$ is a nontrivial algebraic extension. Thus, there exists $\alpha \in L \setminus K$, which is algebraic over K. By Proposition 1.3, the minimal polynomial of α is irreducible and, since $\alpha \notin K$, its degree is at least 2. It follows that K is not algebraically closed.

(2) $\implies$ (3). Let $K \subseteq L$ be any extension and let $\alpha \in L$ be algebraic over K. Thus, $K \subseteq K(\alpha)$ is an algebraic extension, so $K = K(\alpha)$ and $\alpha \in K$.

(3) $\implies$ (1). Let $f(x) \in K[x]$ be a nonzero irreducible polynomial. By Proposition V.5.7, there are an extension $K \subseteq L$ and $\alpha \in L$ such that $f(\alpha) = 0$. This means that α is algebraic over K and, by hypothesis, $\alpha \in K$. Therefore, the polynomial $x - a$ divides $f(x)$ and, since it is irreducible, the degree of $f(x)$ must be 1. Therefore, all irreducible polynomials in $K[x]$ have degree 1 and we conclude that K is algebraically closed. ■

EXERCISE 2.2

■ SOLUTION A ■

EXERCISE 2.3

■ SOLUTION G ■

EXERCISE 2.4

■ SOLUTION T ■

EXERCISE 2.5 Let K be a field, let A be a subset of $K[x_1, \ldots, x_n]$, and let I be the ideal generated by A. Prove that $\mathscr{V}(A) = \mathscr{V}(I)$ in $\mathbb{A}^n_K$. [§2.3]

■ SOLUTION It is immediate that $\mathscr{V}(I) \subseteq \mathscr{V}(A)$ because $A \subseteq I$. Let's prove the other inclusion. Let $p \in \mathscr{V}(A)$ and let $f \in I$ be any

polynomial. Since I is generated by A, there are $a_1, \ldots, a_n \in A$ and $g_1, \ldots, g_n \in K[x]$ such that

$$f = g_1 a_1 + \cdots g_n a_n.$$

By the definition of $\mathscr{V}(A)$, it follows that

$$f(p) = g_1(p)a_1(p) + \cdots + g_n(p)a_n(p) = g_1(p) \cdot 0 + \cdots g_n(p) \cdot 0 = 0.$$

Since f was an arbitrary polynomial of I, we conclude that $p \in \mathscr{V}(I)$ and so $\mathscr{V}(A) \subseteq \mathscr{V}(I)$, as desired. ∎

EXERCISE 2.6

∎ SOLUTION A ∎

EXERCISE 2.7

∎ SOLUTION G ∎

EXERCISE 2.8

∎ SOLUTION T ∎

EXERCISE 2.9 ▷ Prove that every affine algebraic set equals $\mathscr{V}(I)$ for a *radical* ideal I. [§2.3]

∎ SOLUTION Since any affine algebraic set is by definition of the form $\mathscr{V}(I)$ for some ideal $I \subseteq K[x_1, \ldots, x_n]$, it suffices to prove that $\mathscr{V}(I) = \mathscr{V}(\sqrt{I})$. The inclusion $\mathscr{V}(\sqrt{I}) \subseteq \mathscr{V}(I)$ follows from the inclusion $I \subseteq \sqrt{I}$. Now, to prove the other inclusion, let $p \in \mathscr{V}(I)$ be an arbitrary point. For every $f \in \sqrt{I}$, there exists $k \geq 0$ such that

$$f^k \in I \implies f^k(p) = 0 \implies f(p) = 0.$$

Therefore, $p \in \mathscr{V}(\sqrt{I})$ and so $\mathscr{V}(I) \subseteq \mathscr{V}(\sqrt{I})$, as desired. ∎

EXERCISE 2.10

∎ SOLUTION A ∎

EXERCISE 2.11

∎ SOLUTION G ∎

EXERCISE 2.12

∎ SOLUTION T ∎

EXERCISE 2.13 Let K be an algebraically closed field. Prove that every reduced commutative K-algebra of finite type is the coordinate ring of an algebraic set S in some affine space $\mathbb{A}^n_K$.

■ SOLUTION If R is a commutative K-algebra of finite type, it follows that

$$R \cong \frac{K[x_1, \ldots, x_n]}{I}$$

for some n and some ideal I of $K[x_1, \ldots, x_n]$. If R is also reduced, Exercise 2.8 implies that I is radical. Taking $S = \mathscr{V}(I) \subseteq \mathbb{A}^n_K$, we have that $\mathscr{I}(S) = I$ by Corollary 2.18 and so R is isomorphic to the coordinate ring $K[S]$. ■

EXERCISE 2.14

■ SOLUTION A ■

EXERCISE 2.15

■ SOLUTION G ■

EXERCISE 2.16

■ SOLUTION T ■

EXERCISE 2.17 ¬ Let K be an algebraically closed field, and let $\mathfrak{m}$ be a maximal ideal of $K[x_1, \ldots, x_n]$, corresponding to a point p of $\mathbb{A}^n_K$. A *germ* of a function at p is determined by an open set containing p and a function defined on that open set; in our context (dealing with rational functions and where the open set may be taken to be the complement of a function that does not vanish at p) this is the same information as a rational function defined at p, in the sense of Exercise 2.16.

Show how to identify the ring of germs with the localization $K[\mathbb{A}^n_K]_{\mathfrak{m}}$ (defined in Exercise V.4.11).

As in Exercise 2.16, the same discussion can be carried out for any algebraic set. This is the origin of the name 'localization': localizing the coordinate ring of a variety V at the maximal ideal corresponding to a point p amounts to considering only functions defined in a neighborhood of p, thus studying V 'locally', 'near p'. [V.4.7]

■ SOLUTION As pointed in the statement of the exercise, the ring of germs R corresponds to all rational functions defined at p, that is, rationals functions of the form

$$\alpha = \frac{F}{G}$$

where $F, G \in K[x_1, \ldots, x_n]$ are relatively prime and $G(p) \neq 0$. Since α is defined at $p = (c_1, \ldots, c_n)$, we must have

$$G \notin \mathfrak{m} = (x - c_1, \ldots, x - c_n).$$

Thus, we can define the function

$$\begin{aligned} \varphi : R &\to K[\mathbb{A}^n_K]_{\mathfrak{m}} \\ \frac{F}{G} &\mapsto \frac{F}{G}. \end{aligned}$$

This function is clearly a bijection since equality of two fractions in $K[\mathbb{A}^n_K]_{\mathfrak{m}}$ is the same as equality in the field of rational functions $K(x_1, \ldots, x_n)$. (In this case, the 't' in the definition of the localization may be disregarded since $K[\mathbb{A}^n_K]$ is an integral domain.) Moreover, note that φ is indeed an isomorphism of rings because it also preserves operations. ∎

Remark. Germs can be defined more generally for a point in a topological space. Let x be a point in some topological space and let F be some family of functions defined in neighbourhood of x (each in its own neighbourhood). Two functions $f, g \in F$ are said to be equivalent at x if they coincide in some neighbourhood of x. An equivalence class generated by this relation is called a germ of functions of class F at x.

In the exercise above, the topological space considered is $\mathbb{A}^n_K$ endowed with the Zariski topology (see Exercise 2.7) and F is the family of rational functions defined at p.

EXERCISE 2.18

∎ SOLUTION A ∎

EXERCISE 2.19

∎ SOLUTION G ∎

EXERCISE 2.20

∎ SOLUTION T ∎

EXERCISE 2.21 ¬ Let $F(x_0, \ldots, x_n) \in K[x_0, \ldots, x_n]$ be a *homogeneous* polynomial. With notation as in Exercise 2.20, prove that the condition '$F(c_0, \ldots, c_n) = 0$' for a point $(c_0 : \ldots : c_n) \in \mathbb{P}^n_K$ is well-defined: it does not depend on the representative $(c_0, \ldots, c_n)$ chosen for the points $(c_0 : \ldots : c_n)$. We can then define the following subset of $\mathbb{P}^n_K$:

$$\mathcal{V}(F) := \{(c_0 : \ldots : c_n) \in \mathbb{P}^n_K \mid F(c_0, \ldots, c_n) = 0\}.$$

Prove that this 'projective algebraic set' can be covered with $n + 1$ affine algebraic sets.

The basic definitions in 'projective algebraic geometry' can be developed along essentially the same path taken in this section for affine algebraic geometry, using 'homogenous ideals' (that is,

ideals generated by homogeneous polynomials; see §VIII.4.3) rather than ordinary ideals. This problem shows one way to relate projective and affine algebraic sets, in one template example. [VIII.4.8, VIII.4.11]

■ SOLUTION For the first part, let $(c_0, \cdots, c_n)$ and $(c'_0, \ldots, c'_n)$ be two equivalent points in K^{n+1}, accordingly to the equivalence relation defined in Exercise 2.20. Thus, there exists $\lambda \in K^*$ such that

$$(c'_0, \ldots, c'_n) = (\lambda c_0, \ldots, \lambda c_n)$$

and, since F is a homogeneous polynomial, we have that

$$F(c'_0, \ldots, c'_n) = \lambda^l \cdot F(c_0, \ldots, c_n),$$

where l is the degree of F. Therefore,

$$F(c_0, \ldots, c_n) = 0 \iff F(c'_0, \ldots, c'_n) = 0$$

and the considered condition is well-defined.

For the second part, consider the copies of $\mathbb{A}^n_K$ in $\mathbb{P}^n_K$ defined by the injections

$$(c_1, \ldots, c_n) \mapsto (c_1 : \ldots : c_{i-1} : 1 : c_i : \ldots : c_n)$$

for all $1 \leq i \leq n+1$, as in Exercise 2.20. We can define the affine algebraic sets

$$S_i = \mathscr{V}(F(x_1, \ldots, x_{i-1}, 1, x_i, \ldots, x_n)) \subseteq \mathbb{A}^n_K$$

for all $1 \leq i \leq n+1$, that is, we consider the zeroes of the polynomial F when we replace one of its variables by 1. Each S_i can be naturally identified as a subset of the i-th copy of $\mathbb{A}^n_K$ inside $\mathbb{P}^n_K$, as defined above. Since the copies of $\mathbb{A}^n_K$ cover $\mathbb{P}^n_K$, it follows that

$$\mathscr{V}(F) = S_1 \cup \cdots \cup S_{n+1},$$

showing that this projective algebraic set can be covered with $n+1$ affine algebraic sets. ■

3 GEOMETRIC IMPOSSIBILITIES

EXERCISE 3.1

■ SOLUTION A ■

EXERCISE 3.2

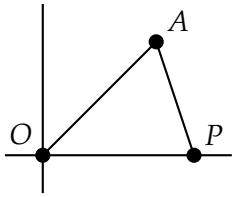
■ SOLUTION G ■

EXERCISE 3.3

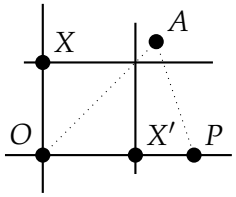
■ SOLUTION T ■

EXERCISE 3.4 Show how to square a *triangle* by straightedge and compass.

■ SOLUTION Choosing two vertices of the given triangle to be the starting points O and P, we may suppose that the vertices are $O = (0,0)$, $P = (1,0)$ and $A = (a,b)$, where a and b are positive constructible real numbers.



Note that the area of this triangle is $\frac{b}{2}$ and so we need to construct a square of side $\sqrt{\frac{b}{2}}$. Proceeding as done just before Definition 3.1, we may mark the point $(b,0)$ on the x-axis and, by Exercise 3.1, we can construct the point $(\frac{b}{2},0)$. Now, with the construction given in the proof of Theorem 3.4, we can construct the point $X = (0,\sqrt{\frac{b}{2}})$ and, thus, the point $X' = (\sqrt{\frac{b}{2}},0)$. Tracing perpendicular lines to the x-axis and the y-axis that pass through these points, we get a square:



It is clear that the area of this square is the same as the area of the triangle. ■

EXERCISE 3.5

■ SOLUTION A ■

EXERCISE 3.6

■ SOLUTION G ■

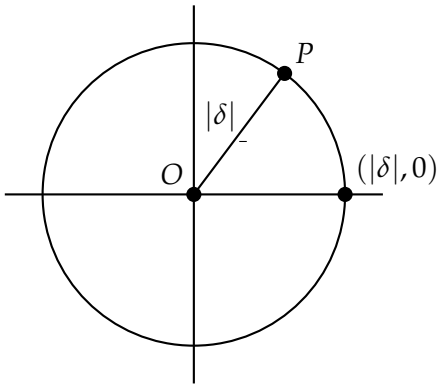
EXERCISE 3.7

■ SOLUTION T ■

EXERCISE 3.8 For $\delta \in \mathbb{C}$, $\delta \neq 0$, let θ_δ be the argument of δ (that is, the angle formed by the line through 0 and δ with the real axis).

Prove that $\delta \in \mathscr{C}_{\mathbb{C}}$ if and only if $|\delta|$, $\cos\theta_\delta$, $\sin\theta_\delta$ are all constructible *real* numbers.

■ SOLUTION ($\Longrightarrow$) If $\delta \in \mathscr{C}_{\mathbb{C}}$ then the point $P = (|\delta|\cos\theta_\delta, |\delta|\sin\theta_\delta)$ is constructible and so $|\delta|\cos\theta_\delta$ and $|\delta|\sin\theta_\delta$ are constructible real numbers. Now, the intersection of the circle centered at the origin and passing through P with the x-axis is precisely the point $(|\delta|, 0)$, so $|\delta|$ is also a constructible real number.



Finally, since $\mathscr{C}_{\mathbb{R}}$ is a field and $|\delta| \neq 0$, it follows that $\cos\theta_\delta$ and $\sin\theta_\delta$ are constructible real numbers.

($\Longleftarrow$) Since $\mathscr{C}_{\mathbb{R}}$ is a field, $|\delta|\cos\theta_\delta$ and $|\delta|\sin\theta_\delta$ are constructible. By Lemma 3.2, it follows that $\delta = (|\delta|\cos\theta_\delta) + i(|\delta|\sin\theta_\delta)$ is constructible and so $\delta \in \mathscr{C}_{\mathbb{C}}$. ■

EXERCISE 3.9

■ SOLUTION A ■

EXERCISE 3.10

■ SOLUTION G ■

EXERCISE 3.11

■ SOLUTION T ■

EXERCISE 3.12 Prove that the angles of 1° and 2° are not constructible. (Hint: Given what we know at this point, you only need to recall that there exist trigonometric formulas for the sum of two angles; the exact shape of these formulas is not important.) For what integers n is the angle n° constructible?

■ SOLUTION Suppose that the angles of 1° and 2° are constructible. By Exercise 3.10, we have that $\cos 1^\circ$ and $\cos 2^\circ$ are constructible real numbers. Applying the formula

$$\cos(\theta + \theta') = \cos(\theta)\cos(\theta') - \sin(\theta)\sin(\theta')$$

repeatedly, we get that $\cos 20^\circ$ can be expressed as a polynomial in $\cos 1^\circ$ and as a polynomial in $\cos 2^\circ$ because 20 is a multiple of 1 and

2. Since $\mathscr{C}_{\mathbb{R}}$ is field, this implies that 20° is a constructible angle, which contradicts what has been proved in §3.3. Therefore, 1° and 2° cannot be constructible.

Since 3° is constructible, the argument above shows that n° is a construcible angle for all integers n divisible by 3. Conversely, if n° is constructible, then n is divisible by 3. Indeed, if the quotient and the remainder of n by 3 are respectively q and r, we can apply the identity above to $\theta = n^\circ$ and $\theta' = (-3q)^\circ$ and obtain that r° is constructible, which implies that $r = 0$. ∎

EXERCISE 3.13

∎ SOLUTION A ∎

EXERCISE 3.14

∎ SOLUTION G ∎

EXERCISE 3.15

∎ SOLUTION T ∎

4 FIELD EXTENSIONS, II

EXERCISE 4.1 ▷ Let k be a field, $f(x) \in k[x]$, and let F be the splitting field for $f(x)$ over k. Let $k \subseteq K$ be an extension such that $f(x)$ splits as a product of linear factors over K. Prove that there is a homomorphism $F \to K$ extending the identity on k. [§4.2]

∎ SOLUTION Since $f(x)$ splits as a product of linear factors over K, $f(x)$ has roots $\alpha_1, \ldots, \alpha_r$ in K. Let $F' = k(\alpha_1, \ldots, \alpha_r) \subseteq K$ be the extension of k generated by the roots of $f(x)$. By definition, it follows that F' is the splitting field for $f(x)$ over k and so Lemma 4.2 implies that there exists an isomorphism $F \to F'$ extending the identity on k. Composing this isomorphism with the inclusion $F' \to K$, we get a homomorphism $F \to K$ extending the identity on k. ∎

EXERCISE 4.2

∎ SOLUTION A ∎

EXERCISE 4.3

∎ SOLUTION G ∎

EXERCISE 4.4

∎ SOLUTION T ∎

EXERCISE 4.5 ▷ Let F be a splitting field for a polynomial $f(x) \in k[x]$, and let $g(x) \in k[x]$ be a factor of $f(x)$. Prove that F contains a unique copy of the splitting field of $g(x)$. [§5.1]

■ SOLUTION Note that $g(x)$ splits in F because it is a factor of $f(x)$. Thus, $g(x)$ has roots $\alpha_1, \ldots, \alpha_r$ in F and we have that $k(\alpha_1, \ldots, \alpha_r) \subseteq F$ is the splitting field of $g(x)$ over k. This is the unique copy of the splitting field of $g(x)$ in F since, by definition, it is uniquely determined by the roots $\alpha_1, \ldots, \alpha_r$ of $g(x)$. ■

EXERCISE 4.6

■ SOLUTION A ■

EXERCISE 4.7

■ SOLUTION G ■

EXERCISE 4.8

■ SOLUTION T ■

EXERCISE 4.9 Using the notion of 'derivative' given in §4.2, prove that $(fg)' = f'g + fg'$ for all polynomials f, g.

■ SOLUTION Let

$$f(x) = \sum_{i \geq 0} a_i x^i \quad \text{and} \quad g(x) = \sum_{j \geq 0} b_j x^j$$

be arbitrary polynomials. A quick computation shows that the k-th coefficient of $(fg)'$ and $f'g + fg'$ are

$$(k+1) \sum_{i+j=k+1} a_i b_j$$

and

$$\sum_{i+j=k} (i+1) a_{i+1} b_j + \sum_{i+j=k} (j+1) a_i b_{j+1},$$

respectively, so we just need to show that these two expressions are the same for all $k \geq 0$. Indeed, in the last expression, replace $i+1$ by i in the first sum and $j+1$ by j in the second. It follows that

$$\begin{aligned} &\sum_{i+j=k} (i+1) a_{i+1} b_j + \sum_{i+j=k} (j+1) a_i b_{j+1} \\ =& \sum_{i+j=k+1} i a_i b_j + \sum_{i+j=k+1} j a_i b_j \\ =& \sum_{i+j=k+1} (i+j) a_i b_j \\ =&(k+1) \sum_{i+j=k+1} a_i b_j, \end{aligned}$$

as needed. ■

Note that we added the term $0 \cdot a_0 b_{k+1}$ to the first sum and the term $0 \cdot a_{k+1} b_0$ to the second, but they do not change the equality since they equal to 0.

EXERCISE 4.10

■ SOLUTION A ■

EXERCISE 4.11

■ SOLUTION G ■

EXERCISE 4.12

■ SOLUTION T ■

EXERCISE 4.13 ▷ Let k be a field of positive characteristic p, and let $f(x)$ be an irreducible polynomial. Prove that there exist an integer d and a *separable* irreducible polynomial $f_{\text{sep}}(x)$ such that

$$f(x) = f_{\text{sep}}(x^{p^d}).$$

The number p^d is called the *inseparable degree* of $f(x)$. If $f(x)$ is the minimal polynomial of an algebraic element α, the inseparable degree of α is defined to be the inseparable degree of $f(x)$. Prove that α is inseparable if and only if its inseparable degree is $\geq p$.

The picture to keep in mind is as follows: the roots of the minimal polynomial $f(x)$ of α are distributed into $\deg f_{\text{sep}}$ 'clumps', each collecting a number of coincident roots equal to the inseparable degree of α. We say that α is 'purely inseparable' if there is only one clump, that is, if all roots of $f(x)$ coincide (see Exercise 4.14). [§4.2, 4.14, 4.18]

■ SOLUTION FALTA A PRIMEIRA PARTE

Now, for the second part of the exercise, it is equivalent to prove that α is separable if and only if its inseparable degree is 1.

($\Longrightarrow$) Suppose that α is separable and let $f(x)$ be its minimal polynomial over k. By the first part of the exercise, there exists a separable polynomial $f_{\text{sep}}(x) \in k[x]$ and an integer d such that $f(x) = f_{\text{sep}}(x^{p^d})$. If $x - a$ divides $f_{\text{sep}}(x)$ in $\overline{k}$, it follows that $x^{p^d} - a$ divides $f(x)$ in $\overline{k}$. But note that $x^{p^d} - a$ has only one root. Indeed, if $b \in \overline{k}$ is such that $b^{p^d} = a$, we have that

$$x^{p^d} - a = x^{p^d} - b^{p^d} = (x - b)^{p^d}$$

after applying Exercise 4.8 successively. Since α is separable, $f(x)$ is separable and so we must have $p^d = 1$, that is, the inseparable degree of α must be 1.

($\Longleftarrow$) If the inseparable degree of α is 1, the definition above immediately implies that the minimal polynomial of α over k is separable. Thus, α is separable. ■

EXERCISE 4.14

■ SOLUTION A ■

EXERCISE 4.15

■ SOLUTION G ■

EXERCISE 4.16

■ SOLUTION T ■

EXERCISE 4.17 ¬ Let $k \subseteq F$ be an algebraic extension, in positive characteristic. With notation as in Exercises 4.14 and 4.16, prove that the extension $F_{\text{sep}} \subseteq F$ is purely inseparable. Prove that the extension $k \subseteq F$ is purely inseparable if and only if $F_{\text{sep}} = k$. [4.18]

■ SOLUTION Let $\alpha \in F$. We claim that $\alpha^{p^d} \in F_{\text{sep}}$, where p^d is the inseparable degree of α over k, as defined in Exercise 4.13. Indeed, let $f(x)$ be the minimal polynomial of α over k and let $f_{\text{sep}}(x)$ be the separable irreducible polynomial such that $f(x) = f_{\text{sep}}(x^{p^d})$. Since α is a root of $f(x)$, α^{p^d} is a root of $f_{\text{sep}}(x)$ and, since this polynomial is irreducible, $f_{\text{sep}}(x)$ is the minimal polynomial of α^{p^d} over k. It follows that α^{p^d} is separable over k, which proves that $F_{\text{sep}} \subseteq F$ is purely inseparable.

For the second part, it suffices to show that $F_{\text{sep}} \subseteq k$. Let $\alpha \in F_{\text{sep}}$. Since $k \subseteq F$ is purely inseparable and $F_{\text{sep}} \subseteq F$, α is purely inseparable over k. Thus, Exercise 4.14 implies that the degree of α over k equals its inseparable degree. But, since $\alpha \in F_{\text{sep}}$, α is separable over k and it follows from Exercise 4.13 that its inseparable degree is 1. Therefore, the degree of α is 1 and $\alpha \in k$, as desired. ■

EXERCISE 4.18

■ SOLUTION A ■

EXERCISE 4.19

■ SOLUTION G ■

EXERCISE 4.20

■ SOLUTION T ■

EXERCISE 4.21 ¬ Let $k \subseteq E \subseteq F$ be finite separable extensions, and let $\alpha \in F$. Prove that

$$N_{k\subseteq F}(\alpha) = N_{k\subseteq E}(N_{E\subseteq F}(\alpha)) \text{ and } \operatorname{tr}_{k\subseteq F}(\alpha) = \operatorname{tr}_{k\subseteq E}(\operatorname{tr}_{E\subseteq F}(\alpha)).$$

(Hint: Use Exercise 4.19: if $d = [E : k]$ and $e = [F : E]$, the de embeddings of F into $\overline{k}$ lifting id_k must divide into d groups of e each, according to their restriction to E.)

This 'transitivity' of norm and trace extends the result of Exercise 1.15 to separable extensions. The separability restriction is actually unnecessary; cf. Exercise 4.22. [4.22]

■ SOLUTION Firstly, since the extensions are finite and separable, Proposition 4.24 states that $d = [E : k]$ and $e = [F : E]$ are the separable degrees of E over k and of F over E, respectively. Now, note that any embedding of F into $\overline{k}$ lifting id_k is an embedding of E into $\overline{k}$ lifting id_k if we restrict it to E. Furthermore, given an embedding $\sigma : E \to \overline{k}$ extending the identity on k, there are exactly e embeddings $\iota_1^\sigma, \dots \iota_e^\sigma$ of F into $\overline{E} = \overline{k}$ extending σ, by the definition of the separable degree of F over E. If $\mathscr{C}$ denotes the set of the d embeddings of E into $\overline{k}$ lifting id_k, we conclude that the distinct embeddings of F into $\overline{k}$ lifting id_k are given by the following disjoint union:

$$\bigcup_{\sigma \in \mathscr{C}} \{\iota_1^\sigma, \dots, \iota_e^\sigma\}. \tag{*}$$

This fact will be used below.

We will prove the result only for the norm; the argument for the trace is very similar. If $\sigma \in \mathscr{C}$ and $\alpha \in F$, let's compute the following product:

$$\prod_{j=1}^{e} \iota_j^\sigma(\alpha).$$

Realizing E in $\overline{k} = \overline{E}$ via σ, Exercise 4.19 tells us that the product above equals to $N_{E \subseteq F}(\alpha)$. However, by the definition given in Exercise 1.12, the norm of α must be in E, while this product is computed in $\overline{k}$. If we were not dealing with different embeddings of E into $\overline{k}$, it would be fine to say that the product equals to $N_{E \subseteq F}(\alpha)$, but, in our case, it is more precise to say that it equals to $\sigma(N_{E \subseteq F}(\alpha))$ because we are realizing E into $\overline{k}$ through σ and not another embedding.

Finally, (*) and Exercise 4.19 implies that

$$N_{k \subseteq F}(\alpha) = \prod_{\sigma \in \mathscr{C}} \prod_{j=1}^{e} \iota_j^\sigma(\alpha) = \prod_{\sigma \in \mathscr{C}} \sigma(N_{E \subseteq F}(\alpha)) = N_{k \subseteq E}(N_{E \subseteq F}(\alpha)),$$

as desired. Note that, this time, there is no ambiguity about the equality of the norms and the products above because we are dealing with only one fixed embedding of k in $\overline{k}$. ■

EXERCISE 4.22

■ SOLUTION A ■

EXERCISE 5.1

■ SOLUTION G ■

EXERCISE 5.2

■ SOLUTION T ■

EXERCISE 5.3 ▷ Find an explicit isomorphism

$$\frac{\mathbb{F}_2[x]}{(x^3+x^2+1)} \xrightarrow{\sim} \frac{\mathbb{F}_2[x]}{(x^3+x+1)}.$$

[§5.1]

■ SOLUTION Let $f : \mathbb{F}_2[x] \to \mathbb{F}_2[x]$ be the function given by $f(p(x)) = p(x+1)$. It follows from Example III.2.3 and Exercise III.2.6 that f is a homomorphism and, since it is bijective, it is indeed an isomorphism. In particular, $\pi \circ f$ is a surjective homomorphism onto $\mathbb{F}_2/(x^3+x+1)$ and so Theorem III.3.8 gives us an isomorphism

$$\varphi : \frac{\mathbb{F}_2[x]}{\ker(\pi \circ f)} \longrightarrow \frac{\mathbb{F}_2[x]}{(x^3+x+1)}.$$

It remains to show that $\ker(\pi \circ f)$ is generated by x^3+x^2+1. Firstly, note that $\ker(\pi \circ f)$ is different from $\mathbb{F}_2[x]$ because $\pi \circ f$ is not trivial. Since x^3+x^2+1 is irreducible in $\mathbb{F}_2[x]$, which is a PID, it suffices to show that this polynomial is in $\ker(\pi \circ f)$. Indeed:

$$\begin{aligned} f(x^3+x^2+1) &= (x+1)^3+(x+1)^2+1 \\ &= (x^3+x^2+x+1)+(x^2+1)+1 \\ &= x^3+x+1 \end{aligned}$$

and thus

$$(\pi \circ f)(x^3+x^2+1) = 0,$$

as desired. ■

EXERCISE 5.4

■ SOLUTION A ■

EXERCISE 5.5

■ SOLUTION G ■

EXERCISE 5.6

■ SOLUTION T ■

EXERCISE 5.7 Let p be a prime integer. View the Frobenius automorphism $\varphi : \mathbb{F}_{p^d} \to \mathbb{F}_{p^d}$ as a linear transformation of the $\mathbb{F}_p$-vector space $\mathbb{F}_{p^d}$. Find the rational canonical form of φ. (Adapt the proof

of Proposition 5.8 to show that the minimal polynomial of φ is $x^d - 1$.)

■ SOLUTION Let $m_\varphi(x)$ be the minimal polynomial of $\varphi(x)$, viewed as a linear transformation of the $\mathbb{F}_p$-vector space $\mathbb{F}_{p^d}$. Since every element of $\mathbb{F}_{p^d}$ is a root of the polynomial $x^{p^d} - x$, we have that $\varphi^d - \mathrm{id}_{\mathbb{F}_{p^d}} = 0$ and so $m_\varphi(x)$ divides $x^d - 1$. On the other hand, if

$$m_\varphi(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

every element of $\mathbb{F}_{p^d}$ is also a root of

$$x^{p^n} + a_{n-1}x^{p^{n-1}} + \cdots + a_1 x^p + a_0 x,$$

because

$$\begin{aligned} & c^{p^n} + a_{n-1}c^{p^{n-1}} + \cdots + a_1 c^p + a_0 c \\ &= (\varphi^n + a_{n-1}\varphi^{n-1} + \cdots + a_1\varphi + a_0 \,\mathrm{id}_{\mathbb{F}_{p^d}})(c) \\ &= (m_\varphi(\varphi))(c) \\ &= 0 \end{aligned}$$

for all $c \in \mathbb{F}_{p^d}$. Thus, Lemma V.5.1 implies $p^d \leq p^n$ and so $d \leq n$. Since the degree of $x^d - 1$ is d, we conclude that $m_\varphi(x) = x^d - 1$. Finally, note that $[\mathbb{F}_{p^d} : \mathbb{F}_p] = d$ and, therefore, it follows that the rational canonical form of φ is the companion matrix of $m_\varphi(x)$, that is,

$$\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix}$$

is the desired matrix. ■

EXERCISE 5.8

■ SOLUTION A ■

EXERCISE 5.9

■ SOLUTION G ■

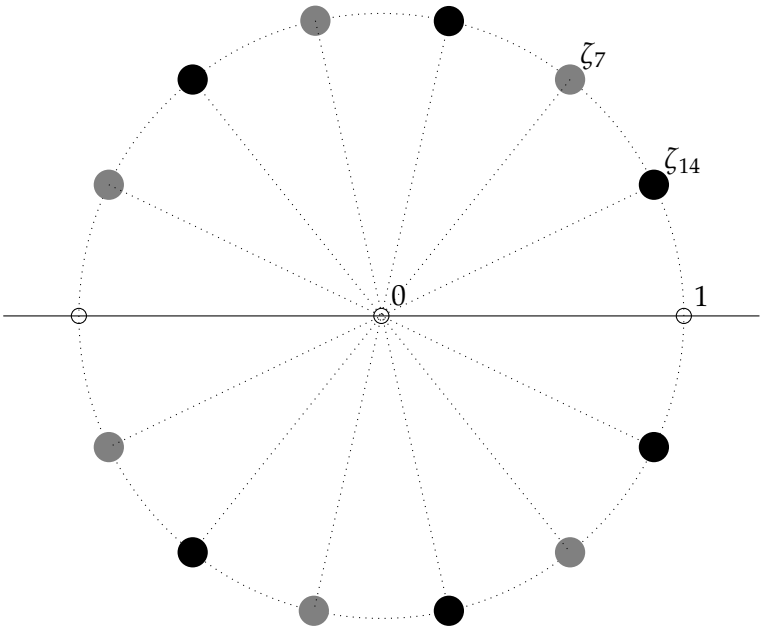
EXERCISE 5.10

■ SOLUTION T ■

EXERCISE 5.11 Prove that if $n > 1$ is odd, then $\Phi_{2n}(x) = \Phi_n(-x)$. (Hint: Draw the primitive 14-th roots of 1 side-by-side to the prim-

itive 7-th roots of 1; then go back to Exercise II.2.15 to justify the fact you observe.)

■ SOLUTION This is the picture of the hint:



The gray and black dots are, respectively, the primitive 7-th and 14-th roots of 1. Note that there is the same number of them and that they are opposite to each other. As will now prove, these facts generalize for any odd integer $n > 1$.

Let α be a primitive n-th root of 1, that is, $\alpha = \zeta_n^m$ with $\gcd(m, n) = 1$. We claim that $-\alpha$ is a primitive $2n$-th root of 1. Indeed, note that

$$-\alpha = (-1) \cdot \alpha = (\zeta_{2n}^n)(\zeta_{2n}^2)^m = \zeta_{2n}^{2m+n}$$

and, since $\gcd(2m + n, 2n) = 1$ by Exercise II.2.15, our claim follows. This implies that $\Phi_n(-x)$ divides $\Phi_{2n}(x)$ because every root of the first polynomial is also a root of the second one. Again by Exercise II.2.15, we have that $\phi(n) = \phi(2n)$ and so $\Phi_n(x)$ and $\Phi_{2n}(x)$ are of the same degree. Finally, since $n \geq 3$, $\phi(n)$ is even (this can be easily derived from the formula in Exercise V.6.8), which implies that $\Phi_n(-x)$ is monic, just as $\Phi_{2n}(x)$ is. From these observations we conclude that $\Phi_{2n}(x) = \Phi_n(-x)$. ■

EXERCISE 5.12

■ SOLUTION A ■

EXERCISE 5.13

■ SOLUTION G ■

EXERCISE 5.14

■ SOLUTION T ■

EXERCISE 5.15 ▷ Let a, p, n be integers, with p, n positive and p prime, $p \nmid n$.

- Show that $x^n - 1$ has no multiple roots modulo p.
- Show that if p divides $\Phi_n(a)$, then $a^n \equiv 1$ modulo p. (In particular, $p \nmid a$, so $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^*$.)
- Show that if p divides $\Phi_n(a)$, then $a^d \not\equiv 1$ modulo p for every $d < n$.
- Deduce that $p \mid \Phi_n(a)$ if and only if the order of $[a]_p$ in $(\mathbb{Z}/p\mathbb{Z})^*$ is n.
- Compute $\Phi_{15}(9)$, and show that it is divisible by 31. Then look back at the first part of Exercise II.4.12.

[§II.4.3, 5.16, 5.17]

■ SOLUTION

- Consider the polynomial $f(x) = x^n - 1$ in $\mathbb{F}_p$. Note that $f'(x) = nx^{n-1}$ and, since $p \nmid n$, $f'(x)$ is not the zero polynomial. It follows that the only non-constant factors (up to associates) of $f'(x)$ are the powers of x, which clearly do not divide $f(x)$. Thus, $f(x)$ and $f'(x)$ are relatively prime and Lemma 4.13 implies that $f(x)$ has no multiple roots.
- Since $\Phi_n(x)$ divides $x^n - 1$, we have that $\Phi_n(a)$ divides $a^n - 1$. Therefore, p divides $a^n - 1$, that is, $a^n \equiv 1$ modulo p.
- FALTA ESSE ITEM.
- If p divides $\Phi_n(a)$, the last two items imply that the order of $[a]_p$ in $(\mathbb{Z}/p\mathbb{Z})^*$ is n. Conversely, if $[a]_p$ is of order n in the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$, the 'only if' part we just proved implies that $p \nmid \Phi_d(a)$ for all $d < n$ such that d divides p, because, otherwise, the order of $[a]_p$ would not be n. By Lemma 5.11,

$$\prod_{1 \le d \mid n} \Phi_d(a) = a^n - 1 \equiv 0 \mod p$$

  and p divides the product above. By our previous observation, we must have $p \mid \Phi_n(a)$.
- By Exercise 5.9,

$$\Phi_{15} = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1,$$

thus,

$$\Phi_{15}(9) = 38316961 = 31 \cdot 1236031$$

is divisible by 31. Since $31 \nmid 15$, the last item implies that the order of $[9]_{31}$ in $(\mathbb{Z}/31\mathbb{Z})^*$ is 15, the same that we obtained in the first part of Exercise II.4.12. ∎

EXERCISE 5.16

∎ SOLUTION A ∎

EXERCISE 5.17

∎ SOLUTION G ∎

EXERCISE 5.18

∎ SOLUTION T ∎

EXERCISE 5.19 ▷ Prove that the regular n-gon can be constructed by straightedge and compass only if $n = 2^m p_1 \cdots p_r$, where $m \geq 0$ and the factors p_i are distinct Fermat primes. (Hint: Use Exercise V.6.8.) [§5.2, §7.2]

∎ SOLUTION Let $n > 1$ be an integer such that the regular n-gon can be constructed by straightedge and compass. As argued just after Example 5.17, $\phi(n)$ must be a power of 2. Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the prime factorization of n. By Exercise V.6.8, we know that

$$\phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_r^{\alpha_r - 1}(p_r - 1).$$

Thus, since $(p_i - 1) \mid \phi(n)$ for all i, each p_i is of the form $2^k + 1$ for some integer k. In particular, Exercise 3.15 implies that every odd prime divisor of n is a Fermat prime. Furthermore, if p_i is odd, it cannot divide $\phi(n)$ and so $\alpha_i = 1$. We conclude that n is of the desired form. ∎

EXERCISE 5.20

∎ SOLUTION A ∎

EXERCISE 5.21

∎ SOLUTION G ∎

EXERCISE 5.22

∎ SOLUTION T ∎

EXERCISE 5.23 ▷ Let k be a field, and let $n > 0$ be an integer. Assume that there are no irreducible polynomials of degree n in $k[x]$. Prove that there are no separable extensions of k of degree n. [§7.1]

■ SOLUTION Suppose that there exists a separable extension F of k of degree n. Since the extension is finite, Proposition 5.19 implies that $F = k(\alpha)$ for some $\alpha \in F$. It follows that the minimal polynomial of α is an irreducible polynomial of degree n in $k[x]$. ■

6 A LITTLE GALOIS THEORY

EXERCISE 6.1

■ SOLUTION A ■

EXERCISE 6.2

■ SOLUTION G ■

EXERCISE 6.3

■ SOLUTION T ■

EXERCISE 6.4 ▷ Let $k \subseteq E$ be a finite separable extension. Prove that E may be identified with an intermediate field of a Galois extension $k \subseteq F$ of k.

In fact, prove that there is a *smallest* such extension $k \subseteq F$, in the sense that if $k \subseteq E \subseteq K$, with $k \subseteq K$ Galois, then there exists an embedding of F in K which is the identity on E. (The extension $k \subseteq F$ is the *Galois closure* of the extension $k \subseteq E$. It is clearly uniquely determined up to isomorphism.) [§6.3, 6.5]

■ SOLUTION R ■

EXERCISE 6.5

■ SOLUTION A ■

EXERCISE 6.6

■ SOLUTION G ■

EXERCISE 6.7

■ SOLUTION T ■

EXERCISE 6.8 Let $k \subseteq F$ be a Galois extension of degree n, and let E be an intermediate field. Assume that $[E : k]$ is the smallest prime dividing n. Prove that $k \subseteq E$ is Galois.

■ SOLUTION R ■

EXERCISE 6.9

■ SOLUTION A ■

EXERCISE 6.10

■ SOLUTION G ■

EXERCISE 6.11

■ SOLUTION T ■

EXERCISE 6.12 Find two algebraic extensions $k \subseteq F$, $k \subseteq K$ and embeddings $F \subseteq \bar{k}$, $\sigma_1 : K \subseteq \bar{k}$, $\sigma_2 : K \subseteq \bar{k}$ extending $k \subseteq \bar{k}$, such that the composites $F\sigma_1(K)$, $F\sigma_2(K)$ are *not* isomorphic.

Prove that no such example exists if F and K are Galois over k.

■ SOLUTION R ■

EXERCISE 6.13

■ SOLUTION A ■

EXERCISE 6.14

■ SOLUTION G ■

EXERCISE 6.15

■ SOLUTION T ■

EXERCISE 6.16 ▷ Let $k \subseteq F$ be a cyclic Galois extension of degree d, and let φ be a generator of $\mathrm{Aut}_k(F)$. Let $\alpha \in F$ be an element such that $N_{k\subseteq F}(\alpha) = 1$.

- Prove that the automorphisms $\mathrm{id}_F, \varphi, \dots, \varphi^{d-1}$ are linearly independent over F. (Exercise 6.14.)
- Prove that there exists a $\gamma \in F$ such that

$$\begin{aligned}\beta :=& \gamma + \alpha\varphi(\gamma) + \alpha\varphi(\alpha)\varphi^2(\gamma) + \cdots \\ &\cdots + \alpha\varphi(\alpha)\cdots\varphi^{d-2}(\alpha)\varphi^{d-1}(\gamma) \neq 0.\end{aligned}$$

- Prove that $\alpha\varphi(\alpha)\varphi^2(\alpha)\cdots\varphi^{d-1}(\alpha)\varphi^d(\gamma) = \gamma$, and deduce that $\alpha = \beta/\varphi(\beta)$.

Together with the result of Exercise 4.20, the conclusion is that an element α of a cyclic Galois extension as above has norm 1 if *and only if* there exists a β such that $\alpha = \beta/\varphi(\beta)$.

This is *Hilbert's theorem 90* (the 90-th theorem in Hilbert's *Zahlbericht*, a report on the state of number theory at the end of the nineteenth century commissioned by the German Mathematical Society). [6.17, §IX.7.6, IX.7.18]

■ SOLUTION R ■

EXERCISE 6.17

■ SOLUTION A ■

EXERCISE 6.18

■ SOLUTION G ■

EXERCISE 6.19

■ SOLUTION T ■

7 SHORT MARCH THROUGH APPLICATIONS OF GALOIS THEORY

EXERCISE 7.1

■ SOLUTION R ■

EXERCISE 7.2

■ SOLUTION A ■

EXERCISE 7.3

■ SOLUTION G ■

EXERCISE 7.4

■ SOLUTION T ■

EXERCISE 7.5

■ SOLUTION R ■

EXERCISE 7.6

■ SOLUTION A ■

EXERCISE 7.7

■ SOLUTION G ■

EXERCISE 7.8

■ SOLUTION T ■

EXERCISE 7.9

■ SOLUTION R ■

EXERCISE 7.10

■ SOLUTION A ■

EXERCISE 7.11

■ SOLUTION G ■

EXERCISE 7.12

■ SOLUTION T ■

EXERCISE 7.13

■ SOLUTION R ■

EXERCISE 7.14

■ SOLUTION A ■

EXERCISE 7.15

■ SOLUTION G ■

EXERCISE 7.16

■ SOLUTION T ■

EXERCISE 7.17

■ SOLUTION R ■

EXERCISE 7.18

■ SOLUTION A ■

EXERCISE 7.19

■ SOLUTION G ■

VIII

LINEAR ALGEBRA, REPRISE

IX

HOMOLOGICAL ALGEBRA