Solutions for Selected Problems from Aluffi's *Algebra: Chapter 0*

June 4, 2025

Contents

Chapter I

Preliminaries: Set theory and categories

1 Naive set theory

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

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

1.3 Given a partition $\mathcal{P}$ on a set S, show how to define an equivalence relation $\sim$ on S such that $\mathcal{P}$ is the corresponding partition. [§1.5]

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

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

Consider, on the set

$$S = \{1, 2, 3\}$$

the relation

$$R = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (2, 3), (3, 2)\}.$$

Note that while R is obviously reflexive and symmetric, it is not transitive. (Since $1R2$ and $2R3$, but $1\not R3$.)

The 'equivalence classes' of R are not disjoint, so a partition of S is not possible.

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]

2 Functions between sets

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

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[13]. [§2.5, V.3.3]

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

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

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]

Solution

The dual notion is as follows: an *epimorphism* is a function $f : A \to B$ such that for any two functions $\alpha', \alpha'' : B \to Z$, if $\alpha' \circ f = \alpha'' \circ f$, then $\alpha' = \alpha''$. The result analogous to Proposition 2.3 is that $f : A \to B$ is an epimorphism if and only if it is surjective.

First assume that f is surjective and $\alpha' \circ f = \alpha'' \circ f$. We must show that for any $b \in B$, $\alpha'(b) = \alpha''(b)$. By surjectivity there exists $a \in A$ such that $f(a) = b$. Then $\alpha'(b) = \alpha'(f(a)) = \alpha''(f(a)) = \alpha''(b)$.

Conversely, assume that f is *not* surjective, so that $\operatorname{im} f$ is not the whole of B. Then we can define functions $\alpha', \alpha'' : B \to \{0, 1\}$ that agree on $\operatorname{im} f$

but differ on some $b \in B \setminus \operatorname{im} f$. Specifically, let $\alpha'(b) = 1$ and $\alpha''(b) = 0$, while α' and α'' agree on all other points in $\operatorname{im} f$. Then $\alpha' \circ f = \alpha'' \circ f$, but $\alpha' \neq \alpha''$, showing that f is not an epimorphism.

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

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

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?)

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

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

Solution

For any $x \in A$, $f(x)$ has $|B|$ possible outputs. Thus, $|B^A| = |B|^{|A|}$, by the fundamental principle of counting.

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]

3 Categories

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

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

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, §VIII.1.1, §IX.1.2, IX.1.10]

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

Solution

By Example 3.2 and Exercise I.2.10, we conclude that $|\mathrm{End}_{\mathsf{Set}}(A)| = n^n$.

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

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

Solution

No, because the relation $<$ is not reflexive. This implies that the identity morphism 1_a cannot be defined for any object a in this category, since there is no element $a \in \mathbb{Z}$ such that $a < a$. In a category, every object must have an identity morphism, which is not the case here.

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

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 $n, m \in \mathbb{N}$. (I 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]

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

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 compositions in C make C' into a category. A subcategory C' is full if $\mathrm{Hom}_{\mathsf{C}'}(A, B) = \mathrm{Hom}_{\mathsf{C}}(A, B)$ for all A, B in $\mathrm{Obj}(\mathsf{C}')$. Construct a category of *infinite sets* and explain how it may be viewed as a full subcategory of Set. [4.4, §VI.1.1, §VIII.1.3]

3.9 An alternative to the notion of *multiset* introduced in §2.2 is obtained by considering sets endowed with equivalence relations; equivalent elements are taken to be multiple instances of elements 'of the same kind'. Define a notion of morphism between such enhanced sets, obtaining a category MSet containing (a 'copy' of) Set as a full subcategory. (There may be more than one reasonable way to do this! This is intentionally an open-ended exercise.) Which objects in MSet determine ordinary multisets as defined in §2.2 and how? Spell out what a morphism of multisets would be from this point of view. (There are several natural notions of morphisms of multisets. Try to define morphisms in MSet so that the notion you obtain for ordinary multisets captures your intuitive understanding of these objects.) [§2.2, §3.2, 4.5]

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, extrapolating the notion of *subset*. 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

The subobject classifier in Set is $\Omega = \{0, 1\}$ (up to isomorphism). Indeed, there is a bijection between subsets (subobjects in the category of sets) $B \subseteq A$ and functions $A \to \Omega$, namely, B corresponds to its indicator function $\chi_B : A \to \Omega$ defined by $\chi_B(a) = 1$ if $a \in B$, and 0 otherwise. This function is a morphism in Set, and every morphism from A to Ω arises in this way from a unique subset of A. Thus, Ω serves as a subobject classifier in Set.

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]

4 Morphisms

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

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

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

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

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

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

Carefully working out the case $n = 5$ is helpful.) [§4.1, §II.1.3]

4.2 In Example 3.3 we have seen how to construct a category from a set endowed with a relation, provided this latter is reflexive and transitive. For what types of relations is the corresponding category a groupoid (cf. Example 4.6)? [§4.1]

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.

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

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!)

5 Universal properties

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

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

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

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

5.5 What are the final objects in the category considered in §5.3? [§5.3]

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]

5.7 Redo Exercise 2.9, this time using Proposition 5.4.

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.)

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.

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.

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 canonical quotient maps $q_A : A \to A/\!\sim_A$, $q_B : B \to B/\!\sim_B$, and $q : A \times B \to (A \times B)/\!\sim_{A\times B}$, and that these induce functions $(A \times B)/\!\sim_{A\times B} \to A/\!\sim_A$ and $(A \times B)/\!\sim_{A\times B} \to B/\!\sim_B$.

- Prove that $(A \times B)/\!\sim_{A\times B}$, together with these induced functions, satisfies the universal property for the product of $A/\!\sim_A$ and $B/\!\sim_B$.
- Conclude (without further work) that $(A\times B)/\!\sim_{A\times B} \cong (A/\!\sim_A)\times(B/\!\sim_B)$.

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]

Chapter II

Groups, first encounter

1 Definition of group

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

Solution

Let G be a group. The corresponding category G consists of a single element $*$, and we define $\mathrm{Hom}_{\mathsf{G}}(*,*) = G$. The composition of morphisms is given by the group operation, and the identity morphism is the identity element of G. This really is a category since:

- The composition of morphisms is associative, since the operation of G is associative.
- The identity morphism is the identity element of G, which acts as the identity for composition.

In fact this is even a groupoid, since every morphism is invertible (again by definition of a group). Finally, what are the isomorphisms of this groupoid G? They are precisely the morphisms $\mathrm{Hom}_{\mathsf{G}}(*,*)$, which is G itself. Thus, every group is indeed the group of isomorphisms of a groupoid.

1.2 Consider the 'sets 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 on the definition of these sets lead to groups (for example, $(\mathbb{R}^*, \cdot)$ is a group; cf. §1.4). [§1.2]

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

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

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

$\bullet$	e	h	$\cdots$
e	e	h	$\cdots$
g	g	$g \bullet h$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\ddots$

(Here e is the identity element. 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!).

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]

1.7 Prove Corollary 1.11.

Solution

We must prove that $N \in \mathbb{Z}$ is a multiple of $|g|$ if and only if $g^N = e$.

For the "only if" direction, $N = k|g|$ for some $k \in \mathbb{Z}$, so

$$g^N = g^{k|g|} = (g^{|g|})^k = e^k = e.$$

For the converse, we have $e = g^N = (g^{|N|})^{\pm 1}$, which implies $e = g^{|N|}$. Then, Lemma 1.10 applies and tells us that $|g|$ divides $|N|$. This means that $\pm N = |N| = k|g|$ for some integer k, thus $N = \pm k|g|$ is a multiple of $|g|$.

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]

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.

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

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.)

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

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

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

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

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 $N = |g||h|$; then $g^N = (h^{-1})^N$. What can you say about this element?) [§1.6, 1.15, §IV.2.5]

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 does not divide $|g|$, then there is a prime integer p such that $|g| = p^m r$, $|h| = p^s s$, 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]

2 Examples of groups

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]

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

2.3 For every positive integer n find an element of order n in S_n.

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.

2.5 Describe generators and relations for all dihedral groups D_{2n}. (Hint: Let r 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[1]. 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 $0 \leq a \leq 1$, $0 \leq b < n$.) [§8.4, §IV.2.5] [2]

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]

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

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

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

2.10 Prove that if $n > 0$, then $\mathbb{Z}/n\mathbb{Z}$ consists of precisely n elements.

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

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?)

[2] Two relations are evident. To 'see' the third one, hold your right hand in front of and away from you, pointing your fingers at the vertices of an imaginary regular pentagon. Flip the pentagon by turning the hand toward you; rotate it counterclockwise w.r.t. the line of sight by 72°; flip it again by pointing it away from you; and rotate it counterclockwise a second time. This returns the hand to the initial position. What does this tell you?

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]

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]

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 $[m]_n \mapsto [2m + n]_{2n}$ 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]

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

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

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.

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 re-ordering of the elements will make them match. (Cf. Exercise 1.6.) [§4.3]

3 The category Grp

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 obvious way with the natural projections.

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

3.2 Let $\varphi : G \to H$, $\psi : H \to K$ 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 is part of the commutativity of the diagram displayed in §3.2.)

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

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?)

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

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]

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.)

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

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.)

4 Group homomorphisms

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 $m \mid n$ necessary? [§4.1]

4.2 Show that the homomorphism $\pi_4 \times \pi_4 \colon C_4 \to C_2 \times C_2$ is not an isomorphism. In fact, is there any isomorphism $C_4 \to C_2 \times C_2$?

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]

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.)

4.5 Prove that the groups $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ are isomorphic.

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?

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.

4.8 Let G be a group, and let $g \in G$. Prove that the function $\gamma_g : G \to G$ defined by $(\forall a \in G) : \gamma_g(a) = gag^{-1}$ 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 a homomorphism. Prove that this homomorphism is trivial if and only if G is abelian. [6.7, 7.11, IV.1.5]

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]

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]

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 $|h|$ divides $|g|$ for all $h \in G$. Therefore...) [§4.3, 4.15, 4.16, §IV.6.3]

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]

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]

4.14 Prove that the order of the group of automorphisms of a 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]

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 4.11.) [IV.5.12]

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

$$(p-1)! \equiv -1 \pmod{p}.$$

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

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

4.18 Prove the second part of Proposition 4.8.

5 Free groups

5.1 Does the category $\mathscr{F}^A$ defined in §5.2 have final objects? If so, what are they?

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 in 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 $A = \emptyset$).

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]

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]

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

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]

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

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

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

5.10 Let $F = F^{\mathrm{ab}}(A)$.

- Define an equivalence relation $\sim$ on F by setting $f' \sim f$ if and only if $f - f' = 2g$ for some $g \in F$. Prove that $F/\sim$ is a finite set if and only if A is finite, and in that case $|F/\sim| = 2^{|A|}$.
- Assume $F^{\mathrm{ab}}(B) \cong F^{\mathrm{ab}}(A)$. If A is finite, prove that B is also, and that $A \cong B$ as sets. (This result holds for free groups as well, and without any finiteness hypothesis. See Exercises 7.13 and VI.1.20.)

[7.4, 7.13]

6 Subgroups

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 I.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[3] 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]

6.2 Prove that the set of 2×2 matrices

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

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]

6.3 Prove that every matrix in $\mathrm{SU}(2)$ may be written in the form

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

[3] If you are not familiar with some of these notions, that's ok: leave this exercise and similar ones alone if that is the case. We will come back to linear algebra and matrices in Chapter VI and following.

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]

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]

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.

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.

6.7 Show that inner automorphisms (cf. Exercise 4.8) form a subgroup of $\mathrm{Aut}(G)$. This subgroup is denoted $\mathrm{Inn}(G)$. Prove that $\mathrm{Inn}(G)$ is cyclic if and only if $\mathrm{Inn}(G)$ is trivial if and only if G is abelian. (Hint: Assume that $\mathrm{Inn}(G)$ is cyclic; with notation as in Exercise 4.8, this means that there exists an element $a \in G$ such that $\forall g \in G \exists k \in \mathbb{Z} : \gamma_g = \gamma_a^k$. In particular, $gag^{-1} = a^k a^{-k}$. Thus a commutes with every g in G. Therefore....) Deduce that if $\mathrm{Aut}(G)$ is cyclic, then G is abelian. [7.10, IV.1.5]

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

$$\mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \to G$$

for some n.

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

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

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

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

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

(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 $\mathrm{SL}_2(\mathbb{Z})$, it 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 $\begin{pmatrix} 1 \\ -q \end{pmatrix}$ are in H, and note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b - qa \\ c & d - qc \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} = \begin{pmatrix} a - bq & b \\ c - dq & d \end{pmatrix}.$$

Note that if c and d are both nonzero, one of these two operations may be used to decrease 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]

6.11 Since direct sums are coproducts in Ab, the classification 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 is may be tempted to conjecture that every finitely generated group is a coproduct of cyclic groups in Grp. Show that this is not the case, by proving that S_3 is not a coproduct of cyclic groups.

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

$$(m, n) = d\mathbb{Z}$$

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

6.13 Draw and compare the lattices of subgroups of $C_2 \times C_2$ and C_4. Draw the lattice of subgroups of S_3, and compare it with the one for C_6. [7.1]

6.14 If m is a positive integer, denote by $\phi(m)$ the number of positive integers $r \leq m$ that are relatively prime 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 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]

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]

6.16 Counterpoint 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]

7 Quotient groups

7.1 List all subgroups of S_3 (cf. Exercise 6.13) and determine which subgroups are normal and which are not normal. [§7.1]

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

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

7.4 Prove that the relation defined in Exercise 5.10 on a free abelian group $F = F^{\mathrm{ab}}(A)$ is compatible with the group structure. Determine the quotient $F/\sim$ as a better known group.

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 $\mathrm{PSL}_2(\mathbb{Z})$ and is called the *modular group*; it is 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

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

(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]

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.

7.7 Let G be a group, n a positive integer, and let $H \subseteq G$ be the subgroup generated by all elements of order n in G. Prove that H is normal.

7.8 Prove Proposition 7.6. [§7.3]

7.9 State and prove the 'mirror' statements of Propositions 7.4 and 7.6, leading to the description of relations satisfying (††).

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]

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* of 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, $g \cdot aba^{-1}b^{-1} \cdot g^{-1} = \gamma_g(a)\gamma_g(b)\gamma_g(a)^{-1}\gamma_g(b)^{-1}$.) Prove that $G/[G,G]$ is commutative. [7.12, §IV.3.3]

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 $F/[F,F] \cong F^{\mathrm{ab}}(A)$. (Use Proposition I.5.4.) [§6.4, 7.13, VI.1.20]

7.13 Let A, B be sets and $F(A), F(B)$ the corresponding free groups. Assume $F(A) \cong F(B)$. 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]

7.14 Let G be a group. Prove that $\mathrm{Inn}(G)$ is a normal subgroup of $\mathrm{Aut}(G)$.

8 Canonical decomposition and Lagrange's theorem

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 follow that $G_1 \cong G_2$? Give a proof or a counterexample.

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]

8.3 Prove that every finite group is finitely presented.

8.4 Prove that (a, b^2, ab) is a presentation of the dihedral group D_{2n}. (Hint: With respect to the generators defined in Exercise 2.5, set $a = x$ and $b = y$; prove you can get the relations given here from the ones you obtained in Exercise 2.5, and conversely.)

8.5 Let a, b be distinct elements of order 2 in a group G, and assume that ab has finite order $n \geq 2$. Prove that the subgroup generated by a and b in G is isomorphic to the dihedral group D_{2n}. (Use the previous 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 3.3 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]

8.7 Let $(A, \mathfrak{R})$, resp. $(A', \mathfrak{R}')$, 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

$$(A \cup A' \mid \mathfrak{R} \cup \mathfrak{R}')$$

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]

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]

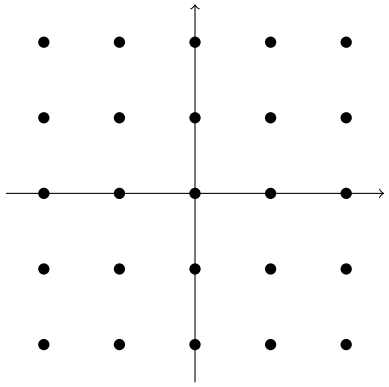
8.9 (Ditto.) Prove that $\mathrm{SO}_3(\mathbb{R}) \cong \mathrm{SU}(2)/\{\pm I_2\}$, where I_2 is the identity matrix. (Hint: It so happens that every matrix in $\mathrm{SO}_3(\mathbb{R})$ can be written in the form

$$\begin{pmatrix} a^2+b^2-c^2-d^2 & 2(bc-ad) & 2(bd+ac) \\ 2(bc+ad) & a^2-b^2+c^2-d^2 & 2(cd-ab) \\ 2(bd-ac) & 2(cd+ab) & a^2-b^2-c^2+d^2 \end{pmatrix}$$

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]

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 1.1.6.)

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.

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.

8.13 Let G be a finite group, and assume $|G|$ is odd. Prove that every element of G is a square. [8.14]

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 $G \to G, g \mapsto g^k$ is surjective.

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.)

8.16 Prove 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.)

8.17 Assume G is a finite abelian group, and let p be a prime divisor of $|G|$. Prove that there exists an element in G of order p. (Hint: Let $g \neq e$ be an element of

G, and consider the subgroup $\langle g\rangle$; use the fact that this subgroup 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]

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?

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 of order d? Give a proof or a counterexample.

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]

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, §IV.4.4]

8.22 Let $\varphi : G \to G'$ be a group homomorphism, and let N be the smallest normal subgroup containing $\operatorname{im}\varphi$. Prove that G'/N satisfies the universal property of coker φ in Grp. [§8.6]

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]

8.24 Show that epimorphisms in Grp do not necessarily have right-inverses. [§I.4.2]

8.25 Let H be a commutative normal subgroup of G. Construct an interesting homomorphism from G/H to $\operatorname{Aut}(H)$. (Cf. Exercise 7.10.)

9 Group actions

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 v returns a column n-vector Mv, 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.)

9.2 The effect of the matrices

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

on the plane is to respectively flip the plane about the x-axis and to rotate it 90° clockwise about the origin. With this in mind, construct an action of D_8 on $\mathbb{R}^2$.

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 $G^\circ \to S_A$ (with the convention for S_A adopted in this section, see the beginning of §9.2), 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 $(g, a) \mapsto ga$ 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.)

9.4 As mentioned in the text, right-multiplication defines a right-action of a group on itself. Find another natural right-action of a group on itself.

9.5 Prove that the action by left-multiplication of a group on itself is free.

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.

9.7 Prove that stabilizers are indeed subgroups.

9.8 For G a group, verify that G-Set is indeed a category, and verify that the isomorphisms in G-Set are precisely the equivariant bijections.

9.9 Prove that G-Set has products and coproducts and that every 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.

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.)

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 $\operatorname{Ker}\sigma$ is (isomorphic to) a subgroup of S_p. What does this say about the index of $\operatorname{Ker}\sigma$ in G?
- Show that $\operatorname{Ker}\sigma \subseteq H$.
- Conclude that $H = \operatorname{Ker}\sigma$, by index considerations.

Thus H is a kernel, proving that it is normal. (This exercise generalizes the result of Exercise 8.2.) [9.12]

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]

9.13 Prove 'by hand' that for all subgroups H of a group G and $\forall g \in G$, G/H and $G/(gHg^{-1})$ (endowed with the action of G by left-multiplication) are isomorphic in G-Set. [§9.3]

9.14 Prove that the modular group $\mathrm{PSL}_2(\mathbb{Z})$ is isomorphic to the coproduct $C_2 * C_3$. (Recall that the modular group $\mathrm{PSL}_2(\mathbb{Z})$ is generated by $x = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Exercise 7.5). The task is to prove that x and y satisfy no other relation: this will show that $\mathrm{PSL}_2(\mathbb{Z})$ is presented by $(x, y \mid x^2, y^3)$, and we have agreed that this is a presentation for $C_2 * C_3$ (Exercise 3.8 or 8.7). Reduce this to verifying that no products $(y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x)$ or $(y^{\pm 1}x)(y^{\pm 1}x)\cdots(y^{\pm 1}x)y^{\pm 1}$ with one or more factors can equal the identity. This latter verification is traditionally carried out by cleverly exploiting an action[4] on the set of irrational real numbers by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} r = \frac{ar + b}{cr + d}$$

Check that this does define an action of $\mathrm{PSL}_2(\mathbb{Z})$, and note that

$$y(r) = 1 - \frac{1}{r}, \quad y^{-1}(r) = 1 - \frac{1}{r'}, \quad yx(r) = 1 + \frac{1}{r'}, \quad y^{-1}x(r) = \frac{1}{r}$$

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]

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]

9.17 Consider G as a G-set, by acting with left-multiplication. Prove that $\mathrm{Aut}_{G\text{-}\mathsf{Set}}(G) \cong G$. [§2.1]

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 groupoid. What will be the morphisms?)

[4] The modular group acts on $\mathbb{C} \cup \{\infty\}$ by Möbius transformations. The observation that it suffices to act on $\mathbb{R} \setminus \mathbb{Q}$ for the purpose of this verification is due to Roger Alperin.

10 Group objects in categories

10.1 Define all the unnamed maps appearing in the diagrams in the definition of group object, and prove 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.)

10.2 Show that groups, as defined in §1.2, are 'group objects in the category of sets'. [§10.1]

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.)

10.4 Prove that every abelian group has exactly one structure of group object in the category Ab.

10.5 By the previous exercise, a group object in Ab is nothing other than an abelian group. What is a group object in Grp?

Chapter III

Rings and modules

6 Products, coproducts, etc., in R-Mod

6.1

7 Complexes and homology

7.1

Chapter IV

Groups, second encounter

1 The conjugation action

1.1

2 The Sylow theorems

2.1

3 Composition series and solvability

3.1

4 The symmetric group

4.1

5 Products of groups

5.1

6 Finite abelian groups

6.1