Huyi Chen

July 30, 2020

Algebra, Chapter 0

By Paolo Aluffi

Contents

Notation for Problems

$\triangleright$: those problems that are directly referenced from the text.

$\neg$: those problems that are referenced from other problems.

[§II.8.1]: related to the text in II.8.1 (Chapter II Section 8 Subsection 1).

[II.8.10]: related to the Definition/Example/Proposition/Lemma/Corollary/Claim 8.10 in Chapter II (the 10th Definition/Example/Proposition/Lemma/Corollary/Claim in Chapter II Section 8).

Acknoledgement

It is kind of Shane Creighton-Young to share his solutions to Paolo Aluffi's "Algebra: Chapter 0" [1] on the Github website `https://github.com/srcreigh/aluffi`. He takes the credit for the first two chapters of this manuscript.

Contact

Github: `https://github.com/hooyuser/Solution-to-Algebra-Chapter-0`
E-mail: `hooyuser@outlook.com`

License

Chapter I. Preliminaries: Set theory and categories

§1. Naive Set Theory

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

Recall that, in naive set theory, any collection of objects that satisfy some property can be called a set. Russel's paradox can be illustrated as follows. Let R be the set of all sets that do not contain themselves. Then, if $R \notin R$, then by definition it must be the case that $R \in R$; similarly, if $R \in R$ then it must be the case that $R \notin R$. ■

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]

Let S be a set with an equivalence relation $\sim$. Consider the family of equivalence classes w.r.t. $\sim$ over S:

$$\mathscr{P}_\sim = \{[a]_\sim \mid a \in S\}$$

Let $[a]_\sim \in \mathscr{P}_\sim$. Since $\sim$ is an equivalence relation, by reflexivity we have $a \sim a$, so $[a]_\sim$ is nonempty. Now, suppose a and b are arbitrary elements in S such that $a \not\sim b$. For contradiction, suppose that there is an $x \in [a]_\sim \cap [b]_\sim$. This means that $x \sim a$ and $x \sim b$. By transitivity, we get that $a \sim b$; this is a contradiction. Hence the $[a]_\sim$ are disjoint. Finally, let $x \in S$. Then $x \in [x]_\sim \in \mathscr{P}_\sim$. This means that

$$\bigcup_{[a]_\sim \in \mathscr{P}_\sim} [a]_\sim = S,$$

that is, the union of the elements of $\mathscr{P}_\sim$ is S. ■

1.3 ▷ Given a partition $\mathscr{P}$ on a set S, show how to define a relation $\sim$ such that $\mathscr{P} = \mathscr{P}_\sim$. [§1.5]

Define, for $a, b \in S$, $a \sim b$ if and only if there exists an $X \in \mathscr{P}$ such that $a \in X$ and $b \in X$. We will show that $\mathscr{P} = \mathscr{P}_\sim$.

1. ($\mathscr{P} \subseteq \mathscr{P}_\sim$). Let $X \in \mathscr{P}$; we want to show that $X \in \mathscr{P}_\sim$. We know that X is nonempty, so choose $a \in X$ and consider $[a]_\sim \in \mathscr{P}_\sim$. We need to show that $X = [a]_\sim$. Suppose $a' \in X$ (it may be that $a' = a$.) Since $a, a' \in X$, $a \sim a'$, so $a' \in [a]_\sim$. Now, suppose $a' \in [a]_\sim$. We have $a' \sim a$, so $a' \in X$. Hence $X = [a]_\sim \in \mathscr{P}_\sim$, so $\mathscr{P} \subseteq \mathscr{P}_\sim$.

2. ($\mathscr{P}_\sim \subseteq \mathscr{P}$). Let $[a]_\sim \in \mathscr{P}_\sim$. From exercise I.1.1 we know that $[a]_\sim$ is non-empty. Suppose $a' \in [a]_\sim$. By definition, since $a' \sim a$, there exists a set X such that $a, a' \in X$. Hence $[a]_\sim \subseteq X$. Also, if $a, a' \in X$ (not necessarily distinct) then $a \sim a'$. Therefore, $\mathscr{P}_\sim \subseteq \mathscr{P}$, and with 1. we get that the sets $\mathscr{P}$ and $\mathscr{P}_\sim$ are equal.

■

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

From the definition of an equivalence relation and the solution to problem **I.1.3**, we can see that an equivalence relation on S is equivalent to a partition of S. Thus the number of equivalence relations on S is equal to the number of partitions of S. Since $\{1, 2, 3\}$ is small we can determine this by hand:

$$\mathscr{P}_0 = \{\, \{1, 2, 3\}\, \}$$

$$\mathscr{P}_1 = \{\, \{1\}, \{2\}, \{3\}\}\, \}$$

$$\mathscr{P}_2 = \{\, \{1, 2\}, \{3\}\, \}$$

$$\mathscr{P}_3 = \{\, \{1\}, \{2, 3\}\, \}$$

$$\mathscr{P}_4 = \{\, \{1, 3\}, \{2\}\, \}$$

Thus there can be only 5 equivalence relations defined on $\{1, 2, 3\}$. ■

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.)

For $a, b \in \mathbb{Z}$, define $a \diamond b$ to be true if and only if $|a - b| \leq 1$. It is reflexive, since $a \diamond a = |a - a| = 0 \leq 1$ for any $a \in \mathbb{Z}$, and it is symmetric since $a \diamond b = |a - b| = |b - a| = b \diamond a$ for any $a, b \in \mathbb{Z}$. However, it is not transitive. Take for example $a = 0, b = 1, c = 2$. Then we have $|a - b| = 1 \leq 1$, and $|b - c| = 1 \leq 1$, but $|a - c| = 2 > 1$; so $a \diamond b$ and $b \diamond c$, but not $a \diamond c$.

When we try to build a partition of $\mathbb{Z}$ using $\diamond$, we get "equivalence classes" that are not disjoint. For example, $[2]_\diamond = \{1, 2, 3\}$, but $[3]_\diamond = \{2, 3, 4\}$. Hence $\mathscr{P}_\diamond$ is not a partition of $\mathbb{Z}$.

■

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]

Suppose $a, b, c \in \mathbb{R}$. We have that $a - a = 0 \in \mathbb{Z}$, so $\sim$ is reflexive. If $a \sim b$, then $b - a = k$ for some $k \in \mathbb{Z}$, so $a - b = -k \in \mathbb{Z}$, hence $b \sim a$. So $\sim$ is symmetric. Now, suppose that $a \sim b$ and $b \sim c$, in particular that $b - a = k \in \mathbb{Z}$ and $c - b = l \in \mathbb{Z}$. Then $c - a = (c - b) + (b - a) = l + k \in \mathbb{Z}$, so $a \sim c$. So $\sim$ is transitive.

An equivalence class $[a]_\sim \in \mathbb{R} / \sim$ is the set of integers $\mathbb{Z}$ transposed by some real number $\epsilon \in [0, 1)$. That is, for every set $X \in \mathbb{R} / \sim$, there is a real number $\epsilon \in [0, 1)$ such that every $x \in X$ is of the form $k + \epsilon$ for some integer k.

Now we will show that $\approx$ is an equivalence relation over $\mathbb{R}\times\mathbb{R}$. Supposing $a_1, a_2 \in \mathbb{R}\times\mathbb{R}$, we have $a_1 - a_1 = a_2 - a_2 = 0 \in \mathbb{Z}$, so $(a_1, a_2) \approx (a_1, a_2)$. If we also suppose that $b_1, b_2, c_1, c_2 \in \mathbb{R}\times\mathbb{R}$, then symmetry and transitivity can be shown as well: $(a_1, a_2) \approx (b_1, b_2) \implies b_1 - a_1 = k$ for some integer k and $b_2 - a_2 = l$ for some integer l, hence $a_1 - b_1 = -k \in \mathbb{Z}$ and $a_2 - b_2 = -l \in \mathbb{Z}$, so $(b_1, b_2) \approx (a_1, a_2)$; also if $(a_1, a_2) \approx (b_1, b_2)$ and $(b_1, b_2) \approx (c_1, c_2)$, then $(b_1, b_2) - (a_1, a_2) = (k_1, k_2) \in \mathbb{Z}\times\mathbb{Z}$ as well as $(c_1, c_2) - (b_1, b_2) = (l_1, l_2) \in \mathbb{Z}\times\mathbb{Z}$, so $(c_1, c_2) - (a_1, a_2) = (c_1, c_2) - (b_1, b_2) + (b_1, b_2) - (a_1, a_2) = (k_1 + l_1, k_2 + l_2 \in \mathbb{Z}\times\mathbb{Z}$. Thus $\approx$ is an equivalence relation.

The interpretation of $\approx$ is similar to $\sim$. An equivalence class $X \in \mathbb{R}\times\mathbb{R}/\approx$ is just the 2-dimensional integer lattice $\mathbb{Z}\times\mathbb{Z}$ transposed by some pair of values $(\epsilon_1, \epsilon_2) \in [0,1)\times[0,1)$.

Imaginatively, $\mathbb{R}/\sim$ can be viewed as a ring of length 1 by bending the real line $\mathbb{R}$ and gluing the points in the same equivalence class. Then we can rotate a ring around an axis of rotation to get $\mathbb{R}\times\mathbb{R}/\approx$, which makes a torus. ∎

§2. Functions between sets

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

There are $n!$ different bijections $S \to S$. ∎

§3. Categories

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, §VIII.1.1, §IX.1.2, IX.1.10]

- For every object A of C, there exists one identity morphism $1_A \in \mathrm{Hom}_{\mathsf{C}}(A, A)$. Since $\mathrm{Obj}(\mathsf{C}^{op}) := \mathrm{Obj}(\mathsf{C})$ and $\mathrm{Hom}_{\mathsf{C}^{op}}(A, A) := \mathrm{Hom}_{\mathsf{C}}(A, A)$, for every object A of C^{op}, the identity on A coincides with $1_A \in \mathsf{C}$.

- For A, B, C objects of C^{op} and $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A, B) = \mathrm{Hom}_{\mathsf{C}}(B, A)$, $g \in \mathrm{Hom}_{\mathsf{C}^{op}}(B, C) = \mathrm{Hom}_{\mathsf{C}}(C, B)$, the composition laws in C determines a morphism $f * g$ in $\mathrm{Hom}_{\mathsf{C}}(C, A)$, which deduces the composition defined on C^{op}:

$$\begin{aligned} \mathrm{Hom}_{\mathsf{C}^{op}}(A, B) \times \mathrm{Hom}_{\mathsf{C}^{op}}(B, C) &\longrightarrow \mathrm{Hom}_{\mathsf{C}^{op}}(A, C) \\ (f, g) &\longmapsto g \circ f := f * g \end{aligned}$$

- Associativity. If $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A,B)$, $g \in \mathrm{Hom}_{\mathsf{C}^{op}}(B,C)$, $h \in \mathrm{Hom}_{\mathsf{C}^{op}}(C,D)$, then

$$f \circ (g \circ h) = f \circ (h * g) = (h * g) * f = h * (g * f) = (g * f) \circ h = (f \circ g) \circ h.$$

- Identity. For all $f \in \mathrm{Hom}_{\mathsf{C}^{op}}(A,B)$, we have

$$f \circ 1_A = 1_A * f = f, \quad 1_B \circ f = f * 1_B = f.$$

Thus we get the full construction of C^{op}. ■

3.3 $\triangleright$ 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]

Suppose S is a set, and $\sim$ is a relation on S satisfying the reflexive and transitive property. Then we can encode this data into a category C:

- Objects: the elements of S;
- Morphisms: if a, b are objects (that is: if $a, b \in S$) then let $\mathrm{Hom}(a,b)$ be the set consisting of the element $(a,b) \in S \times S$ if $a \sim b$, and $\mathrm{Hom}(a,b) = \varnothing$. otherwise.

Given the composition of two morphisms

$$\begin{aligned} \mathrm{Hom}_{\mathsf{C}}(A,B) \times \mathrm{Hom}_{\mathsf{C}}(B,C) &\longrightarrow \mathrm{Hom}_{\mathsf{C}}(A,C) \\ (a,b) \circ (b,c) &\longmapsto (a,c) \end{aligned}$$

we are asked to check $1_a = (a,a)$ is an identity with respect to this composition. ■

§4. Morphisms

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]

For a reflexive and transitive relation $\sim$ on a set S, define the category C as follows:

- Objects: $\mathrm{Obj}(\mathsf{C}) = S$;
- Morphisms: if a, b are objects (that is: if $a, b \in S$) then let

$$\mathrm{Hom}_{\mathsf{C}}(a,b) = \begin{cases} (a,b) \in S \times S & \text{if } a \sim b \\ \varnothing & \text{otherwise} \end{cases}$$

In Example 3.3 we have shown the category. If the relation $\sim$ is endowed with symmetry, we have

$$(a,b) \in \mathrm{Hom}_{\mathsf{C}}(a,b) \implies a \sim b \implies b \sim a \implies (b,a) \in \mathrm{Hom}_{\mathsf{C}}(b,a).$$

Since

$$(a,b)(b,a) = (a,a) = 1_a, \quad (b,a)(a,b) = (b,b) = 1_b,$$

in fact (a,b) is an isomorphism. From the arbitrariness of the choice of (a,b), we show that C is a groupoid. Conversely, if C is a groupoid, we can show the relation $\sim$ is symmetric. To sum up, the category C is a groupoid if and only if the corresponding relation $\sim$ is an equivalence relation. ∎

§5. Universal properties

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

An object F of C is final in C if and only if

$$\forall A \in \mathrm{Obj}(\mathsf{C}) : \mathrm{Hom}_{\mathsf{C}}(A, F) \text{ is a singleton.}$$

That is equivalent to

$$\forall A \in \mathrm{Obj}(\mathsf{C}_{op}) : \mathrm{Hom}_{\mathsf{C}_{op}}(F, A) \text{ is a singleton,}$$

which means F is initial in the opposite category C_{op}. ∎

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.

Assume G is a group. Define a category C as follows:

- Objects: $\mathrm{Obj}(\mathsf{C}) = \{*\}$;
- Morphisms: $\mathrm{Hom}_{\mathsf{C}}(*, *) = \mathrm{End}_{\mathsf{C}}(*) = G$.

The composition of homomorphism is corresponding to the multiplication between two elements in G. The identity morphism on $*$ is $1_* = e_G$, which satisfies for all $g \in \mathrm{Hom}_{\mathsf{C}}(*, *)$,

$$ge_G = e_G g = g,$$

and

$$gg^{-1} = e_G,\ g^{-1}g = e_G.$$

Thus any homomorphism $g \in \mathrm{Hom}_{\mathsf{C}}(*, *)$ is an isomorphism and accordingly C is a groupoid. Now we see $G = \mathrm{End}_{\mathsf{C}}(*)$ is the group of isomorphisms of a groupoid. Moreover, supposing that $*$ is an object in some category D, G would be the group of automorphisms of $*$, which is denoted as $\mathrm{Aut}_{\mathsf{D}}(*)$. ∎

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

For all $a, b \in G$,

$$abab = e \implies a(abab)b = ab \implies (aa)ba(bb) = ab \implies ba = ab.$$

∎

§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 $(i, \sigma(i))$ 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.

By introducing the Kronecker delta function

$$\delta_{i,j} = \begin{cases} 0 & \text{if } i \neq j, \\ 1 & \text{if } i = j, \end{cases}$$

the entry at (i, j) of the matrix $M_{\sigma\tau}$ can be written as

$$(M_{\sigma\tau})_{i,j} = \delta_{\tau(\sigma(i)),j}$$

and the entry at (i, j) of the matrix $M_\sigma M_\tau$ can be written as

$$(M_\sigma M_\tau)_{i,j} = \sum_{k=1}^{n} (M_\sigma)_{i,k} (M_\tau)_{k,j} = \sum_{k=1}^{n} \delta_{\sigma(i),k} \cdot \delta_{\tau(k),j} = \sum_{k=1}^{n} \delta_{\sigma(i),k} \cdot \delta_{k,\tau^{-1}(j)} = \delta_{\sigma(i),\tau^{-1}(j)},$$

where the last but one equality holds by the fact

$$\tau(k) = j \iff k = \tau^{-1}(j).$$

Noticing that

$$\tau(\sigma(i)) = j \iff \sigma(i) = \tau^{-1}(j),$$

we see $M_{\sigma\tau} = M_\sigma M_\tau$ for all $\sigma, \tau \in S_n$. ∎

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

The cyclic permutation

$$\sigma = (1\ 2\ 3 \cdots d)$$

is an element of order d in S_n. ∎

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

The cyclic permutation

$$\sigma = (1\ 2\ 3 \cdots n)$$

is an element of order d 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.

The image of n rotations under the homomorphism are

$$\sigma_1 = e_{D_8},\ \sigma_2 = (1\ 2\ 3\ 4),\ \sigma_3 = (1\ 3)(2\ 4),\ \sigma_4 = (1\ 4\ 3\ 2).$$

The image of n reflections under the homomorphism are

$$\sigma_5 = (1\ 3),\ \sigma_6 = (2\ 4),\ \sigma_7 = (1\ 2)(3\ 4),\ \sigma_8 = (1\ 4)(3\ 2).$$

∎

2.11 Prove that the square of every odd integer is congruent to 1 modulo 8.

Given an odd integer $2k+1$, we have

$$(2k+1)^2 = 4k(k+1) + 1,$$

where $k(k+1)$ is an even integer. So $(2k+1)^2 \equiv 1 \mod 8$. ∎

2.12 Prove that there are no nonzero integers a, b, c such that $a^2 + b^2 = 3c^2$. (Hint: 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?)

$$a^2 + b^2 = 3c^2 \implies [a]_4^2 + [b]_4^2 = 3[c]_4^2.$$

Noting that $[0]_4^2 = [0]_4, [1]_4^2 = [1]_4, [2]_4^2 = [0]_4, [3]_4^2 = [1]_4$, we see $[c]_4^2$ must be $[0]_4$ and so do $[a]_4^2$ and $[b]_4^2$. Hence $[a]_4, [b]_4, [b]_4$ can only be $[0]_4$ or $[2]_4$, which justifies letting $a = 2k_1, b = 2l_2, c = 2m_1$. After substitution we have $k^2 + l^2 = 3m^2$. Repeating this process n times yields $a = 2^n k_n, b = 2^n l_n, c = 2^n m_n$. For a sufficiently large number N, the absolute value of k_N, l_N, m_N must be less than 1. Thus we conclude that $a = b = c = 0$ is the unique solution to the equation $a^2 + b^2 = 3c^2$. ∎

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]

Applying corollary 2.5, we have $\gcd(m, n) = 1$ if and only if $[m]_n$ generates $\mathbb{Z}/n\mathbb{Z}$. Hence

$$\gcd(m, n) = 1 \iff a[m]_n = [1]_n \iff [am]_n = [1]_n \iff am + bn = 1.$$

■

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 $\phi(n)$-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]

- Since $2m+n$ is an odd integer, $\gcd(2m+n, 2n) = 1$ is actually equivalent to $\gcd(2m+n, n) = 1$. According to Exercise 2.13,

  $$\gcd(m, n) = 1 \implies am + bn = 1 \implies \frac{a}{2}(2m + n) + \left(b - \frac{a}{2}\right) n = 1.$$

  If a is even, we have shown $\gcd(2m+n, n) = 1$. Otherwise we can let $a' = a+n$ be an even integer and $b' = b - m$. Then it holds that

  $$\frac{a'}{2}(2m + n) + \left(b' - \frac{a'}{2}\right) n = 1,$$

  which also implies $\gcd(2m + n, n) = 1$.

- If $\gcd(r, 2n) = 1$, then r must be an odd integer and accordingly

  $$\gcd(2r - 2n, 4n) = 1 \implies a(2r - 2n) + b(4n) = 1 \implies 4a\frac{r-n}{2} + 4bn = 1,$$

  which is $\gcd(\frac{r-n}{2}, n) = 1$.

- It is easy to check that the function $f : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/2n\mathbb{Z})^*$, $[m]_n \mapsto [2m + n]_{2n}$ is well-defined. The fact

  $$\begin{aligned} f([m_1]_n) = f([m_2]_n) &\implies f([2m_1 + n]_{2n}) = f([2m_2 + n]_{2n}) \\ &\implies (2m_1 + n) - (2m_2 + n) = 2kn \\ &\implies m_1 - m_2 = kn \\ &\implies [m_1]_n = [m_2]_n \end{aligned}$$

indicates that f is injective. For any $[r]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^*$, we have

$$\gcd(r, 2n) = 1 \implies \gcd\left(\frac{r-n}{2}, n\right) = 1 \implies \left[\frac{r-n}{2}\right]_n \in (\mathbb{Z}/n\mathbb{Z})^*,$$

and

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

which indicates that f is surjective. Thus we show f is a bijection.

■

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

$$1238237^{18238456} \equiv 7^{18238456} \equiv (7^4)^{4559614} \equiv 2401^{4559614} \equiv 1 \mod 10,$$

which indicates that the last digit of $1238237^{18238456}$ is 1. ■

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]

Assume that $m - m' = kn$. If $\gcd(m, n) = 1$, for any common divisor d of m' and n

$$d|m',\ d|n \implies d|(m' + kn) \implies d|m \implies d = 1,$$

which means $\gcd(m', n) = 1$. Likewise, we can show $\gcd(m', n) = 1 \implies \gcd(m, n) = 1$ ■

§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

$$(\varphi \times \varphi) : G \times G \longrightarrow H \times H.$$

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]

By the universal property of product in C, there exist a unique morphism $(\varphi\times\varphi) : G\times G \longrightarrow H \times H$ such that the following diagram commutes.

$$\begin{tikzcd}
G \arrow[r, "\varphi"] & H \\
G \times G \arrow[u, "\pi_G"] \arrow[r, "\varphi\times\varphi"] \arrow[d, "\pi_G"'] & H \times H \arrow[u, "\pi_H"'] \arrow[d, "\pi_H"] \\
G \arrow[r, "\varphi"] & H
\end{tikzcd}$$

■

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.)

By the universal property of product in C, there exists a unique morphism

$$(\psi\varphi) \times (\psi\varphi) : G \times G \to K \times K$$

such that the following diagram commutes.

$$\begin{tikzcd}
G \arrow[rr, "\psi\varphi"] & & H \\
G \times G \arrow[u, "\pi_G"] \arrow[d, "\pi_G"'] \arrow[rr, "(\psi\varphi)\times(\psi\varphi)"] & & H \times H \arrow[u, "\pi_H"'] \arrow[d, "\pi_H"] \\
G \arrow[rr, "\psi\varphi"] & & H
\end{tikzcd}$$

As the following commutative diagram tells us the composition

$$(\psi \times \psi)(\varphi \times \varphi) : G \times G \to K \times K$$

can make the above diagram commute,

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[rr, bend left, "\psi\varphi"] & H \arrow[r, "\psi"] & K \\
G \times G \arrow[u, "\pi_G"] \arrow[d, "\pi_G"'] \arrow[r, "\varphi\times\varphi"] & H \times H \arrow[u, "\pi_H"] \arrow[d, "\pi_H"'] \arrow[r, "\psi\times\psi"] & K \times K \arrow[u, "\pi_K"] \arrow[d, "\pi_K"'] \\
G \arrow[r, "\varphi"] \arrow[rr, bend right, "\psi\varphi"'] & H \arrow[r, "\psi"] & K
\end{tikzcd}$$

there must be $(\psi\varphi) \times (\psi\varphi) = (\psi \times \psi)(\varphi \times \varphi)$.

■

3.3 Show that if G, H are abelian groups, then $G \times H$ satisfies the universal property for coproducts in Ab.

Define two monomorphisms:

$$i_G : G \longrightarrow G \times H, \ a \longmapsto (a, 0_H)$$

$$i_H : H \longrightarrow G \times H,\ b \longmapsto (0_G, b)$$

We are to show that for any two homomorphisms $g : G \to M$ and $h : H \to M$ in Ab, the mapping

$$\begin{aligned} \varphi : \quad & G \times H \longrightarrow M, \\ & (a, b) \longmapsto g(a) + h(b) \end{aligned}$$

is a homomorphism and makes the following diagram commute.

$$\begin{tikzcd} G \arrow[d, "i_G"'] \arrow[dr, "g"] & \\ G \times H \arrow[r, "\varphi"] & M \\ H \arrow[u, "i_H"] \arrow[ur, "h"'] & \end{tikzcd}$$

Exploiting the fact that g, h are homomorphisms and M is an abelian group, it is easy to check that φ preserves the addition operation

$$\begin{aligned} \varphi((a_1, b_1) + (a_2, b_2)) &= \varphi((a_1 + a_2, b_1 + b_2)) \\ &= g(a_1 + a_2) + h(b_1 + b_2) \\ &= (g(a_1) + g(a_2)) + (h(b_1) + h(b_2)) \\ &= (g(a_1) + h(b_1)) + (g(a_2) + h(b_2)) \\ &= g(a_1 + b_1) + h(a_2 + b_2) \\ &= \varphi((a_1, b_1)) + \varphi((a_2, b_2)) \end{aligned}$$

and the diagram commutes

$$\varphi \circ i_G(a) = \varphi((a, 0_H)) = g(a) + h(0_H) = g(a) + 0_M = g(a),$$

$$\varphi \circ i_H(b) = \varphi((0_G, b)) = g(0_G) + h(b) = 0_M + h(b) = h(b).$$

To show the uniqueness of the homomorphism φ we have constructed, suppose a homomorphism φ' can make the diagram commute. Then we have

$$\varphi'((a, b)) = \varphi'((a, 0_H) + (0_G, b)) = \varphi'(i_G(a)) + \varphi'(i_H(b)) = g(a) + h(b) = \varphi((a, b)),$$

that is $\varphi' = \varphi$. Hence we show that there exist a unique homomorphism φ such that the diagram commutes, which amounts to the universal property for coproducts in Ab.

■

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?)

Consider the function

$$\begin{aligned}\varphi : \mathbb{Z} \times \mathbb{Z}[x] &\longrightarrow \mathbb{Z}[x] \\ (n, f(x)) &\longmapsto n + xf(x)\end{aligned}$$

Firstly, we can show φ is a homomorphism as follows

$$\begin{aligned}\varphi((n_1, f_1(x)) + (n_2, f_2(x))) &= \varphi((n_1 + n_2, f_1(x) + f_2(x))) \\ &= (n_1 + n_2) + x(f_1(x) + f_2(x)) \\ &= (n_1 + xf_1(x)) + (n_2 + xf_2(x)) \\ &= \varphi(n_1, f_1(x)) + \varphi(n_2, f_2(x)).\end{aligned}$$

Secondly, we are to show φ is a monomorphism. It follows by

$$\varphi(n, f(x)) = n + xf(x) = 0 \implies n = 0,\ f(x) = 0 \implies \ker\varphi = \{(0, 0)\}.$$

Lastly, since given any $f(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{Z}[x]$ we have

$$\varphi\left(a_0, \sum_{n\geq 1} a_n x^{n-1}\right) = a_0 + \sum_{n\geq 1} a_n x^n = f(x),$$

we claim φ is surjective and indeed an isomorphism. Therefore, as a counterexample we have $\mathbb{Z}[x] \cong \mathbb{Z} \times \mathbb{Z}[x]$ where $\mathbb{Z}$ is non-trivial. ∎

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

Consider the additive group of rationals $(\mathbb{Q}, +)$. Assume that φ is a isomorphism between the product $G \times H = \{(a, b) | a \in G, b \in H\}$ and $(\mathbb{Q}, +)$. Note that $\{e_G\} \times H$ and $G \times \{e_H\}$ are subgroups in $G \times H$ and their intersection is the trivial group $\{(e_G, e_H)\}$. It is easy to check that bijection φ satisfies $\varphi(A \cap B) = \varphi(A) \cap \varphi(B)$. So applying the fact we have

$$\varphi(\{(e_G, e_H)\}) = \varphi(\{e_G\} \times H \cap G \times \{e_H\}) = \varphi(\{e_G\} \times H) \cap \varphi(G \times \{e_H\}) = \{0\}.$$

Suppose both $\varphi(\{e_G\} \times H)$ and $\varphi(G \times \{e_H\})$ are nontrivial groups. If $\dfrac{p}{q} \in \varphi(\{e_G\} \times H) - \{0\}$ and $\dfrac{r}{s} \in \varphi(G \times \{e_H\}) - \{0\}$, there must be

$$rp = rq \cdot \frac{p}{q} = ps \cdot \frac{r}{s} \in \varphi(\{e_G\} \times H) \cap \varphi(G \times \{e_H\}),$$

which implies $rp = 0$. Since both $\dfrac{p}{q}$ and $\dfrac{r}{s}$ are non-zero, it leads to a contradiction. Thus without loss of generality we can assume $\varphi(\{e_G\} \times H)$ is a trivial group $\{0\}$. Since φ is isomorphism, we see that for all $h \in H$,

$$\varphi(e_G, h) = \varphi(e_G, e_H) = 0 \iff h = e_H.$$

That is, H is a trivial group. Therefore, we have shown $(\mathbb{Q}, +)$ will never be isomorphic to the direct product of two nontrivial groups. $\blacksquare$

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.

- Monomorphisms $g : C_2 \to S_3$, $h : C_3 \to S_3$ can be constructed as follows:

$$g([0]_2) = e, g([1]_2) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

$$h([0]_3) = e, h([1]_3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, h([2]_3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

- Supposing that $C_2 \times C_3$ is a coproduct of C_2, C_3, there would be a unique group homomorphism $\varphi : C_2 \times C_3 \to S_3$ such that the following diagram commutes

$$\begin{tikzcd}
C_2 \arrow[d, "i_{C_2}"'] \arrow[dr, "g"] & \\
C_2 \times C_3 \arrow[r, "\varphi"] & S_3 \\
C_3 \arrow[u, "i_{C_3}"] \arrow[ur, "h"'] &
\end{tikzcd}$$

In other words, for all $a \in C_2, b \in C_3$,

$$\begin{aligned}
\varphi(a, b) &= \varphi(([0]_2, b) + (a, [0]_3)) = \varphi(([0]_2, b))\varphi((a, [0]_3)) = \varphi(i_{C_3}(b))\varphi(i_{C_2}(a)) = h(b)g(a) \\
&= \varphi((a, [0]_3) + ([0]_2, b)) = \varphi((a, [0]_3))\varphi(([0]_2, b)) = \varphi(i_{C_2}(a))\varphi(i_{C_3}(b)) = g(a)h(b).
\end{aligned}$$

- Since

$$g([1]_2)h([1]_3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$h([1]_3)g([1]_2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

we see $g(a)h(b) \neq h(b)g(a)$ not always holds. The derived contradiction shows that $C_2 \times C_3$ is not a coproduct of C_2, C_3 in Grp.

■

> **3.7** Show that there is a surjective homomorphism $Z * Z \to C_2 * C_3$. ($*$ denotes coproduct in Grp.)

Consider the mapping

$$\begin{aligned} \varphi : \mathbb{Z} * \mathbb{Z} &\longrightarrow C_2 * C_3 \\ x^{m_1} y^{n_1} \cdots x^{m_k} y^{n_k} &\longmapsto x^{[m_1]_2} y^{[n_1]_3} \cdots x^{[m_k]_2} y^{[n_k]_3} \end{aligned}$$

Since

$$\begin{aligned} &\varphi(x^{m_1} y^{n_1} \cdots x^{m_k} y^{n_k} x^{m'_1} y^{n'_1} \cdots x^{m'_{k'}} y^{n'_k}) \\ =&x^{[m_1]_2} y^{[n_1]_3} \cdots x^{[m_k]_2} y^{[n_k]_3} x^{[m'_1]_2} y^{[n'_1]_3} \cdots x^{[m'_k]_2} y^{[n'_k]_3}, \\ =&\varphi(x^{m_1} y^{n_1} \cdots x^{m_k} y^{n_k}) \varphi(x^{m'_1} y^{n'_1} \cdots x^{m'_{k'}} y^{n'_k}) \end{aligned}$$

φ is a homomorphism. It is clear that φ is surjective. Thus we show there exists a surjective homomorphism $Z * Z \to C_2 * C_3$. ■

> **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]

Given the maps $i_1 : C_2 \to G, [m]_2 \mapsto x^m$ and $i_2 : C_3 \to G, [n]_3 \mapsto y^n$, we can check that i_1, i_2 are homomorphisms. We are to show that for every group H endowed with two homomorphisms $f_1 : C_2 \to H$, $f_2 : C_3 \to H$, there would be a unique group homomorphism $\varphi : G \to H$ such that the following diagram commutes

$$\begin{tikzcd} C_2 \arrow[d, "i_1"'] \arrow[dr, "f_1"] & \\ G \arrow[r, "\varphi"] & H \\ C_3 \arrow[u, "i_2"] \arrow[ur, "f_2"'] & \end{tikzcd}$$

or

$$\varphi(i_1([m]_2)) = \varphi(x^m) = \varphi(x)^m = f_1([m]_2),$$

$$\varphi(i_2([n]_3)) = \varphi(y^n) = \varphi(y)^n = f_2([n]_3).$$

Define $\phi : G \to H$ as $\phi(x^m y^n) = f_1([m]_2) f_2([n]_3)$, $\phi(y^n x^m) = f_2([n]_3) f_1([m]_2)$. It is clear to see ϕ makes the diagram commute. Moreover, if φ makes the diagram commute, it follows that for all $x^m y^n, y^n x^m \in G$,

$$\varphi(x^m y^n) = \varphi(x^m)\varphi(y^n) = f_1([m]_2) f_2([n]_3),$$

$$\varphi(y^n x^m) = \varphi(y^n)\varphi(x^m) = f_2([n]_3)f_1([m]_2),$$

which implies $\varphi = \phi$. Thus we can conclude G is the coproduct of C_2 and C_3 in Grp.

■

§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 $m\vert n$ necessary? [§4.1]

In §4.1 the function π_m^n is defined as

$$\begin{aligned} \pi_m^n \ : \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ [a]_n &\longmapsto [a]_m \end{aligned}$$

with the condition $m|n$. We can check that π_m^n is well-defined as

$$[a_1]_n = [a_2]_n \iff a_1 - a_2 = kn = (kl)m \implies [a_1]_m = [a_2]_m \iff \pi_m^n([a_1]_n) = \pi_m^n([a_2]_n).$$

Note $\pi_m^n(\pi_n(a)) = \pi_m^n([a]_n) = [a]_m = \pi_m(a)$. The diagram in §4.1 must commute.

$$\begin{tikzcd} \mathbb{Z} \arrow[d, "\pi_n"'] \arrow[dr, "\pi_m"] & \\ \mathbb{Z}/n\mathbb{Z} \arrow[r, "\pi_m^n"'] & \mathbb{Z}/m\mathbb{Z} \end{tikzcd}$$

Since

$$\pi_m^n([a]_n + [b]_n) = [a+b]_m = [a]_m + [b]_m = \pi_m^n([a]_n) + \pi_m^n([b]_n),$$

it follows that π_m^n is a group homomorphism. Actually we have shown that without the hypothesis $m|n$, π_m^n may not be well-defined. ■

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

Let calculate the order of each non-zero element in both C_4 and $C_2 \times C_2$. For the group C_4,

$$|[2]_4| = 2, \quad |[1]_4| = |[3]_4| = 4.$$

For the group $C_2 \times C_2$,

$$|([1]_2, [0]_2)| = |([0]_2, [1]_2)| = |([1]_2, [1]_2)| = 2.$$

Since isomorphism must preserve the order, we can assert that there is no such 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]

Assume some group G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$. Since $|[1]_n| = n$ and isomorphism preserves the order, we can affirm that there is an element of order n in G.
Conversely, assume there is a group G of order n in which g is an element of order n. By definition we see $g^0, g^1, g^2 \cdots g^{n-1}$ are distinct pairwise. Noticing group G has exactly n elements, G must consist of $g^0, g^1, g^2 \cdots g^{n-1}$. We can easily check that the function

$$\begin{aligned} f\ :G &\longrightarrow \mathbb{Z}/n\mathbb{Z} \\ g^k &\longmapsto [k]_n \end{aligned}$$

is an isomorphism. ∎

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.)

Suppose there exists an isomorphism $f : \mathbb{Z} \to \mathbb{Q}$. Let $f(1) = p/q$ $(p, q \in \mathbb{Z})$. If $p = 1$, for all $n \in \mathbb{Z}$, we have

$$f(n) = \frac{n}{q} \neq \frac{1}{2q}.$$

If $p \neq 1$, for all $n \in \mathbb{Z}$, we have

$$f(n) = \frac{np}{q} \neq \frac{p+1}{q}.$$

In both cases, it implies $f(\mathbb{Z}) \nsubseteq \mathbb{Q}$. Hence we see f is not a surjection, which contradicts the fact that $f : \mathbb{Z} \to \mathbb{Q}$ is an isomorphism. Compare the cardinality of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$

$$|\mathbb{Z}| = |\mathbb{Q}| < |\mathbb{R}|$$

and we show there exists no such isomorphisms like $f : \mathbb{Z} \to \mathbb{R}$ or $f : \mathbb{Q} \to \mathbb{R}$.
We can prove $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ are isomorphic, if considering the both as vector spaces over $\mathbb{Q}$. ∎

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

Suppose $f : \mathbb{R} \to \mathbb{C}$ is an isomorphism. Then there exists a real number x such that $f(x) = i$.

$$f(x^4) = f(x)^4 = i^4 = 1.$$

Since isomorphism preserves the identity, we have

$$f(1) = 1 = f(x^4).$$

which indicates $x^4 = 1$. Noticing that $x \in \mathbb{R}$, there must be $x^2 = 1$. Now we see

$$f(1) = f(x^2) = f(x)^2 = i^2 = -1,$$

which derives a contradiction. Thus we can conclude that groups $(\mathbb{R} \setminus \{0\}, \cdot)$ and $(\mathbb{C} \setminus \{0\}, \cdot)$ are not isomorphic.

$\blacksquare$

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?

Suppose $f : \mathbb{Q} \to \mathbb{Q}_{>0}$ is an isomorphism. Since isomorphism preserves the multiplication, we have

$$f(1) = f\left(n \cdot \frac{1}{n}\right) = f\left(\frac{1}{n}\right)^n \quad (n \in \mathbb{Z}_{>0}),$$

which implies

$$f\left(\frac{1}{n}\right) = f(1)^{\frac{1}{n}}.$$

Assume

$$f(1) = \frac{p}{q} = \frac{p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}}{q_1^{s_1} q_2^{s_2} \cdots q_l^{s_l}}$$

where p_i, q_i are pairwise distinct positive prime numbers. Then let

$$M = \max\{p, q\} + 1 > \max\{r_1, \cdots, r_k, s_1, \cdots, s_l\}.$$

Thus we assert

$$f\left(\frac{1}{M}\right) = \left(\frac{p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}}{q_1^{s_1} q_2^{s_2} \cdots q_l^{s_l}}\right)^{\frac{1}{M}} \notin \mathbb{Q},$$

which can be proved by contradiction. In fact, Suppose

$$\left(\frac{p}{q}\right)^{\frac{1}{M}} = \frac{a}{b} \in \mathbb{Q}$$

or say

$$pb^M = qa^M,$$

where a, b are coprime. Note that b^M, a^M are also coprime and that the prime factorization of a^M can be written as $a_1^{Mt_1} a_2^{Mt_2} \cdots a_j^{Mt_j}$ where a_i are pairwise distinct positive prime numbers. That forces

$$p = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k} = N \cdot a_1^{Mt_1} a_2^{Mt_2} \cdots a_j^{Mt_j}.$$

Noticing that a_i must coincide with one number in $\{p_1, p_2, \cdots p_k\}$, we can assume $a_1 = p_1$ without loss of generality. However, since $M > \max\{r_1, \cdots, r_k\}$, we see the exponent of p_1 is distinct from that of a_1, which violates the unique factorization property of $\mathbb{Z}$. Hence we get a contradiction and verify $f\left(\frac{1}{M}\right) \notin \mathbb{Q}$. Moreover, it contradicts our assumption that $f : \mathbb{Q} \to \mathbb{Q}_{>0}$ is an isomorphism. Eventually we show that the groups $(\mathbb{Q}, +)$ and $(\mathbb{Q}_{>0}, \cdot)$ are not isomorphic.

$\blacksquare$

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.

Given the function
$$\begin{aligned} f\ : G &\longrightarrow G \\ g &\longmapsto g^{-1} \end{aligned}$$
we have
$$f(g_1g_2) = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1}, \quad f(g_1)f(g_2) = g_1^{-1}g_2^{-1}.$$
If G is abelian, it is clear to see $f(g_1g_2) = f(g_1)f(g_2)$. If f is a homomorphism, $\forall h_1, h_2 \in G$,
$$h_1h_2 = (h_2^{-1}h_1^{-1})^{-1} = f(h_2^{-1}h_1^{-1}) = f(h_2^{-1})f(h_1^{-1}) = h_2h_1.$$
Given the function
$$\begin{aligned} h\ : G &\longrightarrow G \\ g &\longmapsto g^2 \end{aligned}$$
we have
$$h(g_1g_2) = (g_1g_2)^2 = g_1g_2g_1g_2, \quad h(g_1)h(g_2) = g_1^2g_2^2 = g_1g_1g_2g_2.$$
If G is abelian, it is clear to see $h(g_1g_2) = h(g_1)h(g_2)$. If h is a homomorphism, by cancellation we have
$$h(g_1g_2) = h(g_1)h(g_2) \implies g_2g_1 = g_1g_2.$$

$\blacksquare$

4.8 Let G be a group, and $g \in G$. 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.

Since
$$\gamma_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \gamma_g(a)\gamma_g(b),$$
γ_g is an automorphism of G. For all $a \in G$, we have
$$\gamma_{g_1g_2}(a) = g_1g_2ag_2^{-1}g_1^{-1} = \gamma_{g_1}(g_2ag_2^{-1}) = (\gamma_{g_1} \circ \gamma_{g_2})(a),$$
which implies $\gamma_{g_1g_2} = \gamma_{g_1} \circ \gamma_{g_2}$ and $g \mapsto \gamma_g$ is a homomorphism. If G is abelian, for all g the homomorphism
$$\gamma_g(a) = gag^{-1} = gg^{-1}a = a$$

is the identity in $\mathrm{Aut}(G)$. That is, the homomorphism $g \mapsto \gamma_g$ is trivial. If the homomorphism $g \mapsto \gamma_g$ is trivial, we have for all $g, a \in G$,

$$gag^{-1} = a,$$

which implies for all $a, b \in G$,

$$ab = bab^{-1}b = ba.$$

Thus we show the homomorphism $g \mapsto \gamma_g$ is trivial if and only if G is abelian. ■

4.9 Prove that if m, n are positive integers such that $\gcd(m, n) = 1$, then $C_{mn} \cong C_m \times C_n$.

Define a function

$$\begin{aligned} \varphi\ &: C_m \times C_n \longrightarrow C_{mn} \\ &([a]_m, [b]_n) \longmapsto [anp + bmq]_{mn} \end{aligned}$$

where $[pn]_m = [1]_m$ and $[qm]_n = [1]_n$, as $\gcd(m, n) = 1$ guarantees the existence of p, q (see textbook p56). First of all, we have to check whether φ is well-defined. Note that

$$[(anp_1 + bmq_1) - (anp_2 + bmp_2)]_m = [a(p_1 n - p_2 n) + b(q_1 m - q_2 m)]_m = [0]_m$$

$$[(anp_1 + bmq_1) - (anp_2 + bmp_2)]_n = [a(p_1 n - p_2 n) + b(q_1 m - q_2 m)]_n = [0]_n$$

and $\gcd(m, n) = 1$. Thus we have

$$[(anp_1 + bmq_1) - (anp_2 + bmp_2)]_{mn} = [0]_{mn},$$

or

$$[anp_1 + bmq_1]_{mn} = [anp_2 + bmp_2]_{mn}.$$

Then we show φ is a homomorphism.

$$\begin{aligned} \varphi(([a_1]_m, [b_1]_n) + ([a_2]_m, [b_2]_n)) &= \varphi([a_1 + a_2]_m, [b_1 + b_2]_n) \\ &= [(a_1 + a_2)np + (b_1 + b_2)mq]_{mn} \\ &= [a_1 np + b_1 mq]_{mn} + [a_2 np + b_2 mq]_{mn} \\ &= \varphi([a_1]_m, [b_1]_n) + \varphi([a_2]_m, [b_2]_n). \end{aligned}$$

In order to show φ is a monomorphism, we can check

$$\begin{aligned} &\varphi([a_1]_m, [b_1]_n) = \varphi([a_2]_m, [b_2]_n) \\ \Longrightarrow\ &[a_1 np + b_1 mq]_{mn} = [a_2 np + b_2 mq]_{mn} \\ \Longrightarrow\ &[(a_1 - a_2)np + (b_1 - b_2)mq]_{mn} = [0]_{mn} \\ \Longrightarrow\ &[(a_1 - a_2)np + (b_1 - b_2)mq]_m = [a_1 - a_2]_m = [0]_m, \\ &[(a_1 - a_2)np + (b_1 - b_2)mq]_n = [b_1 - b_2]_n = [0]_n \\ \Longrightarrow\ &[a_1]_m = [a_2]_m,\ [b_1]_m = [b_2]_m. \end{aligned}$$

Since $|C_m \times C_n| = |C_{mn}| = mn$, we can conclude φ is an isomorphism. Thus we complete proving $C_{mn} \cong C_m \times C_n$.

■

§5. Free groups

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

Yes, they are functions from A to any trivial group, for example $T = \{t\}$.

$$\begin{tikzcd} G \arrow[r, "\exists!\varphi"] & \{t\} \\ A \arrow[u, "j"] \arrow[ur, "e"'] & \end{tikzcd}$$

For any object (j, G) in $\mathscr{F}^A$, the trivial homomorphism $\varphi : g \mapsto t$ is the unique homomorphism such that the diagram commutes. That is, $\mathrm{Hom}((j, G), (e, T)) = \{\varphi\}$. ■

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 $A = \varnothing$).

Let $G = C_2 = \{[0]_2, [1]_2\}$. Note that $\varphi \circ e(A)$ must be the trivial subgroup $\{[0]_2\}$. If $x \in A$ and $j(x) = [1]_2$, we see $\varphi \circ e \neq j$ and the following diagram does not commute.

$$\begin{tikzcd} T \arrow[r, "\varphi"] & G \\ A \arrow[u, "e"] \arrow[ur, "j"'] & \end{tikzcd}$$

That implies (e, T) is not initial in $\mathscr{F}^A$ unless $A = \varnothing$. ■

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 $f(a) = f(b)$. Why? and how do you construct f and G?) [§III.6.3]

Let $G = S_A$ be the symmetric group over A. Define functions $g_a : A \to A,\ x \mapsto a$ sending every element of A to a. Since $g_a \in S_A$, we can define an injection

$$\begin{aligned} f\ : A &\longrightarrow S_A \\ a &\longmapsto g_a \end{aligned}$$

In light of the commutative diagram

$$\begin{tikzcd}
F(A) \arrow[r, "\varphi"] & S_A \\
A \arrow[u, "j"] \arrow[ur, "f"'] &
\end{tikzcd}$$

we have $\forall a, b \in A$,

$$j(a) = j(b) \implies \varphi(j(a)) = \varphi(j(b)) \implies f(a) = f(b) \implies a = b.$$

$\blacksquare$

5.4 In the ‘concrete’ construction of free groups, one can try to reduce words by performing cancellations in any order; the ‘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]

We use induction on the length of w. If w is reduced, there is nothing to show. If not, there must be some pair of symbols that can be cancelled, say the underlined pair

$$w = \cdots \underline{xx^{-1}} \cdots .$$

(Let’s allow x to denote any element of A', with the understanding that if $x = a^{-1}$ then $x^{-1} = a$.) If we show that we can obtain every reduced form of w by cancelling the pair xx^{-1} first, the proposition will follow by induction, because the word $w^* = \cdots \underline{\cancel{x}\cancel{x}^{-1}} \cdots$ is shorter.

Let w_0 be a reduced form of w. It is obtained from w by some sequence of cancellations. The first case is that our pair xx^{-1} is cancelled at some step in this sequence. If so, we may as well cancel xx^{-1} first. So this case is settled. On the other hand, since w_0 is reduced, the pair xx^{-1} can not remain in w_0. At least one of the two symbols must be cancelled at some time. If the pair itself is not cancelled, the first cancellation involving the pair must look like

$$\cdots \cancel{x}^{-1}\underline{\cancel{x}x}^{-1} \cdots \qquad \text{or} \qquad \cdots \underline{x\cancel{x}}^{-1}\cancel{x} \cdots$$

Notice that the word obtained by this cancellation is the same as the one obtained by cancelling the pair xx^{-1}. So at this stage we may cancel the original pair instead. Then we are back in the first case, so the proposition is proved.

$\blacksquare$

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

Assume the A is a set and H is an abelian group. $H^{\oplus A}$ are defined as follows

$$H^{\oplus A} := \{\alpha : A \to H | \alpha(a) \neq e_H \text{ for only finitely many elements } a \in A\}.$$

Now that $H^{\oplus A} \subset H^A := \mathrm{Hom}_{\mathsf{Set}}(A, H)$, we can first show $(H^A, +)$ is a group, where for all $\phi, \psi \in H^A$, $\phi + \psi$ is defined by

$$(\forall a \in A) : (\phi + \psi)(a) := \phi(a) + \psi(a).$$

Here is the verification:

- Identity: Define a function $\varepsilon : A \to H, a \mapsto e_H$ sending all elements in A to e_H. Then for any $\alpha \in H^A$ we have

  $$(\forall a \in A) : (\alpha + \varepsilon)(a) = \alpha(a) + \varepsilon(a) = \alpha(a),$$

  which is $\alpha + \varepsilon = \alpha$. Because of the commutativity of the operation $+$ defined on H^A, ε is the identity indeed.

- Associativity: This follows by the associativity in H:

  $$(\forall a \in A) : ((\alpha+\beta)+\gamma)(a) = (\alpha+\beta)(a)+\gamma(a) = \alpha(a)+(\beta+\gamma)(a) = (\alpha+(\beta+\gamma))(a).$$

- Inverse: Every function $\phi \in H^A$ has inverse $-\phi$ defined by

  $$(\forall a \in A) : (-\phi)(a) = -\phi(a).$$

Thus H^A makes a group.

Then it is time to show $H^{\oplus A}$ is a subgroup of H^A. For all $\alpha, \beta \in H^{\oplus A}$, let $N_\alpha = \{a \in A | \alpha(a) \neq e_H\}$, $N_\beta = \{a \in A | \beta(a) \neq e_H\}$, $N_{\alpha-\beta} = \{a \in A | (\alpha - \beta)(a) \neq e_H\}$. Since

$$(\forall a \in A) : (\alpha - \beta)(a) = \alpha(a) - \beta(a),$$

we have

$$(\alpha - \beta)(a) \neq e_H \implies \alpha(a) \neq e_H \text{ or } \beta(a) \neq e_H,$$

which implies $N_{\alpha-\beta} \subset N_\alpha \cup N_\beta$. Note that N_α, N_β are both finite sets, which forces $N_{\alpha-\beta}$ to be finite. So there must be $\alpha - \beta \in H^{\oplus A}$. Now we see $H^{\oplus A}$ is closed under additions and inverses. And $e_{H^A} = \varepsilon \in H^{\oplus A}$ means that $H^{\oplus A}$ is nonempty. Finally we can conclude $H^{\oplus A}$ is a subgroup of H^A. ■

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]

Define two homomorphisms

$$\begin{aligned} i_1 &: \mathbb{Z} \longrightarrow F(\{x, y\}), \quad n \longmapsto x^n, \\ i_2 &: \mathbb{Z} \longrightarrow F(\{x, y\}), \quad n \longmapsto y^n. \end{aligned}$$

We need to show that for any group G with two homomorphisms $f_1, f_2 : \mathbb{Z} \to G$, there exists a unique homomorphism φ such that the following diagram commutes.

$$
\begin{tikzcd}
\mathbb{Z} \arrow[d, "i_1"'] \arrow[dr, "f_1"] & \\
F(\{x,y\}) \arrow[r, "\varphi"] & G \\
\mathbb{Z} \arrow[u, "i_2"] \arrow[ur, "f_2"'] &
\end{tikzcd}
$$

Given the notation of indicator function

$$
\mathbf{1}_A(x) := \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{if } x \notin A, \end{cases}
$$

we can define a function

$$
\begin{aligned}
\varphi : F(\{x,y\}) &\longrightarrow G, \\
z_1^{n_1} \cdots z_k^{n_k} &\longmapsto f_1(n_1)^{\mathbf{1}_{\{x\}}(z_1)} f_2(n_1)^{\mathbf{1}_{\{y\}}(z_1)} \cdots f_1(n_k)^{\mathbf{1}_{\{x\}}(z_n)} f_2(n_k)^{\mathbf{1}_{\{y\}}(z_n)}, \ z_i \in \{x,y\}
\end{aligned}
$$

and check that it is a homomorphism indeed. For all $n \in \mathbb{Z}$, we have

$$
\begin{aligned}
(\varphi \circ i_1)(n) = \varphi(x^n) = f_1(n), \\
(\varphi \circ i_2)(n) = \varphi(y^n) = f_2(n),
\end{aligned}
$$

that is, the diagram commutes. Now we see φ exists. For the uniqueness of φ, let φ^* be another homomorphism that makes diagram commute. For all $z_1^{n_1} \cdots z_k^{n_k} \in F(\{x,y\})$, $z_i \in \{x,y\}$, we have

$$
\begin{aligned}
\varphi^*(z_1^{n_1} \cdots z_k^{n_k}) &= \varphi^*(z^{n_1}) \cdots \varphi^*(z^{n_k}) \\
&= \varphi^*(i_1(n_1))^{\mathbf{1}_{\{x\}}(z_1)} \varphi^*(i_2(n_1))^{\mathbf{1}_{\{y\}}(z_1)} \cdots \varphi^*(i_1(n_k))^{\mathbf{1}_{\{x\}}(z_1)} \varphi^*(i_2(n_k))^{\mathbf{1}_{\{y\}}(z_1)} \\
&= f_1(n_1)^{\mathbf{1}_{\{x\}}(z_1)} f_2(n_1)^{\mathbf{1}_{\{y\}}(z_1)} \cdots f_1(n_k)^{\mathbf{1}_{\{x\}}(z_n)} f_2(n_k)^{\mathbf{1}_{\{y\}}(z_n)} \\
&= \varphi(z_1^{n_1} \cdots z_k^{n_k}).
\end{aligned}
$$

To sum up, we have shown that the group $F(\{x,y\})$ is a coproduct $\mathbb{Z} * \mathbb{Z}$ of $\mathbb{Z}$ by itself in the category Grp. ∎

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

Let $*$ be coproduct. Then we have $\underbrace{\mathbb{Z} * \mathbb{Z} * \cdots * \mathbb{Z}}_{n \text{ times}} \cong F(\{x_1, \ldots, x_n\})$, as the following diagram demonstrates:

$$\begin{tikzcd}
\mathbb{Z} \arrow[drr, "i_1"] \arrow[drrr, "f_1"] & & & \\
\vdots & \vdots & F(\{x_1,\dots,x_n\}) \arrow[r, "\varphi"] & G \\
\mathbb{Z} \arrow[urr, "i_n"] \arrow[urrr, "f_n"'] & & &
\end{tikzcd}$$

Dually, let $\times$ be product. Then we have $\underbrace{\mathbb{Z}\times\mathbb{Z}\times\cdots\times\mathbb{Z}}_{n \text{ times}} \cong F^{ab}(\{x_1,\cdots,x_n\})$, as the following diagram demonstrates:

$$\begin{tikzcd}
 & & & \mathbb{Z} \\
G \arrow[urrr, "f_1"] \arrow[drrr, "f_n"'] \arrow[r, "\varphi"] & F^{ab}(\{x_1,\dots,x_n\}) \arrow[urr, "\pi_1"] \arrow[drr, "\pi_n"'] & \vdots & \vdots \\
 & & & \mathbb{Z}
\end{tikzcd}$$

■

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, F^{ab} 'preserve coproducts'.)

In order to show $F(A) * F(B)$ is a free group generated by $A \amalg B$, we should first set an appropriate function $\psi : A \amalg B \to F(A) * F(B)$ and then prove that given any (θ, G) there exists a unique group homomorphism g such that the following diagram commutes.

$$\begin{tikzcd}
A \amalg B \arrow[r, "\psi"] \arrow[rr, bend right, "\theta"'] & F(A) * F(B) \arrow[r, dashed, "\exists! g"] & G
\end{tikzcd}$$

The complete proof can be divided into three steps, by decomposing the following diagram into parts.

$$\begin{tikzcd}
A \arrow[r, "j_1"] \arrow[d, "i_1"] & F(A) \arrow[d, "f_1"] \arrow[dr, dashed, "\varphi_1"] & \\
A \amalg B \arrow[r, dashed, "\psi"] \arrow[rr, bend right, "\theta"] & F(A) * F(B) \arrow[r, dashed, "g"] & G \\
B \arrow[u, "i_2"] \arrow[r, "j_1"] & F(B) \arrow[u, "f_2"] \arrow[ur, dashed, "\varphi_2"'] &
\end{tikzcd}$$

Step 1. Construct $\psi : A \amalg B \longrightarrow F(A) * F(B)$.
Define injective functions

$$\begin{aligned}
i_1 &: A \longrightarrow A \amalg B, \quad a \longmapsto (a, 1), \\
i_2 &: B \longrightarrow A \amalg B, \quad b \longmapsto (b, 2), \\
j_1 &: A \longrightarrow F(A), \quad a \longmapsto a, \\
j_2 &: B \longrightarrow F(B), \quad b \longmapsto b.
\end{aligned}$$

Let f_1, f_2 be the homomorphisms specified by the coproduct in Grp. Since $A \amalg B$ is a coproduct in Set, the universal property guarantees a unique mapping $\psi : A \amalg B \to F(A) * F(B)$ such that the following diagram commutes

$$\begin{tikzcd}
A \arrow[r, "j_1"] \arrow[d, "i_1"] & F(A) \arrow[d, "f_1"] \\
A \amalg B \arrow[r, dashed, "\exists!\psi"] & F(A) * F(B) \\
B \arrow[u, "i_2"] \arrow[r, "j_1"] & F(B) \arrow[u, "f_2"]
\end{tikzcd}$$

That is,

$$\exists!\ \psi : A \amalg B \longrightarrow F(A) * F(B) \quad (\psi \circ i_1 = f_1 \circ j_1) \wedge (\psi \circ i_2 = f_2 \circ j_2).$$

Step 2. Prove the existence of g.

$$\begin{tikzcd}
A \arrow[r, "j_1"] \arrow[d, "i_1"] & F(A) \arrow[dr, dashed, "\exists!\varphi_1"] & \\
A \amalg B \arrow[rr, "\theta"] & & G \\
B \arrow[u, "i_2"] \arrow[r, "j_1"] & F(B) \arrow[ur, dashed, "\exists!\varphi_2"'] &
\end{tikzcd}$$

Given some (θ, G), according to the universal property of free groups $F(A)$, $F(B)$, we have

$$\exists! \ \varphi_1 : F(A) \longrightarrow G \quad (\varphi_1 \circ j_1 = \theta \circ i_1),$$
$$\exists! \ \varphi_2 : F(B) \longrightarrow G \quad (\varphi_2 \circ j_2 = \theta \circ i_2).$$

$$\begin{tikzcd}
F(A) \arrow[d, "f_1"] \arrow[dr, dashed, "\varphi_1"] & \\
F(A) * F(B) \arrow[r, dashed, "\exists! g"] & G \\
F(B) \arrow[u, "f_2"] \arrow[ur, dashed, "\varphi_2"'] &
\end{tikzcd}$$

Then according to the universal property of coproduct $F(A) * F(B)$ in Grp, we have

$$\exists! \ g : F(A) * F(B) \longrightarrow G \quad (g \circ f_1 = \varphi_1) \wedge (g \circ f_2 = \varphi_2).$$

The commutative diagram tells us

$$g \circ \psi \circ i_1 = g \circ f_1 \circ j_1 = \varphi_1 \circ j_1 = \theta \circ i_1,$$
$$g \circ \psi \circ i_2 = g \circ f_2 \circ j_2 = \varphi_2 \circ j_2 = \theta \circ i_2.$$

Note that $A \amalg B = i_1(A) \cup i_2(B)$. For all $x \in A \amalg B$, x must be either $i_1(a)$ or $i_2(b)$. If $x = i_1(a)$, then

$$g \circ \psi(x) = g \circ \psi \circ i_1(a) = \theta \circ i_1(a) = \theta(x).$$

If $x = i_2(b)$, then

$$g \circ \psi(x) = g \circ \psi \circ i_2(b) = \theta \circ i_2(b) = \theta(x).$$

Hence we show that given some (θ, G) there exists $g : F(A) * F(B) \longrightarrow G$ such that $g \circ \psi = \theta$.

Step 3. Prove the uniqueness of g.
Assume there exists another homomorphism h such that $h \circ \psi = \theta$. We have

$$h \circ f_1 \circ j_1 = h \circ \psi \circ i_1 = \theta \circ i_1,$$
$$h \circ f_2 \circ j_2 = h \circ \psi \circ i_2 = \theta \circ i_2.$$

Since

$$\exists! \ \varphi_1 : F(A) \longrightarrow G \quad (\varphi_1 \circ j_1 = \theta \circ i_1),$$
$$\exists! \ \varphi_2 : F(B) \longrightarrow G \quad (\varphi_2 \circ j_2 = \theta \circ i_2),$$

there must be

$$
\begin{aligned}
h \circ f_1 = \varphi_1, \\
h \circ f_2 = \varphi_2.
\end{aligned}
$$

Again by universal property

$$
\exists!\ g : F(A) * F(B) \longrightarrow G \quad (g \circ f_1 = \varphi_1) \wedge (g \circ f_2 = \varphi_2)
$$

we get $h = g$, which implies g is unique.

Conclusion.
To sum up, we prove that there exists a unique group homomorphism g such that the first diagram in this proof commutes. As a result, we have $F(A \amalg B) = F(A) * F(B)$. Note that if Grp turns into Ab, the method of diagram chasing applied here also works. In the light of the following diagram, we can get $F^{ab}(A \amalg B) = F^{ab}(A) \oplus F^{ab}(B)$ step by step.

$$
\begin{tikzcd}
A \arrow[r, "j_1"] \arrow[d, "i_1"] & F^{ab}(A) \arrow[d, "f_1"] \arrow[dr, dashed, "\varphi_1"] & \\
A \amalg B \arrow[r, dashed, "\psi"] \arrow[rr, bend right, "\theta"'] & F^{ab}(A) \oplus F^{ab}(B) \arrow[r, dashed, "g"] & G \\
B \arrow[r, "j_1"] \arrow[u, "i_2"] & F^{ab}(B) \arrow[u, "f_2"] \arrow[ur, dashed, "\varphi_2"'] &
\end{tikzcd}
$$

■

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

Define a function

$$
\begin{aligned}
\varphi : G \times G &\longrightarrow G \\
((a_1, a_2, \cdots), (b_1, b_2, \cdots)) &\longmapsto (a_1, b_1, a_2, b_2, \cdots)
\end{aligned}
$$

It is plain to check that φ is a homomorphism

$$
\begin{aligned}
&\varphi[((a_1, a_2, \cdots), (b_1, b_2, \cdots)) + ((a_1', a_2', \cdots), (b_1', b_2', \cdots))] \\
=&\varphi[((a_1 + a_1', a_2 + a_2', \cdots), (b_1 + b_1', b_2 + b_2', \cdots))] \\
=&(a_1 + a_1', b_1 + b_1', a_2 + a_2', b_2 + b_2', \cdots) \\
=&(a_1, b_1, a_2, b_2, \cdots) + (a_1', b_1', a_2', b_2', \cdots) \\
=&\varphi[((a_1, a_2, \cdots), (b_1, b_2, \cdots))] + \varphi[((a_1', a_2', \cdots), (b_1', b_2', \cdots))].
\end{aligned}
$$

Since $\ker \varphi = \{(0, 0, \cdots)\}$ and $\varphi(G \times G) = G$, we can conclude that φ is an isomorphism and accordingly $G \times G \cong G$. ■

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

- 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 $F^{ab}(B) \cong F^{ab}(A)$. If A is finite, prove that so is B, and $A \cong B$ 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]

- If $|A| = \infty$, let $F = F^{ab}(A) = \mathbb{Z}^{\oplus A}$ and accordingly every element of $\mathbb{Z}^{\oplus A}$ can be written uniquely as a finite sum

$$\sum_{a\in A} m_a j(a), \qquad m_a \neq 0 \text{ for only finitely many } a.$$

Apparently, the elements in $j(A) = \{j(a) \mid a \in A\}$ are not equivalent pairwise. Note that j is an injection. Hence we see

$$|F/\sim| \geq |j(A)| = A > \infty.$$

In other words, $F/\sim$ is a finite set only if A is finite.
If $|A| = n < \infty$, we can set $F = F^{ab}(A) = \mathbb{Z}^{\oplus n}$. Assume $f = (a_1, a_2, \cdots, a_n)$, $f' = (a'_1, a'_2, \cdots, a'_n)$. Then $f \sim f'$ if and only if $a_i - a'_i \in 2\mathbb{Z}$ $(i = 1, 2, \cdots, n)$. Let $[f]$ denote the equivalence class including f. Thus we get

$$F/\sim = \{[(k_1, k_2, \cdots, k_n)] \mid k_i = 0 \text{ or } 1,\ i = 1, 2, \cdots, n\}$$

and accordingly $|F/\sim| = 2^{|A|}$.

- Assume $\varphi : F^{ab}(A) \to F^{ab}(B)$ is a group isomorphism. Since for all $f, f' \in F^{ab}(A)$,

$$\begin{aligned} f \sim f' &\iff \exists\, g \in F^{ab}(A),\ f - f' = 2g \\ &\iff \exists\, \varphi(g) \in F^{ab}(B),\ \varphi(f) - \varphi(f') = 2\varphi(g) \\ &\iff \varphi(f) \sim \varphi(f') \end{aligned}$$

in Set we have

$$F^{ab}(A)/\sim \; \simeq F^{ab}(B)/\sim .$$

If A is finite, then $F^{ab}(A)/\sim$ is finite. Furthermore it follows that

$$|F^{ab}(A)/\sim| = |F^{ab}(B)/\sim| \implies 2^{|A|} = 2^{|B|} \implies |A| = |B|.$$

Hence we see B is finite and $A \cong B$ in Set .

∎

§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 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:

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

Here In 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]

The following diagram commutes, where all arrows are inclusions.

$$\begin{tikzcd}
\mathrm{GL}_n(\mathbb{R}) \arrow[r] & \mathrm{GL}_n(\mathbb{C}) \\
\mathrm{SL}_n(\mathbb{R}) \arrow[r] \arrow[u] & \mathrm{SL}_n(\mathbb{C}) \arrow[u] \\
\mathrm{O}_n(\mathbb{R}) \arrow[r] \arrow[u] & \mathrm{U}(n) \arrow[u] \\
\mathrm{SO}_n(\mathbb{R}) \arrow[r] \arrow[u] & \mathrm{SU}(n) \arrow[u]
\end{tikzcd}$$

■

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 $(a_{ij})_{1 \le i,j \le n}$ 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]

Let A, B are $n \times n$ upper triangular matrices. If $i > j$,

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{i-1} a_{ik}b_{kj} + \sum_{k=i}^{n} a_{ik}b_{kj} = \sum_{k=1}^{i-1} 0b_{kj} + \sum_{k=i}^{n} a_{ik}0 = 0,$$

which means the set of upper triangular matrices is closed with respect to the matrix multiplication. Thus it is a subgroup of $\mathrm{GL}_n(\mathbb{C})$. ∎

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]

Let

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{SU}(2)$$

and we have

$$AA^\dagger = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} \overline{a_{11}} & \overline{a_{21}} \\ \overline{a_{12}} & \overline{a_{22}} \end{pmatrix} = \begin{pmatrix} |a_{11}|^2 + |a_{12}|^2 & a_{11}\overline{a_{21}} + a_{12}\overline{a_{22}} \\ a_{21}\overline{a_{11}} + a_{22}\overline{a_{12}} & |a_{21}|^2 + |a_{22}|^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\det(A) = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21} = 1$$

Note

$$\overline{a_{11}a_{12}} = \overline{a_{11}a_{12}} \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \begin{vmatrix} |a_{11}|^2 & |a_{12}|^2 \\ a_{21}\overline{a_{11}} & a_{22}\overline{a_{12}} \end{vmatrix} = \begin{vmatrix} |a_{11}|^2 & |a_{11}|^2 + |a_{12}|^2 \\ a_{21}\overline{a_{11}} & a_{21}\overline{a_{11}} + a_{22}\overline{a_{12}} \end{vmatrix} = \begin{vmatrix} |a_{11}|^2 & 1 \\ a_{21}\overline{a_{11}} & 0 \end{vmatrix} = -a_{21}\overline{a_{11}}$$

$$\implies \overline{a_{11}}(\overline{a_{12}} + a_{21}) = 0,$$

and

$$\overline{a_{21}a_{22}} = \overline{a_{21}a_{22}} \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \begin{vmatrix} a_{11}\overline{a_{21}} & a_{12}\overline{a_{22}} \\ |a_{21}|^2 & |a_{22}|^2 \end{vmatrix} = \begin{vmatrix} a_{11}\overline{a_{21}} & a_{11}\overline{a_{21}} + a_{12}\overline{a_{22}} \\ |a_{21}|^2 & |a_{21}|^2 + |a_{22}|^2 \end{vmatrix} = \begin{vmatrix} a_{11}\overline{a_{21}} & 0 \\ |a_{21}|^2 & 1 \end{vmatrix} = a_{11}\overline{a_{21}}$$

$$\implies \overline{a_{21}}(\overline{a_{11}} - a_{22}) = 0.$$

If $\overline{a_{11}} \neq 0$, it must be $\overline{a_{12}} + a_{21} = 0$. If $\overline{a_{11}} = 0$, then $|a_{12}|^2 = 1$, $a_{12}\overline{a_{22}} = 0$ and accordingly $a_{22} = 0$. Since $-a_{12}a_{21} = 1 = a_{12}\overline{a_{12}}$, we also have $\overline{a_{12}} + a_{21} = 0$, that is $a_{12} = c + di, a_{21} = -c + di$. Likewise, we can show $\overline{a_{11}} - a_{22} = 0$ and $a_{11} = a + bi, a_{22} = a - bi$. And we have

$$|a_{11}|^2 + |a_{12}|^2 = a^2 + b^2 + c^2 + d^2 = 1.$$

■

6.4 Let G be a group, and $g \in G$. 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).

If $|g| = \infty$, then $g^i \neq g^j (i \neq j)$. Define

$$\varphi : \mathbb{Z} \longrightarrow \epsilon_g(\mathbb{Z}), n \longmapsto g^n$$

and we can check it is an isomorphism.
If $|g| = k$, then $e_G, g, g^2, \cdots, g^{k-1}$ are distinct. Define

$$\varphi : \mathbb{Z}/k\mathbb{Z} \longrightarrow \epsilon_g(\mathbb{Z}), [n]_k \longmapsto g^n$$

and we can check it is an isomorphism.
Since $\epsilon_g(\mathbb{Z})$ is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}/k\mathbb{Z}$, we show $\epsilon_g(\mathbb{Z})$ is a cyclic group. ■

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 $\cup_{i \geq 0} H_i$ is a subgroup of G.

- Let $H \cup H'$ be a subgroup of G. Suppose neither $H \subseteq H'$ nor $H' \subseteq H$ hold. Let $a \in H - H'$, $b \in H' - H$, $h = ab^{-1} \in H \cup H'$. In the case of $h \in H$, we have $b = h^{-1}a \in H$, contradiction! In the case of $h \in H'$, we have $a = hb \in H'$, contradiction again! Therefore, there must be $H \subseteq H'$ or $H' \subseteq H$.
- For all $a, b \in \cup_{i \geq 0} H_i$, we can suppose $a \in H_j, b \in H_k$ and we have $a, b \in H_{\max\{j,k\}}$. Then $ab \in H_{\max\{j,k\}} \subseteq \cup_{i \geq 0} H_i$, implies that $\cup_{i \geq 0} H_i$ is closed and that $\cup_{i \geq 0} H_i$ is a subgroup of G.

■

6.7 ¬ Show that inner automorphisms (cf. Exercise II.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 $\forall g \in G\ \exists n \in Z\ \gamma_g = \gamma_a^n$. In particular, $gag^{-1} = a^n a a^{-n} = a$. 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]

With notation as in Exercise 4.8, we assume $\gamma_g \in \mathrm{Inn}(G)$ is defined by

$$\forall h \in G \ \ (\gamma_g(h) = ghg^{-1}).$$

We have

$$\begin{aligned}
& \mathrm{Inn}(G) \text{ is cyclic} \\
\iff & \exists \gamma_a \in \mathrm{Inn}(G),\ \mathrm{Inn}(G) = \langle \gamma_a \rangle \\
\iff & \exists a \in G\ \forall g \in G\ \exists n \in \mathbb{Z}\ (\gamma_g = \gamma_a^n) \\
\implies & \exists a \in G\ \forall g \in G\ \exists n \in \mathbb{Z}\ (\gamma_g(a) = gag^{-1} = \gamma_a^n(a) = a^n a a^{-n} = a) \\
\implies & \exists a \in G\ \forall g \in G\ (ga = ag) \\
\implies & \forall h \in G, \gamma_a(h) = aha^{-1} = haa^{-1} = h \\
\implies & \mathrm{Inn}(G) = \langle \mathrm{id} \rangle \\
\implies & \mathrm{Inn}(G) \text{ is trivial}
\end{aligned}$$

$$\begin{aligned}
& \mathrm{Inn}(G) \text{ is trivial} \\
\implies & \forall g \in G\ \forall h \in G\, (\gamma_g(h) = ghg^{-1} = h) \\
\implies & \forall g \in G\ \forall h \in G\, (gh = hg) \\
\iff & G \text{ is abelian}
\end{aligned}$$

$$\begin{aligned}
& G \text{ is abelian} \\
\implies & \forall g \in G\ \forall h \in G\, (\gamma_g(h) = ghg^{-1} = h) \\
\implies & \mathrm{Inn}(G) = \{\mathrm{id}\} \\
\implies & \mathrm{Inn}(G) \text{ is cyclic}
\end{aligned}$$

If $\mathrm{Aut}(G)$ is cyclic, its subgroup $\mathrm{Inn}(G)$ is also cyclic. As we have shown, that means G is abelian. ∎

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.

Given any set $H \subseteq G$, there exists a unique homomorphism φ_H such that the following diagram commutes.

$$\begin{tikzcd}
F^{ab}(H) \arrow[r, "\exists!\varphi"] & G \\
H \arrow[u, "j"] \arrow[ur, hook, "i"'] &
\end{tikzcd}$$

The homomorphism image $\varphi_H(F^{ab}(H)) \leq G$ is called the subgroup generated by H in G, denoted by $\langle H\rangle$.

If G is finitely generated, there is a finite subset $G_n \subseteq G$ with n elements such that $\varphi_H(F^{ab}(G_n)) = \varphi_H(\mathbb{Z}^{\oplus n}) = G$. And φ_H is exactly the surjective homomorphism that we need.

If there is a surjective homomorphism $\psi : \mathbb{Z}^{\oplus n} \twoheadrightarrow G$ for some n. Suppose

$$\psi : \mathbf{1}_i = (0, \cdots, 0, \underset{i\text{-th place}}{1}, 0, \cdots, 0) \longmapsto g_i$$

and $G_n = \{g_1, g_2, \cdots, g_n\}$. Then define

$$j : G_n \longrightarrow \mathbb{Z}^{\oplus n}, \quad g_i \longmapsto \mathbf{1}_i.$$

We can check the following diagram commutes

$$\begin{tikzcd}
\mathbb{Z}^{\oplus n} \arrow[r, two heads, "\psi"] & G \\
G_n \arrow[u, "j"] \arrow[ur, hook, "i"'] &
\end{tikzcd}$$

which means $\langle G_n\rangle = \psi(\mathbb{Z}^{\oplus n})$. Since ψ is surjective, we have $\langle G_n\rangle = G$. Hence we show G is finitely generated. ■

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

Given any two rationals

$$a_1 = \frac{p_1}{q_1} \in \mathbb{Q}, (p_1, q_1) = 1,$$
$$a_2 = \frac{p_2}{q_2} \in \mathbb{Q}, (p_2, q_2) = 1,$$

there exists $r = \frac{1}{q_1 q_2} \in \mathbb{Q}$ such that $\langle a_1, a_2\rangle \leq \langle r_1\rangle$. Then for some a_3 we have $\langle a_1, a_2, a_3\rangle \leq \langle r_1, a_3\rangle \leq \langle r_2\rangle$. In general, let's set $B_n = \{a_1, a_2, \cdots, a_n\}$. If $\langle B_n\rangle \leq \langle r_{n-1}\rangle$. we have $\langle B_{n+1}\rangle = \langle B_n, a_{n+1}\rangle \leq \langle r_{n-1}, a_{n+1}\rangle \leq \langle r_n\rangle$. By induction we can prove $\langle a_1, a_2, \cdots, a_n\rangle \leq \langle r_{n-1}\rangle$ for $n \in \mathbb{N}_+$. Since the subgroups of a cyclic group are also cyclic, we see finitely generated subgroup $\langle a_1, a_2, \cdots, a_n\rangle \leq \mathbb{Q}$ is cyclic.
Supposing $\mathbb{Q}$ is finitely generated, $\mathbb{Q}$ must be a cyclic group, which contradicts the fact. Thus we show $\mathbb{Q}$ is not finitely generated. ■

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

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

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

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

Let H be the subgroup generated by s and t. We can check that both

$$P = \begin{pmatrix} 1 & -p \\ 0 & 1 \end{pmatrix} = t^{-p} \quad \text{and} \quad Q = \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} = s^{-1} t^q s$$

are in H. Given an arbitrary matrix

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

it suffices to show that we can obtain the identity I_2 by multiplying m by matrices in H. Note that

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -p \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b - pa \\ c & d - pc \end{pmatrix}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -q & 1 \end{pmatrix} = \begin{pmatrix} a - qb & b \\ c - qd & d \end{pmatrix},$$

and c, d cannot be nonzero simultaneously. Without loss of generality, we can assume that $0 < c < d$ and perform Euclidean algorithm. Let $p_1 = \lfloor \frac{d}{c} \rfloor, d_1 = d - p_1 c < c$. Multiplying m by $P_1 = \begin{pmatrix} 1 & -p_1 \\ 0 & 1 \end{pmatrix}$ on the right yields

$$m_1 = mP_1 \begin{pmatrix} a & b - p_1 a \\ c & d_1 \end{pmatrix}.$$

Then let $q_1 = \lfloor \frac{c}{d_1} \rfloor, c_1 = c - q_1 d_1 < d_1$ and right multiplying m by $Q_1 = \begin{pmatrix} 1 & 0 \\ -q_1 & 1 \end{pmatrix}$ yields

$$m_2 = mP_1Q_1 \begin{pmatrix} a - q_1(b - p_1 a) & b - p_1 a \\ c_1 & d_1 \end{pmatrix}.$$

We can repeat this procedure until some d_i or c_i reduce to 0. The Euclidean algorithm generates a sequence

$$d > c > d_1 > c_1 > d_2 > c_2 > \cdots.$$

If c_i, d_i never reduce to 0, we will get an infinite decreasing positive sequence, which is impossible. Suppose d_N is the first number reducing to 0. Then

$$m_{2N-1} = mP_1Q_1 \cdots P_N = \begin{pmatrix} a_N & b_N \\ c_{N-1} & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

which implies

$$m_{2N-1} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and $m_{2N-1}s^{-1} = I_2$. Suppose c_N is the first number reducing to 0. Then

$$m_{2N} = mP_1Q_1 \cdots P_NQ_N = \begin{pmatrix} a_N & b_N \\ 0 & d_N \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

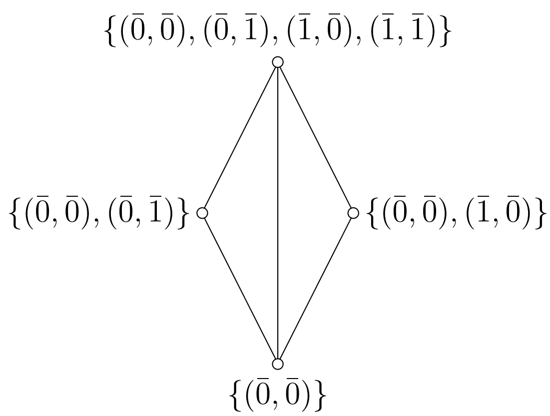
which implies

$$m_{2N} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

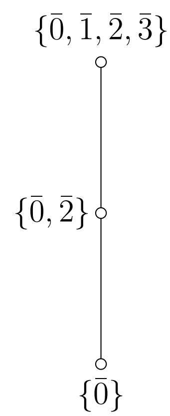
We have shown that we can obtain the identity I_2 by multiplying m by matrices in H, that is, m can be represented as a product of matrices in H. Thus we can conclude $\mathrm{SL}_2(\mathbb{Z})$ is generated by s and t. ∎

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

Lattices of subgroups $C_2 \times C_2$ and C_4 are drawn as follows:

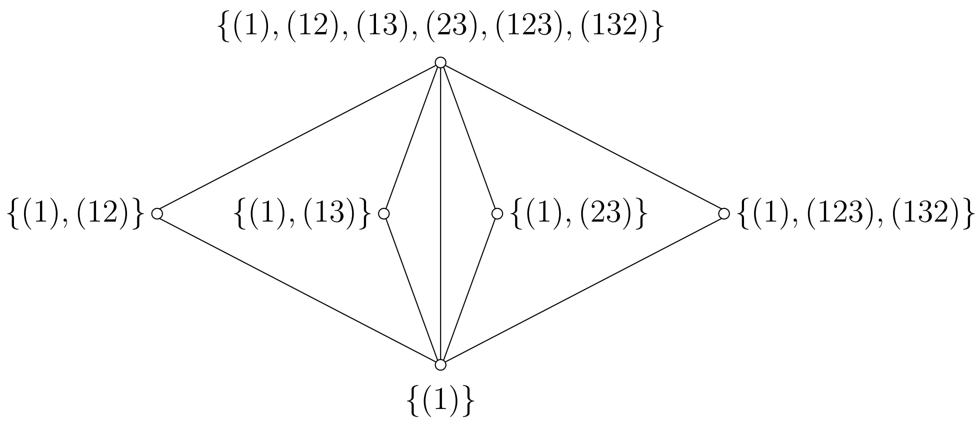


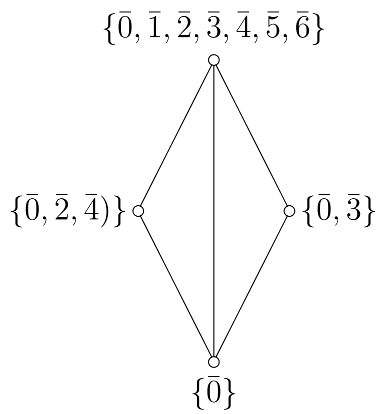
$C_2 \times C_2$



C_4

Lattices of subgroups S_3 and C_6 are drawn as follows:





■

§7. Quotient groups

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

The subgroups of S_3 are $\{(1)\}, \{(1),(12)\}, \{(1),(13)\}, \{(1),(23)\}, \{(1),(123),(132)\}$ and S_3. We can check that $\{(1)\}, \{(1),(123),(132)\}, S_3$ are normal subgroups while others are not. ■

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

No. According to exercise 7.1 we have seen not all subgroups are normal. Suppose H is a subgroup of G but not normal. Then H itself is the image of the inclusion homomorphism $i : H \hookrightarrow G$, which makes a counterexample. ■

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

That a subgroup N of G is normal has four equivalent conditions:

(i) $\forall g \in G,\ gNg^{-1} = N$;

(ii) $\forall g \in G,\ gNg^{-1} \subseteq N$;

(iii) $\forall g \in G,\ gN \subseteq Ng$;

(iv) $\forall g \in G,\ gN = Ng$.

(i) $\Longrightarrow$ (ii) is straightforward.
(ii) $\Longrightarrow$ (iii). For any $g \in G$, the element $a \in gN$ can be written as $a = gn_1 (n_1 \in N)$. Since $gn_1g^{-1} \in gNg^{-1} \subseteq N$, there exists an $n_2 \in N$ such that $gn_1g^{-1} = n_2$, which implies $gn_1 = n_2g \in Ng$. Thus we have $gN \subseteq Ng$.
(iii) $\Longrightarrow$ (iv). Given any $g \in G$, for all $n_1 \in N$, the element $g^{-1}n_1 \in g^{-1}N_1$ also belongs to Ng^{-1}, which implies that there exists $n_2 \in N$ such that $g^{-1}n_1 = n_2g^{-1}$, namely $n_1g = gn_2$. Thus we get $Ng \subseteq gN$ and accordingly $gN = Ng$.
(iv) $\Longrightarrow$ (i). For any $g \in G$, the element $b \in gNg^{-1}$ can be written as $a = gn_1g^{-1}(n_1 \in N)$. Since $gn_1 \in gN = Ng$, there exists an $n_2 \in N$ such that $gn_1 = n_2g$, which implies $gn_1g^{-1} = n_2 \in N$. Thus we have

$$\begin{aligned} & \forall g \in G, \quad gNg^{-1} \subseteq N \\ \Longrightarrow & \forall g^{-1} \in G, \quad g^{-1}(gNg^{-1})g \subseteq gNg^{-1} \\ \Longrightarrow & \forall g \in G, \quad N \subseteq gNg^{-1}. \end{aligned}$$

Hence we have $\forall g \in G,\ gNg^{-1} = N$. ∎

7.4 Prove that the relation defined in Exercise II.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.

For all $f, f', h \in F$,

$$f \sim f' \iff f - f' = 2g,\ (g \in F) \implies (h+f)-(h+f') = 2g,\ (g \in F) \iff h+f \sim h+f'.$$

Since F is abelian, wee see the relation $\sim$ defined on a free abelian group $F = F^{ab}(A)$ is compatible with the group structure. By the notation of quotient group, we have

$$F/\!\sim\, = F/2F,$$

where $2F = \{2g \in F \,|\, g \in F\}$. ∎

7.5 $\neg$ 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 would be a serious contender in a context 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

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

(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]

For all $A_1, A_2, B \in \mathrm{SL}_2(\mathbb{Z})$,

$$A_1 \sim A_2 \iff A_2 = \pm A_1 \iff BA_2 = \pm BA_1 \iff BA_1 \sim BA_2.$$

Hence $\sim$ is compatible with the group structure and $\mathrm{PSL}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})/\{I_2, -I_2\}$. In Exercise 6.10 we have shown $\mathrm{SL}_2(\mathbb{Z})$ is generated by the matrices

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

It is clear that $\mathrm{SL}_2(\mathbb{Z})$ can also be generated by the matrices

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

which implies $\mathrm{PSL}_2(\mathbb{Z})$ is generated by the cosets of the matrices s and ts. ■

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.

- Let G be the symmetric group S_4 and let $n = 2$. We can check that

$$(3\ 4)(2\ 3)^{-1} = (2\ 4\ 3) = (2\ 3\ 4)^2 \implies (3\ 4) \sim (2\ 3)$$
$$(2\ 3)(1\ 2)^{-1} = (1\ 3\ 2) = (1\ 2\ 3)^2 \implies (2\ 3) \sim (1\ 2)$$

  but $(3\ 4)(1\ 2)^{-1} = (1\ 2)(3\ 4)$ is not the square of any element in S_4.

- Suppose that G is commutative. $aa^{-1} = e^n$ implies $\sim$ is reflexive. Since

  $$a \sim b \implies ab^{-1} = g^n \ (g \in G) \implies b^{-1}a = g^{-n} \ (g^{-1} \in G) \implies b \sim a,$$

  $\sim$ is symmetric. Since G is commutative, we have

  $$\begin{aligned} a \sim b, b \sim c &\implies ab^{-1} = g_1^n, bc^{-1} = g_2^n \ (g_1, g_2 \in G) \\ &\implies ac^{-1} = ab^{-1}bc^{-1} = g_1^n g_2^n = (g_1 g_2)^n \ (g_1 g_2 \in G) \implies a \sim c, \end{aligned}$$

  which means $\sim$ is transitive. Thus we show that $\sim$ is an equivalence relation. Since

  $$a \sim b \implies ab^{-1} = g^n \implies ga(gb)^{-1} = (ag)(bg)^{-1} = g^n \implies ga \sim gb, ag \sim bg,$$

  we see $\sim$ is compatible with the group G and the equivalence class of the identity $H = \{g^n | g \in G\}$ is a 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.

For all $h \in H, g \in G$, we have

$$(ghg^{-1})^n = gh^n g^{-1} = gg^{-1} = e_G \implies ghg^{-1} \in H,$$

which means $gHg^{-1} \subseteq H$ for all $g \in G$. Thus we show that H is normal. ■

7.10 $\neg$ Let G be a group, and $H \subseteq G$ a subgroup. With notation as in Exercise II.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]

Consistent with the notation as in Exercise II.6.7, suppose

$$\gamma_g : G \longrightarrow G, \ h \longmapsto ghg^{-1}.$$

Then we have

$$\forall \gamma_g \in \mathrm{Inn}(G), \gamma_g(H) \subseteq H \iff \forall g \in G, gHg^{-1} \subseteq H \iff H \text{ is normal in } G.$$

Thus we see that if H is normal in G, γ can be restricted to H so that $\gamma|_H : H \to H$ is an automorphism on H. Let

$$i : \mathrm{Inn}(G) \longrightarrow \mathrm{Aut}(H), \ \gamma \longmapsto \gamma|_h$$

and with the property of γ we have shown in Exercise II.4.8, it is straightforward to check that

$$i(\gamma_{g_1}\gamma_{g_2}) = i(\gamma_{g_1 g_2}) = \gamma_{g_1 g_2}|_h = (\gamma_{g_1}\gamma_{g_2})|_h = \gamma_{g_1}|_h \gamma_{g_2}|_h = i(\gamma_{g_1}) i(\gamma_{g_2}).$$

That is, i is the interest homomorphism $\mathrm{Inn}(G) \to \mathrm{Aut}(H)$ that we expect. ∎

> **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 notations in Exercise II.4.8, $gaba^{-1}b^{-1}g^{-1} = \gamma_g(aba^{-1}b^{-1})$.) Prove that $[G, G]$ is normal in G. [7.12, §IV.3.3]

Since for all $g \in G, aba^{-1}b^{-1} \in [G, G]$, we have

$$gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} \in [G, G],$$

it follows that that $[G, G]$ is normal in G. Then we can show $[G, G]$ is normal in G by

$$[g_1][g_2] = [g_1g_2] = [g_1g_2(g_2^{-1}g_1^{-1}g_2g_1)] = [g_2g_1] = [g_2][g_1], \quad \forall [g_1], [g_2] \in [G, G].$$

∎

> **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 II.7.11. (Use Theorem 7.12.) Conclude that $F/[F, F] \simeq F^{ab}(A)$. (Use Proposition I.5.4.) [§6.4, 7.13, VI.1.20]

By the universal property of free group, there exists a unique homomorphism $\varphi : F \to G$ such that $\forall a \in A$, $\varphi(j(a)) = f(a)$ where $j : A \to F(A)$ is a inclusion. Note that G is commutative, we have

$$\varphi(aba^{-1}b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1} = e_G,$$

which implies $[F, F] \subseteq \ker \varphi$. Theorem 7.12 indicates that there exists a unique group homomorphism $\tilde{\varphi} : F/[F, F] \to G$ so that $\tilde{\varphi} \circ \pi = \varphi$. Now we deduce that the diagram

$$\begin{tikzcd}
A \arrow[d, "j"'] \arrow[dr, "f"] & \\
F \arrow[r, "\exists!\varphi"] \arrow[d, "\pi"'] & G \\
F/[F,F] \arrow[ur, "\exists!\tilde{\varphi}"'] &
\end{tikzcd}$$

commutes. For the diagram we see $\tilde{\varphi} \circ \pi \circ j = f$. Suppose there exists ψ such that $\psi \circ \pi \circ j = f$, which amounts to $(\psi \circ \pi) \circ j = \varphi \circ j$. By the uniqueness of φ we have $\psi \circ \pi = \varphi$. Then by the uniqueness of $\tilde{\varphi}$ we have $\psi = \tilde{\varphi}$. Thus we show that there exists unique $\tilde{\varphi}$ such that $\tilde{\varphi} \circ \pi \circ j = f$. According to the property of free abelian group, we can conclude that $F/[F, F] \simeq F^{ab}(A)$. ∎

7.13 ¬ Let A, B be sets, and $F(A), F(B)$ the corresponding free groups. Assume $F(A) \simeq F(B)$. If A is finite, prove that so is B, and $A \simeq B$. (Use Exercise II.7.12 to upgrade Exercise II.5.10.) [5.10, VI.1.20]

Exercise II.7.12 tells us that the free abelian group generated by a set is merely determined by its free group, which means

$$F(A) \simeq F(B) \implies F(A)/[F(A), F(A)] \simeq F(B)/[F(B), F(B)] \implies F^{ab}(B) \cong F^{ab}(A).$$

Then under the auspices of the conclusion in Exercise II.5.10 we complete the proof. ∎

§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

$$\frac{G_1}{H} \cong \frac{G_2}{H},$$

does it follows that $G_1 \cong G_2$. Give a proof or a counterexample.

A counterexample is given as follows. Take $H = C_3$, the cyclic group of order 3. Take $G_1 = D_6$ and $G_2 = C_6$, then one sees both G_1/H and G_2/H are C_2. But obviously G_1 and G_2 are not isomorphic, one being abelian while the other is not. ∎

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]

Since $[G/H] = 2$, there must be $G/H = \{H, G - H\}$. For any $g \in G$:

- if $g \in H$, then $gH = Hg = H$;
- if $g \in G - H$, then $gH \neq H$ and $Hg \neq H$. Thus we have $gH = Hg = G - H$.

In either case $gH = Hg$ holds for all $g \in G$, which implies H is normal in G. ∎

8.7 Let $(A|\mathscr{R})$, resp. $(A'|\mathscr{R}')$ be presentations for two groups 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].

Assume that $F(A)/R = (A|\mathscr{R})$, $F(A')/R' = (A|\mathscr{R}')$, and $F(A \amalg A')/R'' = (A \cup A'|\mathscr{R} \cup \mathscr{R}')$.

$$\begin{tikzcd}
& G & \\
F(A)/R \arrow[ur, "f"] \arrow[r, dashed, "\psi"] & F(A \amalg A')/R'' \arrow[u, dashed, "\delta"] & F(A')/R' \arrow[ul, "f'"'] \arrow[l, dashed, "\psi'"'] \\
A \arrow[u, "k"] \arrow[dr, "i"'] & F(A \amalg A') \arrow[u, "\pi"] & A' \arrow[u, "k'"'] \arrow[dl, "i'"] \\
& A \amalg A' \arrow[u, "j"'] &
\end{tikzcd}$$

According to Lemma II.1, there exist unique ψ and ψ' such that

$$\psi \circ k = \pi \circ j \circ i, \ \psi' \circ k' = \pi \circ j \circ i'.$$

Define

$$\begin{aligned} \delta : & F(A \amalg A')/R'' \longrightarrow G \\ & [\{a_1\} * \{a_1'\} * \cdots * \{a_n\} * \{a_n'\}] \longmapsto f([\{a_1\}])f'([\{a_1'\}]) \cdots f([\{a_n\}])f'([\{a_n'\}]). \end{aligned}$$

where $*$ means the junction of words and $\{a_i\} = a_{i1} * a_{i2} * \cdots * a_{im_i}$, $a_{ij} \in A$ $(1 \le i \le n, 1 \le j \le m_i)$ and $\{a_i'\} = a_{i1}' * a_{i2}' * \cdots * a_{im_i'}$, $a_{ij'} \in A$ $(1 \le i \le n, 1 \le j' \le m_i')$. It is routine to check that δ is a well-defined homomorphism such that

$$\delta \circ \psi = f, \ \delta \circ \psi' = f'.$$

Then verify that if $\hat{\delta}$ is a homomorphism such that

$$\delta \circ \psi = f, \ \delta \circ \psi' = f',$$

there must be $\hat{\delta} = \delta$. After these tasks are done, we can conclude that $F(A \amalg A')/R''$ satisfies the universal property of coproduct.

∎

§9. Group actions

§10. Group objects in categories

Chapter III Rings and modules

§1. Definition of ring

1.1 $\triangleright$ Prove that if $0 = 1$ in a ring R, then R is a zero-ring. [§1.2]

For any x in the ring R, we have

$$1 \cdot x = x, \qquad 0 \cdot x = 0.$$

Since $0 = 1$ we see that $x = 0$, which implies R is a ring with only one element 0. ■

1.2 $\neg$ Let S be a set, and define operations on the power set $\mathscr{P}(S)$ of S by setting $\forall A, B \in \mathscr{P}(S)$ $$A + B := (A \cup B) \backslash (A \cap B) \quad , \quad A \cdot B = A \cap B$$ Prove that $(\mathscr{P}(S), +, \cdot)$ is a commutative ring. [2.3, 3.15]

First, we need to check that $(\mathscr{P}(S), +)$ is an abelian group:

- associativity:

$$\begin{aligned}
&(A + B) + C \\
&= ((A \cup B) \backslash (A \cap B)) + C \\
&= ((A \cup B) \cap (A^C \cup B^C)) + C \\
&= (A \cap (A^C \cup B^C)) \cup (B \cap (A^C \cup B^C)) + C \\
&= (A \cap B^C) \cup (A^C \cap B) + C \\
&= (((A \cap B^C) \cup (A^C \cap B)) \cap C^C) \cup (((A \cap B^C) \cup (A^C \cap B))^C \cap C) \\
&= ((A \cap B^C \cap C^C) \cup (A^C \cap B \cap C^C)) \cup ((A^C \cup B) \cap (A \cup B^C) \cap C) \\
&= ((A \cap B^C \cap C^C) \cup (A^C \cap B \cap C^C)) \cup ((A^C \cap B^C) \cup (A \cap B) \cap C) \\
&= (A \cap B^C \cap C^C) \cup (A^C \cap B \cap C^C) \cup (A^C \cap B^C \cap C) \cup (A \cap B \cap C) \\
&= (A \cap (B \cap C) \cup (B^C \cap C^C)) \cup ((A^C \cap B \cap C^C) \cup (A^C \cap B^C \cap C)) \\
&= (A \cap (B^C \cup C) \cap (B \cup C^C)) \cup ((A^C \cap B \cap C^C) \cup (A^C \cap B^C \cap C)) \\
&= (A \cap ((B \cap C^C) \cup (B^C \cap C))^C) \cup (A^C \cap ((B \cap C^C) \cup (B^C \cap C))) \\
&= A + ((B \cap C^C) \cup (B^C \cap C)) \\
&= A + (B + C);
\end{aligned}$$

- commutativity:

$$A + B = (A \cup B) \backslash (A \cap B) = (B \cup A) \backslash (B \cap A) = B + A;$$

- additive identity: the additive identity is $\varnothing$ since

$$A + \varnothing = (A \cup \varnothing) \backslash (A \cap \varnothing) = A; \backslash \varnothing = A$$

- inverse: the inverse of some set A is just itself since

$$A + A = (A \cup A) \backslash (A \cap A) = A \backslash A = \varnothing.$$

Then we have to show that $(\mathscr{P}(S), \cdot)$ is a commutative monoid, which clearly holds with the multiplicative identity S. What is left to show is the distributive properties and the check is straightforward.

$$\begin{aligned}
&(A + B) \cdot C \\
&= ((A \cap B^C) \cup (A^C \cap B)) \cap C \\
&= (A \cap B^C \cap C) \cup (A^C \cap B \cap C) \\
&= (A \cap C \cap (B^C \cup C^C)) \cup ((A^C \cup C^C) \cap (B \cap C)) \\
&= (A \cap C \cap (B \cap C)^C) \cup ((A \cap C)^C \cap (B \cap C)) \\
&= A \cdot C + B \cdot C.
\end{aligned}$$

■

1.3 $\neg$ 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]

To make $(R^S, +, \cdot)$ a ring , for all $f, g \in R^S$ we define addition and multiplication as

$$\begin{aligned}
f + g : S \longrightarrow R, \quad x \longmapsto f(x) + g(x) \\
f \cdot g : S \longrightarrow R, \quad x \longmapsto f(x) \cdot g(x).
\end{aligned}$$

■

1.4 ▷ The set of $n \times n$ matrices with entries in a ring R isdenoted $\mathcal{M}_n(R)$. Prove that componentwise addition and matrix multiplication makes $\mathcal{M}_n(R)$ into a ring, for any ring R. The notation $\mathfrak{gl}_n(R)$ is also commonly used, especially $R = \mathbb{R}$ or $\mathbb{C}$ (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:

- $\mathfrak{sl}_n(\mathbb{R}) = \{M \in \mathfrak{gl}_n(\mathbb{R}) | \mathrm{tr}(M) = 0\}$;
- $\mathfrak{sl}_n(\mathbb{C}) = \{M \in \mathfrak{gl}_n(\mathbb{C}) | \mathrm{tr}(M) = 0\}$;
- $\mathfrak{so}_n(\mathbb{R}) = \{M \in \mathfrak{sl}_n(\mathbb{R}) | M + M^t = 0\}$;
- $\mathfrak{su}(n) = \{M \in \mathfrak{sl}_n(\mathbb{C}) | M + M^\dagger = 0\}$.

Here $\mathrm{tr}(M)$ is the trace of M, that is, the sum of its diagonal entries. The other notation matches the notation used in Exercise II.6.1. Can we make rings of these sets, by endowing them of 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]

It is plain to show $\mathcal{M}_n(R)$ is a ring according to the definition. For multiplicative associativity, it follows that for all $A, B, C \in \mathcal{M}_n(R)$,

$$\begin{aligned}
&((AB)C)_{\alpha,\delta} \\
&= \sum_{i=1}^{n} (AB)_{\alpha,i} c_{i,\delta} \\
&= \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{\alpha,j} b_{j,i} \right) c_{i,\delta} \\
&= \sum_{i=1}^{n} \sum_{j=1}^{n} (a_{\alpha,j} b_{j,i}) c_{i,\delta} \\
&= \sum_{j=1}^{n} \sum_{n=1}^{n} a_{\alpha,j} (b_{j,i} c_{i,\delta}) \\
&= \sum_{j=1}^{n} a_{\alpha,j} \left(\sum_{i=1}^{n} b_{j,i} c_{i,\delta} \right) \\
&= \sum_{j=1}^{n} a_{\alpha,j} (BC)_{j,\delta} \\
&= (A(BC))_{\alpha,\delta}.
\end{aligned}$$

Under the ordinary addition and multiplication of matrices, $\mathfrak{sl}_n(\mathbb{R}), \mathfrak{sl}_n(\mathbb{C}), \mathfrak{so}_n(\mathbb{R}), \mathfrak{su}_n(\mathbb{C})$ are not rings. In fact, they are not closed under the multiplication. ∎

1.5 Let R be a ring. If a, b are zero-divisors in R, is $a+b$ necessarily a zero-divisor?

That is not true. Let's take $\mathbb{Z}/6\mathbb{Z}$ as an counterexample. Though both $[2]_6$ and $[3]_6$ are zero-divisors, their sum $[5]_6$ is not a zero-divisor. ∎

1.6 ¬ An element a of a ring R is *nilpotent* if $a^n = 0$ for some n.

1. Prove that if a and b are nilpotent in R and $ab = ba$, then $a+b$ is also nilpotent.
2. Is the hypothesis $ab = ba$ in the previous statement necessary for its conclusion to hold?

[3.12]

1. Assume that $a^n = b^m = 0$ and let $k = 2\max\{n, m\}$. If $ab = ba$, we can get

$$(a+b)^k = \sum_{p=0}^{\frac{k}{2}} \binom{k}{p} a^k b^{k-p} + \sum_{p=\frac{k}{2}+1}^{k} \binom{k}{p} a^k b^{k-p} = \sum_{p=0}^{\frac{k}{2}} \binom{k}{p} a^k \cdot 0 + \sum_{p=\frac{k}{2}+1}^{k} \binom{k}{p} 0 \cdot b^{k-p} = 0,$$

which means $a+b$ is also nilpotent.

2. The hypothesis $ab = ba$ is necessary. A counterexample can be found in the ring $\mathfrak{gl}_2(\mathbb{R})$. Let

$$a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

and then we have $a^2 = b^2 = 0$. In other words, a and b are nilpotent. However, by diagonalization we see that

$$(a+b)^n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^n \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}^{-1} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Thus in such case, $a+b$ is no longer nilpotent.

∎

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 more than 2 solutions.

It clearly holds that $1 \cdot 1 = 1$ and $(-1) \cdot (-1) = ((-1) \times (-1))1 \cdot 1 = 1$. That is to say, $x = \pm 1$ are the solutions to the equation $x^2 = 1$. Note that if there exists x in an integral domain such that $x^2 = 1$, then we have

$$(x-1) \cdot (x+1) = x^2 - 1 = 0,$$

which implies $x - 1 = 0$ or $x + 1 = 0$. Therefore, we can assert $x = \pm 1$ are the solutions. In the ring $\mathbb{Z}/8\mathbb{Z}$, $[3]_8$ and $[5]_8$ are also the solutions to the equation $x^2 = 1$. ∎

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.

Since $a \in R$ is a right unit, it cannot be a left-zero-divisor. Assume there exist two distinct elements $x, y \in R$ such that $xa = ya = 1$ and it deduces $(y - x)a = 0$. Thus we show that a a right-zero-divisor. ■

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]

Define

$$(0, 1) \cdot (0, 1) = (0, 1), \quad (0, 1) \cdot (1, 0) = (0, 0), \quad (1, 0) \cdot (1, 0) = (1, 0),$$

and the the rest definition of multiplication will be determined uniquely according to field properties. For example, we have no alternatives but to define

$$(0, 1) \cdot (1, 1) = (0, 1) \cdot ((0, 1) + (1, 0)) = (0, 1) \cdot (0, 1) + (0, 1) \cdot (1, 0) = (0, 1) + (0, 0) = (0, 1).$$

Then we can check $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ forms a field by definition. ■

1.12 Just as complex numbers may be viewed 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 commute with $\mathbb{R}$ and satisfy the following relations:

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

Addition in $\mathbb{H}$ is defined componentwise, while multiplication is defined by imposing distributivity and applying the relations. For example,

$$(1+i+j)\cdot(2+k) = 1\cdot 2+i\cdot 2+j\cdot 2+1\cdot k+i\cdot k+j\cdot k = 2+2i+2j+k-j+i = 2+3i+j+k.$$

(i) Verify that this prescription does indeed define a ring.

(ii) Compute $(a + bi + cj + dk)(a - bi - cj - dk)$, where $a, b, c, d \in \mathbb{R}$.

(iii) Prove that $\mathbb{H}$ is a division ring. Elements of $\mathbb{H}$ are called quaternions. Note that $Q_8 := \{\pm 1, \pm i, \pm j, \pm k\}$ forms a subgroup of the group of units of $\mathbb{H}$; it is a noncommutative group of order 8, called the quaternionic group.

(iv) List all subgroups of Q_8, and prove that they are all normal.

(v) Prove that Q_8, D_8 are not isomorphic.

(vi) Prove that Q_8 admits the presentation $(x, y | x^2 y^{-2}, y^4, xyx^{-1}y)$.

[§II.7.1, 2.4, IV.1.12, IV.5.16, IV.5.17, V.6.19]

(i) Verifying the $(\mathbb{H}, +)$ is a abelian group is immediate and we just omitted it. It is easy to see the multiplicative identity is 1 and the distributive properties are guaranteed by definition. The check of the associativity of multiplication looks straightforward but tedious.

$$\begin{aligned}
&((a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k)) \cdot (a_3 + b_3 i + c_3 j + d_3 k) \\
= &[-c_3 (a_2 c_1 + a_1 c_2 + b_2 d_1 - b_1 d_2) - b_3 (a_2 b_1 + a_1 b_2 - c_2 d_1 + c_1 d_2) \\
&+ a_3 (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) - d_3 (-b_2 c_1 + b_1 c_2 + a_2 d_1 + a_1 d_2)] \\
&+ [-c_3 (-b_2 c_1 + b_1 c_2 + a_2 d_1 + a_1 d_2) + a_3 (a_2 b_1 + a_1 b_2 - c_2 d_1 + c_1 d_2) \\
&+ b_3 (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + d_3 (a_2 c_1 + a_1 c_2 + b_2 d_1 - b_1 d_2)] i \\
&+ [b_3 (-b_2 c_1 + b_1 c_2 + a_2 d_1 + a_1 d_2) + a_3 (a_2 c_1 + a_1 c_2 + b_2 d_1 - b_1 d_2) \\
&+ c_3 (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) - d_3 (a_2 b_1 + a_1 b_2 - c_2 d_1 + c_1 d_2)] j \\
&+ [a_3 (-b_2 c_1 + b_1 c_2 + a_2 d_1 + a_1 d_2) - b_3 (a_2 c_1 + a_1 c_2 + b_2 d_1 - b_1 d_2) \\
&+ c_3 (a_2 b_1 + a_1 b_2 - c_2 d_1 + c_1 d_2) + d_3 (a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2)] k
\end{aligned}$$

$$
\begin{aligned}
&(a_1 + b_1 i + c_1 j + d_1 k) \cdot ((a_2 + b_2 i + c_2 j + d_2 k) \cdot (a_3 + b_3 i + c_3 j + d_3 k)) \\
= &[-d_1 (a_3 d_2 + a_2 d_3 - b_3 c_2 + b_2 c_3) - c_1 (a_3 c_2 + a_2 c_3 + b_3 d_2 - b_2 d_3) \\
&- b_1 (a_3 b_2 + a_2 b_3 - c_3 d_2 + c_2 d_3) + a_1 (a_2 a_3 - b_2 b_3 - c_2 c_3 - d_2 d_3)] \\
&+ [c_1 (a_3 d_2 + a_2 d_3 - b_3 c_2 + b_2 c_3) - d_1 (a_3 c_2 + a_2 c_3 + b_3 d_2 - b_2 d_3) \\
&+ a_1 (a_3 b_2 + a_2 b_3 - c_3 d_2 + c_2 d_3) + b_1 (a_2 a_3 - b_2 b_3 - c_2 c_3 - d_2 d_3)] i \\
&+ [-b_1 (a_3 d_2 + a_2 d_3 - b_3 c_2 + b_2 c_3) + a_1 (a_3 c_2 + a_2 c_3 + b_3 d_2 - b_2 d_3) \\
&+ d_1 (a_3 b_2 + a_2 b_3 - c_3 d_2 + c_2 d_3) + c_1 (a_2 a_3 - b_2 b_3 - c_2 c_3 - d_2 d_3)] j \\
&+ [a_1 (a_3 d_2 + a_2 d_3 - b_3 c_2 + b_2 c_3) + b_1 (a_3 c_2 + a_2 c_3 + b_3 d_2 - b_2 d_3) \\
&- c_1 (a_3 b_2 + a_2 b_3 - c_3 d_2 + c_2 d_3) + d_1 (a_2 a_3 - b_2 b_3 - c_2 c_3 - d_2 d_3)] k
\end{aligned}
$$

(ii) Expand it by distributive properties and we get

$$
\begin{aligned}
&(a + bi + cj + dk)(a - bi - cj - dk) \\
&= a^2 - abi - acj - adk + abi + b^2 - bck + bdj + acj + bck + c^2 - cdi + adk - bdj + cdi + d^2 \\
&= a^2 + b^2 + c^2 + d^2.
\end{aligned}
$$

(iii) Applying the results in (ii) we see that for any non-zero element $a + bi + cj + dk \in \mathbb{H}$,

$$
(a + bi + cj + dk) \cdot \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2} \cdot (a + bi + cj + dk) = 1,
$$

which implies $a + bi + cj + dk$ is a two-sided unit. Thus we show that $\mathbb{H}$ is a division ring.

(iv) Q_8 has 6 subgroups: $\{1\}$, $\{1, -1\}$, $\{1, -1, i, -i\}$, $\{1, -1, j, -j\}$, $\{1, -1, k, -k\}$, Q_8. We can just prove that they are all normal by the definition of normal subgroups.

(v) Note that $D_8 = \{e, r, r^2, r^3, s_1, s_2, s_3, s_4\}$ has 7 subgroups: $\{e\}$, $\{e, r, r^2, r^3\}$, $\{e, s_1\}$, $\{e, s_2\}$, $\{e, s_3\}$, $\{e, s_4\}$, D_8, while Q_8 has 6 subgroups. Thus Q_8, D_8 are not isomorphic.

(vi) Let $P = (x, y | x^2 y^{-2}, y^4, xyx^{-1}y)$. The relation $x^2 y^{-2} = e$ implies $x^2 = y^2$ and the relation $xyx^{-1}y = e$ implies $yx = yx^{-1}x^2 = x^{-1}y^{-1}x^2 = x^3 y^3 x^2 = x^3 y^5 = x^3 y$. First, we can always replace yx by $x^3 y$ until we obtain a word of the form $x^i y^j$. Then applying $x^4 = y^4 = e$ and replace y^2 by x^2, we can transform it into the form $x^i y^j$ with $0 \le i \le 3$ and $0 \le j \le 1$. Thus we see P has at most 8 elements.

Next we will complete our proof by means of the Lemma II.1 in the appendix. Define a mapping

$$
\begin{aligned}
f : \{x, y\} \longrightarrow Q_8, \quad & x \longmapsto i, \\
& y \longmapsto j.
\end{aligned}
$$

Let $\varphi : F(\{x,y\}) \to Q_8$ be the unique homomorphism induced by the universal property of free group. Since

$$\begin{aligned}
&\varphi(x^2y^{-2}) = i^2j^{-2} = 1,\\
&\varphi(y^4) = j^4 = 1,\\
&\varphi(xyx^{-1}y) = iji^{-1}j = 1,
\end{aligned}$$

we see $\mathscr{R} = \{x^2y^{-2}, y^4, xyx^{-1}y\} \subset \ker\varphi$. And it is immediate to show that Q_8 can be generated by $\{i,j\}$. Thus according to the lemma, there exists a unique homomorphism $\psi : P \to Q_8$ such that $f = \psi \circ \pi \circ i$ and actually ψ is surjective.

$$\begin{tikzcd}
P \arrow[dr, dashed, "\exists!\psi"] & \\
F(\{x,y\}) \arrow[u, "\pi"] \arrow[r, dashed, "\varphi"] & Q_8 \\
\{x,y\} \arrow[u, "i"] \arrow[ur, "f"'] &
\end{tikzcd}$$

Hence we get the inequality of cardinality $|P| \geq |Q_8|$. Since we have shown $|P| \leq 8 = |Q_8|$, there must be $|P| = |Q_8| = 8$, which implies ψ is indeed an isomorphism. Finally we conclude that $Q_8 \cong (x,y|x^2y^{-2}, y^4, xyx^{-1}y)$ and complete our proof.

∎

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]

Assume

$$f(x) = \sum_{i\geq 0} a_i x^i, \quad g(x) = \sum_{i\geq 0} b_i x^i, \quad a_i, b_i \in R$$

and n, m are respectively the largest integers p, q for which a_p, b_q are non-zero. In others words, we have $a_n \neq 0$, $a_i = 0$ for $i > n$ and $b_m \neq 0$, $b_i = 0$ for $i > m$. Since

$$f(x) + g(x) = \sum_{i\geq 0} (a_i + b_i)x^i = \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)x^i,$$

we see that

$$\deg(f(x)+g(x)) \leq \max\{n,m\} = \max(\deg(f(x)), \deg(g(x))).$$

Now Suppose that R is an integral domain. Noticing $a_n \neq 0$ and $b_m \neq 0$ implies $a_n b_m \neq 0$, we can see

$$f(x)\cdot g(x) = \sum_{k\geq 0}\sum_{i+j=k} a_i b_j x^{i+j} = \sum_{k=0}^{n+m}\sum_{i+j=k} a_i b_j x^{i+j}$$

has a degree of $n+m$. That is,

$$\deg(f(x)\cdot g(x)) = \deg(f(x)) + \deg(g(x)).$$

■

1.15 $\triangleright$ Prove that $R[x]$ is an integral domain if and only if R is an integral domain. [§1.3]

Assume R is an integral domain. Exercise III.1.14 tells us if $f(x)$, $g(x) \in R[x]$ are nonzero polynomials, we have

$$\deg(f(x)\cdot g(x)) = \deg(f(x)) + \deg(g(x)),$$

which implies $f(x)\cdot g(x)$ is also nonzero polynomial. Thus we show $R[x]$ is a integral domain.

Conversely, assume $R[x]$ is an integral domain. Note that given any $a, b \in R$, they also belong to $R[x]$. Hence we obtain

$$a \neq 0, b \neq 0 \implies ab \neq 0,$$

which means R is an integral domain. ■

1.16 Let R be a ring, and consider the ring of power series $R[[x]]$ (cf. §1.3).

1. Prove that a power 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 $1-x$ in $R[[x]]$?
2. Prove that $R[[x]]$ is an integral domain if and only if R is.

1. If a_0 is a unit in R then we can assume there exists $b_0 \in R$ such that $a_0 b_0 = 1$. Let

$$f(x) = \sum_{n\geq 0} a_n x^n, \quad g(x) = \sum_{n\geq 0} b_n x^n,$$

where

$$b_n = -b_0 \sum_{i=1}^{n} a_i b_{n-i}, \quad n \geq 1.$$

Noticing that

$$a_0 b_n = -a_0 b_0 \sum_{i=1}^{n} a_i b_{n-i} = -\sum_{i=1}^{n} a_i b_{n-i}, \quad n \geq 1,$$

we have

$$\begin{aligned} f(x)g(x) &= \sum_{n\geq 0} \sum_{i=0}^{n} a_{n-i} b_i x^n \\ &= 1 + \sum_{n\geq 1} \sum_{i=0}^{n} a_i b_{n-i} x^n \\ &= 1 + \sum_{n\geq 1} \left(a_0 b_n + \sum_{i=1}^{n} a_i b_{n-i} \right) x^n \\ &= 1 + \sum_{n\geq 1} (a_0 b_n - a_0 b_n) x^n \\ &= 1. \end{aligned}$$

Hence we show $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ is a unit.

For the other direction, supposing $f(x) = a_0 + a_1 x + a_2 x^2 + \cdots$ is a unit, then there exists $g(x) = b_0 + b_1 x + b_2 x^2 + \cdots$ such that

$$f(x)g(x) = a_0 b_0 + \sum_{n\geq 1} \sum_{i=0}^{n} a_i b_{n-i} x^n = 1.$$

By comparing the both sides of the equality we can find $a_0 b_0 = 1$, which implies a_0 is a unit in R.

We can check that the inverse of $1 - x$ in $R[[x]]$ is $1 + x + x^2 + \cdots$ since

$$(1 - x) \sum_{i\geq 0} x^i = \sum_{i\geq 0} x^i - \sum_{i\geq 0} x^{i+1} = 1.$$

2. Suppose R is an integral domain. If $f(x)$, $g(x) \in R[x]$ are nonzero polynomials, we can assume that

$$f(x) = \sum_{i\geq 0} a_i x^i, \quad g(x) = \sum_{i\geq 0} b_i x^i, \quad a_i, b_i \in R$$

and that n, m are respectively the smallest integers p, q for which a_p, b_q are non-zero. In others words, we have $a_n \neq 0$, $a_i = 0$ for $i < n$ and $b_m \neq 0$, $b_i = 0$ for $i < m$. Noticing $a_n \neq 0$ and $b_m \neq 0$ implies $a_n b_m \neq 0$, we can see

$$f(x) \cdot g(x) = \sum_{k\geq 0} \sum_{i+j=k} a_i b_j x^{i+j} = a_n b_m x^{n+m} + \sum_{k\geq n+m+1} \sum_{i+j=k} a_i b_j x^{i+j} \neq 0.$$

Thus we show $R[[x]]$ is an integral domain.

Conversely, assume that $R[[x]]$ is an integral domain. Note that given any $a, b \in R$, they also belong to $R[[x]]$. Hence we obtain

$$a \neq 0, b \neq 0 \implies ab \neq 0,$$

which means that R is also an integral domain.

■

§2. The category Ring

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]

Suppose that φ is a homomorphism from a zero-ring O to a ring R. Since $\varphi(0_O) = 0_R$, $\varphi(1_O) = 1_R$, $0_O = 1_O$, we have $0_R = 1_R$, which implies that R is a zero-ring. ■

2.4 Define functions $\mathbb{H} \to \mathfrak{gl}_4(\mathbb{R})$ and $\mathbb{H} \to \mathfrak{gl}_2(\mathbb{C})$ (cf. Exercise III.1.4 and 1.12) by

$$a + bi + cj + dk \longmapsto \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix}$$

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

for all $a, b, c, d \in \mathbb{R}$. Prove that both functions are injective ring homomorphisms. Thus, quaternions may be viewed as real or complex matrices.

Let f be the function $\mathbb{H} \to \mathfrak{gl}_4(\mathbb{R})$ described above. For simplicity, we omit trivial check and only verify f preserves multiplication

$$\begin{aligned}
&f((a_1 + b_1 i + c_1 j + d_1 k) \cdot (a_2 + b_2 i + c_2 j + d_2 k)) \\
&= f((a_1 a_2 - b_1 b_2 - c_1 c_2 - d_1 d_2) + (a_2 b_1 + a_1 b_2 - c_2 d_1 + c_1 d_2) i \\
&\quad + (a_2 c_1 + a_1 c_2 + b_2 d_1 - b_1 d_2) j + (a_2 d_1 + a_1 d_2 - b_2 c_1 + b_1 c_2) k) \\
&= \begin{pmatrix} a_1 & b_1 & c_1 & d_1 \\ -b_1 & a_1 & -d_1 & c_1 \\ -c_1 & d_1 & a_1 & -b_1 \\ -d_1 & -c_1 & b_1 & a_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 & c_2 & d_2 \\ -b_2 & a_2 & -d_2 & c_2 \\ -c_2 & d_2 & a_2 & -b_2 \\ -d_2 & -c_2 & b_2 & a_2 \end{pmatrix} \\
&= f(a_1 + b_1 i + c_1 j + d_1 k) f(a_2 + b_2 i + c_2 j + d_2 k)
\end{aligned}$$

■

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 $\mathrm{SU}_2(\mathbb{C})$ (cf. Exercise II.6.3). [4.10, IV.5.17 V.6.19]

According to Exercise III.2.4, $w \in \mathbb{H}^*$ can be viewed as a matrix $i(w) \in \mathfrak{gl}_2(\mathbb{C})$ where $i : \mathbb{H} \to \mathfrak{gl}_2(\mathbb{C})$ is a monomorphism in Ring. Then the function $N : \mathbb{H}^* \to \mathbb{R}^+$ can be just viewed as the determinant mapping $\det : i(\mathbb{H}^*) \subset \mathfrak{gl}_2(\mathbb{C}) \to \mathbb{R}^+$. More precisely, it means $N = \det \circ i$. We can check that

$$N(w_1w_2) = \det(i(w_1w_2)) = \det(i(w_1)i(w_2)) = \det(i(w_1))\det(i(w_2)) = N(w_1)N(w_2)$$

and

$$w \in \ker N \iff N(w) = \det(i(w)) = 1 \iff i(w) \in \mathrm{SU}_2(\mathbb{C}).$$

Therefore, N is a homomorphism and $\ker N$ isomorphic to $\mathrm{SU}_2(\mathbb{C})$. ■

2.6 Verify the 'extension property' of polynomial rings, stated in Example 2.3. [§2.2]

Define the following ring homomorphisms

$$\begin{aligned} \alpha : R &\longrightarrow S, \quad r \longmapsto \alpha(r) \\ \epsilon : R &\longrightarrow R[x], \quad r \longmapsto r, \end{aligned}$$

and functions

$$\begin{aligned} j : \{s\} &\longrightarrow R[x], \quad s \longmapsto x, \\ i : \{s\} &\longrightarrow S, \quad s \longmapsto s. \end{aligned}$$

Assume that $s \in S$ is an element commuting with $\alpha(r)$ for all $r \in R$, we are to show that there exists a unique ring homomorphism $\overline{\alpha} : R[x] \to S$ such that the following diagram commutes.

$$\begin{tikzcd} R \arrow[d, "\epsilon"'] \arrow[dr, "\alpha"] & \\ R[x] \arrow[r, dashed, "\exists!\overline{\alpha}"] & S \\ \{s\} \arrow[u, "j"] \arrow[ur, hook, "i"'] & \end{tikzcd}$$

Uniqueness. If $\overline{\alpha}$ exists, then the postulated commutativity of the diagram means that for all $f(x) = \sum_{n\geq 0} a_n \in R[x]$, there must be

$$\overline{\alpha}\left(f(x)\right) = \overline{\alpha}\left(\sum_{n\geq 0} a_n x^n\right) = \sum_{n\geq 0} \overline{\alpha}\left(a_n\right)\overline{\alpha}\left(x\right)^n = \sum_{n\geq 0} \alpha\left(a_n\right) s^n.$$

That is, $\overline{\alpha}$ is unique.
Existence. The only choice is to define

$$\overline{\alpha}: \ R[x] \longrightarrow S, \quad \sum_{n\geq 0} a_n x^n \longmapsto \sum_{n\geq 0} \alpha\left(a_n\right) s^n$$

and to check whether it is a ring homomorphism.

1. Preserving addition:

$$\begin{aligned}
\overline{\alpha}\left(\sum_{n\geq 0} a_n x^n + \sum_{n\geq 0} b_n x^n\right) &= \overline{\alpha}\left(\sum_{n\geq 0}(a_n + b_n)x^n\right) \\
&= \sum_{n\geq 0} \alpha\left(a_n + b_n\right) s^n \\
&= \sum_{n\geq 0} \alpha\left(a_n\right) s^n + \sum_{n\geq 0} \alpha\left(b_n\right) s^n \\
&= \overline{\alpha}\left(\sum_{n\geq 0} a_n x^n\right) + \overline{\alpha}\left(\sum_{n\geq 0} b_n x^n\right).
\end{aligned}$$

2. Preserving multiplication:

$$\begin{aligned}
\overline{\alpha}\left(\sum_{n\geq 0} a_n x^n \sum_{n\geq 0} b_n x^n\right) &= \overline{\alpha}\left(\sum_{n\geq 0}\sum_{i+j=n} a_i b_j x^n\right) \\
&= \sum_{n\geq 0} \alpha\left(\sum_{i+j=n} a_i b_j\right) s^n \\
&= \sum_{n\geq 0}\sum_{i+j=n} \alpha\left(a_i\right) s^i \alpha\left(b_j\right) s^j \\
&= \left(\sum_{n\geq 0} \alpha\left(a_n\right) s^n\right)\left(\sum_{n\geq 0} \alpha\left(b_n\right) s^n\right) \\
&= \overline{\alpha}\left(\sum_{n\geq 0} a_n x^n\right) \overline{\alpha}\left(\sum_{n\geq 0} b_n x^n\right).
\end{aligned}$$

3. Preserving identity element:

$$\overline{\alpha}(1_R) = \alpha(1_R) = 1_S.$$

Integrating the two parts we finally conclude there exists a unique ring homomorphism $\overline{\alpha}$ such that the diagram commutes.

$\blacksquare$

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]

It determines a function $f : \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ sends all elements to identity, that is, $f([0]_2) = [0]_2$, $f([1]_2) = [0]_2$. ■

2.8 Prove that every subring of a field is an integral domain.

Suppose $\varphi : R \hookrightarrow K$ is a inclusion homomorphism. If $a \neq 0$, we have

$$ab = ac \implies \varphi(a)\varphi(b) = \varphi(a)\varphi(c) \implies \varphi(b) = \varphi(c) \implies b = c.$$

Due to the community of field it also holds that $ba = ca$. Thus we show R is an integral domain. ■

2.9 $\neg$ 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]

Denote the center of R by $Z(R)$. We can check that

1. for all $x, y \in Z(R)$, for all $r \in R$,
$$(x - y)r = xr - yr = rx - ry = r(x - y) \implies x - y \in Z(R);$$
2. for all $r \in R$,
$$1r = r1 \implies 1 \in Z(R);$$
3. for all $x, y \in Z(R)$, for all $r \in R$,
$$(xy)r = xry = r(xy) \implies xy \in Z(R).$$

Thus we show that $Z(R)$ is a subring of R. If R is a division ring, then $Z(R)$ is a also a division ring. Note that for all $x, y \in Z(R)$, $xy = yx$, we see that $Z(R)$ is a commutative division ring, namely field. ■

2.10 $\neg$ The *centralizer* of an element a of a ring R consists of the elements $r \in R$ such that $ar = ra$. Prove that the centralizer of a is a subring of R, for every $a \in R$. Prove that the center of R is the intersection of all its centralizers. Prove that every centralizer in a division ring is a division ring. [2.11, IV.2.17, VII.5.16]

Denote the centralizer of an element a of R by $Z_a(R)$. That is,

$$Z_a(R) = \{r \in R \mid ar = ra\}.$$

We can check that

1. for all $x, y \in Z_a(R)$,
$$(x - y)a = xa - ya = ax - ay = a(x - y) \implies x - y \in Z_a(R);$$

2. $$1a = a1 \implies 1 \in Z_a(R);$$

3. for all $x, y \in Z_a(R)$,
$$(xy)a = xay = a(xy) \implies xy \in Z_a(R).$$

Thus we show that $Z_a(R)$ is a subring of R.

By definition we have $Z(R) \subseteq Z_a(R)$ for all $a \in R$, which implies $Z(R) \subseteq \bigcap_{a\in R} Z_a(R)$. Assume $s \in \bigcap_{a\in R} Z_a(R)$, then we see $sa = as$ for all $a \in R$, which means $s \in Z(R)$ and accordingly $\bigcap_{a\in R} Z_a(R) \subseteq Z(R)$. Thus we deduce that $Z(R) = \bigcap_{a\in R} Z_a(R)$.

If R is a division ring and $r \in Z_a(R)$, we can assume that there exists $a \in R$ such as $ar = ra$, which means that
$$r^{-1}(ar)r^{-1} = r^{-1}(ra)r^{-1} \implies r^{-1}a = ar^{-1}.$$

According to the definition of $Z_a(R)$, we see $r^{-1} \in Z_a(R)$. Thus we show that $Z_a(R)$ is a division ring. ∎

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 III.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 III.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]

If R is not commutative, then its center $Z(R)$ is a proper subring of R, which means $|Z(R)| < p^2$. By considering $Z(R)$ as a subgroup of the underlying abelian group R, we can deduce that $|Z(R)|$ divides p^2 according to the Lagrange theorem. Thus we see that $Z(R)$ consist of p elements. Given any $r \in R - Z(R)$, in Exercise III.2.10 we have shown that $Z_r(R)$ is a subring of R and $Z(R) \in Z_r(R)$. By the definition of $Z_r(R)$, it is clear that $r \in Z_r(R)$. Hence we have $Z(R) \cup \{r\} \subseteq Z_r(R)$ and $|Z_r(R)| > p$. Again by Lagrange theorem we have

$|Z_r(R)|$ divides p^2, which forces $|Z_r(R)| = p^2$. Thus we show that $Z_r(R) = R$. Note that $Z_a(R) = R$ for all $a \in Z(R)$. We have $Z_a(R) = R$ for all $a \in R$. In Exercise III.2.10, we have derived that $\bigcap_{a\in R} Z_a(R) \subseteq Z(R)$, which implies $R \subseteq Z(R)$. Thus we have $Z(R) = R$, which contradicts with the previous deduction that $Z(R)$ is a proper subring of R. Therefore, we can conclude that R is commutative. ∎

> **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 non-isomorphic 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 2.16.) [§2.1]

∎

§3. Ideals and quotient rings

> **3.1** Prove that the image of a ring homomorphism $\varphi : R \to S$ is a subring of S. What can you say about φ, if its image is an ideal of S? What can you say about φ, if its kernel is a subring of R?

We can see that $\operatorname{im}\varphi$ is a subring of S from the canonical decomposition

$$\begin{tikzcd} R \arrow[r, two heads] \arrow[rrr, bend left, "\varphi"] & R/\ker\varphi \arrow[r, "\sim", "\tilde{\varphi}"'] & \operatorname{im}\varphi \arrow[r, hook] & S \end{tikzcd}$$

If $\operatorname{im}\varphi$ is an ideal, then $s \in S, 1 \in \operatorname{im}\varphi \implies s \in \operatorname{im}\varphi$. So $\operatorname{im}\varphi = S$ and φ is an epimorphism. Since $\ker\varphi$ is a ideal, if it is also a subring, we have $\ker\varphi = R$. ∎

> **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]

In Ab we see $\varphi^{-1}(J)$ is a subgroup of R. For all $r \in R$, $a \in \varphi^{-1}(J)$, we have

$$\varphi(ra) = \varphi(r)\varphi(a) \in J \implies ra \in \varphi^{-1}(J).$$

Similarly we can obtain $ar \in \varphi^{-1}(J)$. Therefore, we conclude that $I = \varphi^{-1}(J)$ is an ideal of R. ∎

3.3 $\neg$ Let $\varphi : R \to S$ be a ring homomorphism, and let J be an 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]

- Let $\varphi : \mathbb{Z} \hookrightarrow \mathbb{Q}$ and $J = \mathbb{Z}$. It is clear that $\varphi(J) = \mathbb{Z}$ is not an ideal of $\mathbb{Q}$.
- Assume that φ is surjective. In Ab we see $\varphi(J)$ is a subgroup of S. For all $a' = \varphi(a) \in \varphi(J)$, $r' = \varphi(r) \in S$,

$$ra \in J \implies r'a' = \varphi(r)\varphi(a) = \varphi(ra) \in \varphi(J).$$

  Similarly we can obtain $a'r' \in \varphi(J)$. Therefore, we conclude that $\varphi(J)$ is an ideal of S.

- Assume that φ is surjective. The universal property yields a unique homomorphism

$$\begin{aligned} \psi : R/I &\longrightarrow R/(I+J), \\ r + I &\longmapsto r + I + J. \end{aligned}$$

  Since

$$\begin{aligned} \ker \psi &= \{r + I \in R/I \mid r \in I + J\} \\ &= \{a + b + I \in R/I \mid a \in I, b \in J\} \\ &= \{b + I \in R/I \mid b \in J\} \\ &= \{\varphi(b) \in S \mid b \in J\} \\ &= \varphi(J) = \overline{J} \end{aligned}$$

  and ψ is surjective,

$$\frac{R/I}{\overline{J}} = \frac{R/I}{\ker \psi} \cong \frac{R}{I+J}.$$

$\blacksquare$

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. $R = Ra$.

For all $r \in R$, $r(Ra) \subseteq Ra$, $(aR)r \subseteq aR$. Therefore, Ra is a left-ideal of R, and aR is a right-ideal of R. Since $aR \subseteq R$, $R \subseteq aR$ actually amounts to $R = aR$.

$$a \text{ is a left-unit} \iff \exists b \in R, ab = 1 \implies \forall r \in R, r = abr \in aR \implies R \subseteq aR$$

$$R \subseteq aR \implies \forall r \in R, \exists r' \in R, r = ar' \implies \exists r' \in R, ar' = 1 \iff a \text{ is a left-unit}$$

Therefore, a is a left-unit if and only if $R = aR$. Similarly we can prove a is a right-unit if and only if $R = Ra$. ∎

3.8 Prove that a ring R is a division ring if and only if its only left-ideals and right-ideals are $\{0\}$ and R.
In particular, a commutative ring R is a field if and only if the only ideals of R are $\{0\}$ and R. [3.9, §4.3]

Assume the only left-ideals and right-ideals that ring R have are $\{0\}$ and R. If $a \neq 0$, we have $Ra = aR = R$. As a result of Exercise III.3.7, it implies that a is two-side unit and that accordingly R is a division ring.

Now assume that R is a division ring. Suppose I is a nonzero left-ideal of R and that $a \in I$ is not 0. Note that the condition of division ring guarantees there exists $b \in R$ such that $ba = 1$. Since for all $r \in R$, $r = (rb)a \in I$, there must be $I = R$. Supposing that I' is a nonzero right-ideal of R and that $a' \in I'$ is not 0, in a similar way we can deduce $I' = R$. Therefore, we conclude that the only left-ideals of R and right-ideals of R are $\{0\}$ and R. ∎

3.11 Let R be a ring containing $\mathbb{C}$ as a subring. Prove that there are no ring homomorphisms $R \to \mathbb{R}$.

Suppose $f : R \to \mathbb{R}$ is a homomorphism. On the one hand, we have

$$f(1) = f(1 * 1) = f(1)^2 \geq 0.$$

On the other hand, we can calculate $f(1)$ by

$$f(1) = f(-i * i) = -f(i)^2 \leq 0,$$

which forces $f(1)$ to be 0. Thus we see f sends some nonzero element in R to 0 in $\mathbb{R}$, which is a contradiction. ∎

3.12 Let R be a commutative ring. Prove that the set of nilpotent elements of R is an ideal of R. (Cf. Exercise III.1.6. This ideal is called the nilradical of R.)
Find a non-commutative ring in which the set of nilpotent elements is not an ideal. [3.13, 4.18, V.3.13, §VII.2.3]

Suppose N is the set of nilpotent elements of R. In Exercise III.1.6 we have shown that if R is commutative, then $a + b \in N$ for all $a, b \in N$. Since for all $r \in R$, $a \in N$,

$$a^n = 0 \implies r^n a^n = a^n r^n = 0 \implies ra, ar \in N,$$

we prove that N is an ideal of R. A counterexample for non-commutative ring can be found in the ring $\mathfrak{gl}_2(\mathbb{R})$, as is shown in Exercise III.1.6. ∎

3.13 ¬ Let R be a commutative ring, and let N be its nilradical (cf. Exercise III.3.12). Prove that R/N contains no nonzero nilpotent elements. (Such a ring is said to be reduced.) [4.6, VII.2.8]

Suppose there exists a nilpotent element $r + N \in R/N$ and $n > 0$ such that

$$r^n + N = N \iff r^n \in N.$$

Then we have $r^{nm} = 0$ for some $m > 0$, which implies $r \in N$. Therefore, the only nilpotent element in R/N is N. ∎

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?

Suppose the characteristic of the integral domain R is pq where p, q are positive prime integers. Then we have $p1_R \neq 0$ and $q1_R \neq 0$, since the order of 1_R is pq. However, we can deduce

$$(p1_R)(q1_R) = pq1_R = 0_R,$$

which contradicts the assumption that R is an integral domain.

If the characteristic of the integral domain R is 1, then the inclusion homomorphism $i : \mathbb{Z} \to R$ will send all integers to 0_R, which means $0_R = 1_R$ and R is actually a zero ring instead of an integral domain. Thus the characteristic of an integral domain is either be 0 or a prime integer. ∎

3.17 Let I, J be ideals of a ring R. State and prove a precise result relating the ideals $(I + J)/I$ of R/I and $J/(I \cap J)$ of $R/(I \cap J)$. [§3.3]

As abelian groups, the second isomorphism theorem ensures $(I + J)/I \cong J/(I \cap J)$. ∎

§4. Ideals and quotients: remarks and examples. Prime and maximal ideals

4.2 Prove that the homomorphic image of a Noetherian ring is Noetherian. That is, prove that if $\varphi : R \to S$ is a surjective ring homomorphism, and R is Noetherian, then S is Noetherian. [§6.4]

According to Exercise III.3.2, given any ideal J of S, we see $\varphi^{-1}(J)$ is an ideal of R. Since R is a Noetherian ring, we have $\varphi^{-1}(J) = (a_1, a_2, \cdots, a_n)$. Since φ is surjective, there must be

$$J = \varphi(\varphi^{-1}(J)) = (\varphi(a_1), \varphi(a_2), \cdots, \varphi(a_n)),$$

which means J is finitely generated. Thus we conclude S is Noetherian. ■

4.3 Prove that the ideal $(2, x)$ of $\mathbb{Z}[x]$ is not principal.

Suppose $(f) = (2, x)$. Since it is easy to see $f \neq 0$ and $f \neq 1$, there must be

$$2 = gf \implies f = 2.$$

However, it is impossible to find some $h \in \mathbb{Z}[x]$ such that

$$2 + x = hf = 2h,$$

which leads to a contradiction. Thus we show that the ideal $(2, x)$ of $\mathbb{Z}[x]$ is not principal. ■

4.5 Let I, J be ideals in a commutative ring R, such that $I + J = (1)$. Prove that $IJ = I \cap J$.[§4.1]

For any $k \in IJ$, we can assume that $k = ab$, $(a \in I,\ b \in J)$. Note that $k \in aJ = J$ and $k \in Ib = I$. It deduces that $k \in I \cap J$. Thus we show $IJ \subseteq I \cap J$.
Suppose $l \in I \cap J$. If $1 = a+b$ $(a \in I,\ b \in J)$, Then we have $l = 1 * l = (a+b)l = al + lb \in IJ$, which implies that $I \cap J \subseteq IJ$. Therefore, we show $IJ = I \cap J$. ■

4.6 Let I, J be ideals in a commutative ring R. Assume that $R/(IJ)$ is reduced (that is, it has no nonzero nilpotent elements; cf. Exercise III.3.13). Prove that $IJ = I \cap J$.

The notation (IJ) suggests R is commutative. As is shown in Exercise III.4.5, it holds that $IJ \subseteq I \cap J$. Thus we are left to show $I \cap J \subseteq IJ$. Suppose $l \in I \cap J$. The condition that $R/(IJ)$ is reduced tells that $\forall r \in R$,

$$r^n \in IJ \implies r \in IJ.$$

Noticing $l \in I$ and $l \in J$, it is clear that $l^2 \in IJ$ which implies $l \in IJ$. There we show $I \cap J \subseteq IJ$ and complete the proof. ■

4.7 $\triangleright$ 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]

Suppose I is an nonzero ideal in $k[x]$ and the least degree of nonzero polynomials in I is d. Since k is a field, we can find a monic polynomial $f(x) = k_0x^d + k_1x^{d+1} + \cdots + x^{d+n}$ in I. Given any $g(x) \in I$, there exist unique polynomials $q(x), r(x) \in k[x]$ such that $g(x) = f(x)q(x) + r(x)$ and $\deg r(x) < \deg f(x) = d$. Since $r(x) = g(x) - f(x)q(x) \in I$ and the least degree of nonzero polynomials in I is d, there must be $r(x) = 0$. Thus we show that I is generated by a monic polynomial $f(x)$. Suppose $I = (f(x))$ can be also generated by a monic polynomial $\bar{f}(x)$. Then we have $\bar{f}(x) = cf(x)$ for some $c \neq 0$. Since the two monic polynomials $\bar{f}(x), f(x)$ have the same degree, they are forced to be equal. Therefore, we conclude that every nonzero ideal in $k[x]$ is generated by a unique monic polynomial. ■

4.8 ▷ Let R be a ring, and $f(x) \in R[x]$ a monic polynomial. Prove that $f(x)$ is not a (left-, or right-) zero-divisor. [§4.2, 4.9]

Suppose $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ is a monic polynomial in $R[x]$ and $f(x)g(x) = 0$ for some $g(x) = b_sx^s + b_{s-1}x^{s-1} + \cdots + b_1x + b_0 \in R[x]$. Since the term of the degree of $d+s$ of $f(x)g(x)$ is b_sx^{d+s}, there must be $b_s = 0$. Then the term of the degree of $d+s-1$ of $f(x)g(x)$ is $b_{s-1}x^{d+s-z}$, which implies $b_{s-1} = 0$. Repeating this process we can show that $b_s = b_{s-1} = \cdots = b_0 = 0$, that is, $g(x) = 0$. Thus we see $f(x)$ is not a left-zero-divisor. In a similar way we can show that $f(x)$ is not a right-zero-divisor. ■

4.10 ¬ Let d be an integer that is not the square of an integer, and consider the subset of $\mathbb{C}$ defined by

$$\mathbb{Q}(\sqrt{d}) := \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}$$

- Prove that $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$.
- Define a function $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ by $N(a + b\sqrt{d}) := a^2 - b^2d$. Prove that

  $$N(zw) = N(z)N(w), \text{ and that } N(z) \neq 0 \text{ if } z \in \mathbb{Q}(\sqrt{d}), z \neq 0$$

  The function N is a 'norm'; it is very useful in the study of $\mathbb{Q}(\sqrt{d})$ and of its subrings. (Cf. also Exercise III.2.5.)
- Prove that $\mathbb{Q}(\sqrt{d})$ is a field, and in fact the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$. (Use N.)
- Prove that $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(t^2 - d)$. (Cf. Example 4.8.)
  [V.1.17, V.2.18, V.6.13, VII.1.12]

- We only show the check on multiplication

  $$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d} \in \mathbb{Q}(\sqrt{d}).$$

- It is immediate to check $N(zw) = N(z)N(w)$. Let $z \in \mathbb{Q}(\sqrt{d})$ and $z = a + b\sqrt{d} \neq 0$. Suppose $N(z) = a^2 - b^2d = 0$. If $b = 0$, we have $a = 0$, which contradicts with

$a + b\sqrt{d} \neq 0$. Otherwise we have $b \neq 0$ and $d = (a/b)^2$. Thus we get a contradiction again.

- We have known $\mathbb{Q}(\sqrt{d})$ is a commutative ring. For any $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ such that $z \neq 0$,
$$N(z) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d \neq 0.$$
Therefore
$$\left(a + b\sqrt{d}\right)\left(\frac{a}{N(z)} - \frac{b}{N(z)}\sqrt{d}\right) = 1$$
and $\mathbb{Q}(\sqrt{d})$ is a field.

- The mapping
$$\begin{aligned} \overline{\varphi} : \mathbb{Q}[t]/\left(t^2 - d\right) &\longrightarrow \mathbb{Q}(\sqrt{d}), \\ a + bt + (t^2 - d) &\longmapsto a + b\sqrt{d}. \end{aligned}$$
is well-defined since if $(a_1 + b_1 t) - (a_2 + b_2 t) = g(t)(t^2 - d)$, then
$$\begin{aligned} \overline{\varphi}(a_1 + b_1 t + (t^2 - d)) - \overline{\varphi}(a_2 + b_2 t + (t^2 - d)) &= \left(a_1 + b_1\sqrt{d}\right) - \left(a_2 + b_2\sqrt{d}\right) \\ &= g\left(\sqrt{d}\right)\left(\left(\sqrt{d}\right)^2 - d\right) \\ &= 0. \end{aligned}$$
It is clear that $\overline{\varphi}$ preserves addition. Then we can check $\overline{\varphi}$ preserve multiplication:
$$\begin{aligned} &\overline{\varphi}\left((a_1 + b_1 t + (t^2 - d))(a_2 + b_2 t + (t^2 - d))\right) \\ =\ &\overline{\varphi}\left((a_1 a_2 + (a_1 b_2 + a_2 b_1)t + b_1 b_2 t^2 + (t^2 - d)\right) \\ =\ &\overline{\varphi}\left(((a_1 a_2 + b_1 b_2 d) + (a_1 b_2 + a_2 b_1)t + b_1 b_2(t^2 - d) + (t^2 - d)\right) \\ =\ &(a_1 a_2 + b_1 b_2 d) + (a_1 b_2 + a_2 b_1)\sqrt{d} \\ =\ &(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) \\ =\ &\overline{\varphi}\left(a_1 + b_1 t + (t^2 - d)\right)\overline{\varphi}\left(a_2 + b_2 t + (t^2 - d)\right). \end{aligned}$$
Thus we see $\overline{\varphi}$ is a ring homomorphism. Note
$$a + bt + (t^2 - d) \in \ker\overline{\varphi} \iff a + b\sqrt{d} = 0 \iff a = b = 0.$$
It implies that $\ker\overline{\varphi} = \{0 + (t^2 - d)\}$ and $\overline{\varphi}$ is injective. It is clear that $\overline{\varphi}$ is surjective. Therefore, $\overline{\varphi}$ is an isomorphism.

∎

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 III.3.3.)

- According to the polynomial remainder theorem, we have

$$f_i(x) = (x-a)q(x) + f_i(a),$$

which suffices to show that $(f_1(x), \ldots, f_r(x), x-a) = (f_1(a), \ldots, f_r(a), x-a)$.

- Define

$$\begin{aligned} \varphi : R[x] &\longrightarrow R, \\ f(x) &\longmapsto f(a). \end{aligned}$$

We can check that φ is a surjective ring homomorphism and $\ker \varphi = (x-a)$. According to Exercise III.3.3, we have

$$\frac{R[x]}{(f_1(x), \cdots, f_r(x), x-a)} \cong \frac{R[x]}{(f_1(a), \cdots, f_r(a), x-a)} \cong \frac{R[x]/(x-a)}{\overline{(f_1(a), \cdots, f_r(a))}},$$

where

$$\overline{(f_1(a), \cdots, f_r(a))} = (f_1(a) + (x-a), \cdots, f_r(a) + (x-a)).$$

The ring isomorphism

$$\begin{aligned} \psi : R[x]/(x-a) &\longrightarrow R, \\ f(x) + (x-a) &\longmapsto f(a) \end{aligned}$$

gives the following isomorphism

$$\frac{R[x]/(x-a)}{\overline{(f_1(a), \cdots, f_r(a))}} \cong \frac{R}{(f_1(a), \ldots, f_r(a))},$$

which completes the proof.

■

4.12 $\triangleright$ Let R be a commutative ring, and $a_1, \cdots, a_n$ elements of R. Prove that

$$\frac{R[x_1, \ldots, x_n]}{(x_1 - a_1, \ldots, x_n - a_n)} \cong R$$

[VII.2.2]

$$R \cong \frac{R[x_1]}{(x_1 - a_1)} \cong \frac{R[x_1, x_2]}{(x_1 - a_1, x_2 - a_2)}$$

The mapping

$$\begin{aligned} \overline{\varphi} : \frac{R[x_1, \ldots, x_n]}{(x_1 - a_1, \ldots, x_n - a_n)} &\longrightarrow \frac{R[x_1, \ldots, x_{n-1}]}{(x_1 - a_1, \ldots, x_{n-1} - a_{n-1})}, \\ f(x_1, \cdots, x_n) + (x_1 - a_1, \ldots, x_n - a_n) &\longmapsto f(x_1, \cdots, x_{n-1}, a_n) + (x_1 - a_1, \ldots, x_{n-1} - a_{n-1}) \end{aligned}$$

is well-defined since if $f_1(x_1, \cdots, x_n) - f_2(x_1, \cdots, x_n) = \sum_{i=1}^{n} g_i(x_1, \cdots, x_n)(x_i - a_i)$, then

$$\begin{aligned} \overline{\varphi}\left(\overline{f_1(x_1, \cdots, x_n)}\right) - \overline{\varphi}\left(\overline{f_2(x_1, \cdots, x_n)}\right) &= f_1(x_1, \cdots, x_{n-1}, a_n) - f_2(x_1, \cdots, x_{n-1}, a_n) \\ &= \sum_{i=1}^{n-1} g_i(x_1, \cdots, x_{n-1}, a_n)(x_i - a_i) + g_n(t)(a_n - a_n) \\ &= \sum_{i=1}^{n-1} g_i(x_1, \cdots, x_{n-1}, a_n)(x_i - a_i). \end{aligned}$$

It is clear that $\overline{\varphi}$ preserves addition and multiplication. Thus we see $\overline{\varphi}$ is a ring homomorphism. Note

$$\begin{aligned} & f(x_1, \cdots, x_n) \in \ker \overline{\varphi} \\ \iff & f(x_1, \cdots, x_{n-1}, a_n) = \sum_{i=1}^{n-1} g_i(x_1, \cdots, x_{n-1}, a_n)(x_i - a_i) \\ \iff & f(x_1, \cdots, x_{n-1}, x_n) = \sum_{i=1}^{n-1} g_i(x_1, \cdots, x_{n-1}, a_n)(x_i - a_i) + g_n(x_1, \cdots, x_{n-1}, a_n)(x_n - a_n) \\ \iff & f(x_1, \cdots, x_n) \in (x_1 - a_1, \ldots, x_n - a_n), \end{aligned}$$

where the last but one line can be deduced by the polynomial remainder theorem if we fix $x_1, \cdots, x_{n-1}$ and regard x_n as a variable. It implies that $\ker \overline{\varphi} = \{0 + (x_1 - a_1, \ldots, x_n - a_n)\}$ and $\overline{\varphi}$ is injective. It is clear that $\overline{\varphi}$ is surjective. Therefore, $\overline{\varphi}$ is an isomorphism and

$$R \cong \frac{R[x_1]}{(x_1 - a_1)} \cong \frac{R[x_1, x_2]}{(x_1 - a_1, x_2 - a_2)} \cong \cdots \cong \frac{R[x_1, \ldots, x_n]}{(x_1 - a_1, \ldots, x_n - a_n)}.$$

$\blacksquare$

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 $M_p = \{f \in R | f(p) = 0\}$. 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).)

If further K is Hausdorff (and, as Bourbaki would have it, compact spaces are Hausdorff), then Urysohn's lemma shows that for any two points $p \neq q$ in K there exists a function $f \in R$ such that $f(p) = 0$ and $f(q) = 1$. If this is the case, 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]

(i) Suppose all functions in R that have same value in a neighborhood of p are identified. It is easy to check that M_p is an ideal and R/M_p is commutative. Given any $f \in R - M_p$, we have $f(p) \neq 0$ and

$$(f + M_p)\left(\frac{1}{f} + M_p\right) = 1 + M_p$$

Therefore, R/M_p is a field and M_p is a maximal ideal in R.

(ii) If $f_1, \ldots, f_r \in R$ have no common zeros, $(f_1, \ldots, f_r) = (1)$ follows from

$$\sum_{i=1}^{n} \frac{f_i}{f_1^2 + \cdots + f_n^2} f_i = 1.$$

(iii) Let M be a maximal ideal in R. Then R/M is a field. For any $f \in R - M$, there exists $g \in R - M$ such that

$$(f + M)(g + M) = fg + M = 1 + M \implies fg - 1 \in M$$

■

§5. Modules over a ring

5.1 $\triangleright$ 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]

Let i denote the identity map $R \to R^\circ$. If R is commutative, we have

$$i(ab) = ab = b \bullet a = i(b) \bullet i(a) = i(a) \bullet i(b).$$

Given that $i(a+b) = a+b$ and identity map is a bijection, we see that i is an isomorphism.

If i is an isomorphism, we have

$$ab = b \bullet a = i^{-1}(b \bullet a) = i^{-1}(b) i^{-1}(a) = ba,$$

which implies that R is commutative.

Suppose $A, B \in \mathcal{M}_n(\mathbb{R})$. We can show that the transpose of matrix $\cdot^T : A \mapsto A^T$ is an isomorphism by checking

$$(AB)^T = B^T A^T = A^T \bullet B^T.$$

Let M be a right-R-module with right multiplication $\odot$. If $R \cong R^\circ$ and $f : R \to R^\circ$ is an isomorphism, then

$$f(ab) = f(a) \bullet f(b) = f(b) f(a)$$

Define left multiplication $\odot_L$ as

$$r \odot_L m := m \odot f(r), \qquad \forall r \in R, m \in M.$$

We can check that

$$\begin{aligned}
&1 \odot_L m = m \odot f(1) = 1,\\
&(rs) \odot_L m = m \odot f(rs) = m \odot (f(s) f(r)) = (m \odot f(s)) \odot f(r)\\
&\qquad\qquad = (s \odot_L m) \odot f(r) = r \odot_L (s \odot_L m),\\
&r \odot_L (m_1 + m_2) = (m_1 + m_2) \odot f(r) = m_1 \odot f(r) + m_2 \odot f(r) = r \odot_L m_1 + r \odot_L m_2.
\end{aligned}$$

Therefore, we show that M is a left-R-module with right multiplication $\odot_L$.

If M is a left-R-module with left multiplication $*$ and $f : R \to R^\circ$ is an isomorphism, then we can show that M is a right-R-module with right multiplication $*_R$ defined as

$$m *_R r := f^{-1}(r), \qquad \forall r \in R, m \in M.$$

∎

5.3 $\triangleright$ 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]

$$\begin{aligned} 0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m &\implies 0 \cdot m = 0, \\ 0 = (1-1) \cdot m = 1 \cdot m + (-1) \cdot m &\implies (-1) \cdot m = -m. \end{aligned}$$

■

5.4 $\neg$ Let R be a ring. A nonzero R-module M is *simple* (or *irreducible*) if its only submodules are $\{0\}$ and M. Let M, N be simple modules, and let $\varphi : M \to N$ be a homomorphism of R-modules. Prove that either $\varphi = 0$, or φ is an isomorphism. (This rather innocent statement is known as Schur's lemma.) [5.10, 6.16, VI.1.16]

For convenience, we talk about the identity of modules up to isomorphism. Since the nonzero R-module M is simple, $\ker \varphi$ is either $\{0\}$ or M. Thus $\operatorname{im} \varphi = M/\ker \varphi$ is either $\{0\}$ or M. Note that $\operatorname{im} \varphi \subset N$ is either $\{0\}$ or N. If $\operatorname{im} \varphi = \{0\}$, then we have $\varphi = 0$. If $\operatorname{im} \varphi = M$, then we have $\operatorname{im} \varphi = M = N$. Therefore we show that either $\varphi = 0$, or φ is an isomorphism.

■

5.5 Let R be a commutative ring, viewed as an R-module over itself, and let M be an R-module. Prove that $\operatorname{Hom}_{R-\mathrm{Mod}}(R, M) \cong M$ as R-modules.

Define

$$\begin{aligned} \varphi : \operatorname{Hom}_{R-\mathrm{Mod}}(R, M) &\longrightarrow M, \\ f &\longmapsto f(1) \end{aligned}$$

Since

$$\begin{aligned} \varphi(f+g) = (f+g)(1) = f(1) + g(1) = \varphi(f) + \varphi(g), \\ \varphi(rf) = (rf)(1) = rf(1) = r\varphi(f), \end{aligned}$$

we see φ is a homomorphism. If $\varphi(f_1) = \varphi(f_2)$, we have $f_1(1) = f_2(1)$. Multiply both sides by any $r \in R$ and we get

$$rf_1(1) = rf_2(1) \implies f_1(r) = f_2(r),$$

which means $f_1 = f_2$. Thus we show φ is injective. Given any $m \in M$, let

$$\begin{aligned} h_m : R &\longrightarrow M, \\ r &\longmapsto rm \end{aligned}$$

Since $\varphi(h_m) = h_m(1) = m$, we show that φ is surjective. Therefore, we conclude that φ is an isomorphism and $\operatorname{Hom}_{R-\mathrm{Mod}}(R, M) \cong M$ as R-modules. ■

5.6 Let G be an abelian group. Prove that if G has a structure of $\mathbb{Q}$-vector space, then it has only one such structure. (Hint: First prove that every nonidentity element of G has necessarily infinite order. Alternative hint: The unique ring homomorphism $\mathbb{Z} \to \mathbb{Q}$ is an epimorphism.)

Assume that G has two structures of $\mathbb{Q}$-vector space with scalar multiplication operations $\cdot$ and $*$ respectively. Note that $1 \cdot g = 1 * g = g$ for all $g \in G$. With the conventional notation $\sum_{i=1}^{n} g = ng$, we have for all $g \in G$,

$$\sum_{i=1}^{n} 1 \cdot g = \sum_{i=1}^{n} 1 * g = ng \implies \left(\sum_{i=1}^{n} 1\right) \cdot g = \left(\sum_{i=1}^{n} 1\right) * g = ng \implies n \cdot g = n * g = ng.$$

Since

$$\sum_{i=1}^{m} \frac{1}{m} \cdot h = \left(\sum_{i=1}^{m} \frac{1}{m}\right) \cdot h = h, \qquad \forall h \in G,$$
$$\sum_{i=1}^{m} \frac{1}{m} * h = \left(\sum_{i=1}^{m} \frac{1}{m}\right) * h = h, \qquad \forall h \in G,$$

it holds that for all $h \in G$,

$$\sum_{i=1}^{m} \frac{1}{m} \cdot h = \sum_{i=1}^{m} \frac{1}{m} * h \implies \sum_{i=1}^{m} \left(\frac{1}{m} \cdot h - \frac{1}{m} * h\right) = 0 \implies m \cdot \left(\frac{1}{m} \cdot h - \frac{1}{m} * h\right) = 0.$$

According to the property of vector space, we have $m = 0$ or $\frac{1}{m} \cdot h - \frac{1}{m} * h = 0$. However, m is a positive integer, which forces $\frac{1}{m} \cdot h = \frac{1}{m} * h$. Thus we can deduce that for all $h \in G$, $n, m \in \mathbb{Z}_+$,

$$n \cdot \left(\frac{1}{m} \cdot h\right) = n * \left(\frac{1}{m} * h\right) \implies \frac{n}{m} \cdot h = \frac{n}{m} * h.$$

In other words, for all $h \in G$, $q \in \mathbb{Q}_+$, we have $q \cdot h = q * h$. Note that $(-q) \cdot h = (-q) * h$ and $0 \cdot h = 0 * h$, finally we obtain that for all $h \in G$, $q \in \mathbb{Q}$,

$$q \cdot h = q * h.$$

Therefore, the two scalar multiplication operations $\cdot$ and $*$ coincide, which completes the proof. ∎

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.

Define the scalar multiplication $\cdot$ as

$$a \cdot x := ax, \qquad \forall a \in k, x \in K.$$

Then we can check that for all $a, b \in k$, $x, y \in K$,

$$\begin{aligned}
&1 \cdot x = x, \\
&(ab) \cdot x = (ab)x = a(bx) = a \cdot (b \cdot x), \\
&(a+b) \cdot x = (a+b)x = ax + bx = a \cdot x + b \cdot x, \\
&a \cdot (x+y) = a(x+y) = ax + ay = a \cdot x + a \cdot y, \\
&(a \cdot x)(b \cdot y) = (ax)(by) = (ab)(xy) = (ab) \cdot (xy).
\end{aligned}$$

Therefore, K is a k-vector space and a k-algebra as well. ■

5.8 What is the initial object of the category R-Alg?

The ring R can be seen as a R-algebra if it is endowed with a scalar multiplication $\cdot$ in a natural way, that is

$$r \cdot x := rx, \qquad \forall r \in R, x \in R.$$

Given any R-algebra A, define the following map

$$\begin{aligned}
f : R &\longrightarrow A, \\
r &\longmapsto r \cdot 1_A.
\end{aligned}$$

We can check that

$$\begin{aligned}
f(r_1 + r_2) &= (r_1 + r_2) \cdot 1_A = r_1 \cdot 1_A + r_2 \cdot 1_A = f(r_1) + f(r_2), \\
f(r_1 r_2) &= (r_1 r_2) \cdot 1_A = r_1 \cdot (r_2 \cdot 1_A) = r_1 \cdot (1_A(r_2 \cdot 1_A)) = (r_1 \cdot 1_A)(r_2 \cdot 1_A) = f(r_1)f(r_2), \\
f(r_1 \cdot r_2) &= f(r_1 r_2) = r_1 \cdot (r_2 \cdot 1_A) = r_1 \cdot f(r_2).
\end{aligned}$$

Hence f is a morphism in the category R-Alg.

Suppose $g : R \to A$ is a morphism in R-Alg. Then for all $r_1, r_2 \in R$,

$$g(r_1 r_2) = g(r_1 \cdot r_2) \implies g(r_1)g(r_2) = r_1 \cdot g(r_2) = r_1 \cdot (1_A g(r_2)) = (r_1 \cdot 1_A)g(r_2).$$

Take $r_2 = 1_R$ and then for all $r_1 \in R$,

$$g(r_1)g(1_R) = (r_1 \cdot 1_A)g(1_R) \implies g(r_1) = r_1 \cdot 1_A.$$

Thus we have $g = f$. Therefore, we show that for any R-algebra A, there exists a unique morphism $f : R \to A$ in R-Alg. In other words, R is the initial object of the category R-Alg. ■

5.9 $\neg$ Let R be a commutative ring, and let M be an R-module. Prove that the operation of composition on the R-module $\mathrm{End}_{R-\mathsf{Mod}}(M)$ makes the latter an R-algebra in a natural way.
Prove that $\mathcal{M}_n(R)$ (cf. Exercise III.1.4) is an R-algebra, in a natural way. [VI.1.12, VI.2.3]

In textbook we have show that $\mathrm{End}_{R-\mathsf{Mod}}(M)$ is an R-module with natural addition and scalar multiplication. We can check that for all $f, g, h \in \mathrm{End}_{R-\mathsf{Mod}}(M)$, $r, s \in R$, $x \in M$,

$$\begin{aligned}
(id_M \circ f)(x) &= id_M(f(x)) = f(x), \\
((f+g)\circ h)(x) &= (f+g)(h(x)) = f(h(x)) + g(h(x)) = (f\circ h)(x) + (g \circ h)(x) \\
&= (f\circ h + g\circ h)(x), \\
((r\cdot f)\circ (sg))(x) &= (r\cdot f)((s\cdot g)(x)) = r\cdot f(s\cdot g(x)) = r\cdot (s\cdot f(g(x))) \\
&= (rs)\cdot (f(g(x)) = (rs)\cdot ((f\circ g)(x)) = ((rs)\cdot (f\circ g))(x).
\end{aligned}$$

Thus we prove that the operation of composition $\circ$ on the R-module $\mathrm{End}_{R-\mathsf{Mod}}(M)$ makes $\mathrm{End}_{R-\mathsf{Mod}}(M)$ an R-algebra.

In Exercise III.1.4 we have shown that $\mathcal{M}_n(R)$ is a ring. Let the scalar multiplication $\cdot$ be componentwise multiplication, namely

$$r\cdot (a_{ij})_{n\times n} := (ra_{ij})_{n\times n}, \qquad \forall r\in R, (a_{ij})_{n\times n} \in \mathcal{M}_n(R).$$

We can check that

$$\begin{aligned}
1_R \cdot (a_{ij})_{n\times n} &= (1_R a_{ij})_{n\times n} = (a_{ij})_{n\times n}, \\
(r+s)\cdot (a_{ij})_{n\times n} &= ((r+s)a_{ij})_{n\times n} = (ra_{ij})_{n\times n} + (sa_{ij})_{n\times n} \\
&= r\cdot (a_{ij})_{n\times n} + s\cdot (a_{ij})_{n\times n}, \\
r\cdot \left((a_{ij})_{n\times n} + (b_{ij})_{n\times n}\right) &= r\cdot (a_{ij}+b_{ij})_{n\times n} = \left(r\left(a_{ij} + rb_{ij}\right)\right)_{n\times n} \\
&= (ra_{ij})_{n\times n} + (rb_{ij})_{n\times n} = r\cdot (a_{ij})_{n\times n} + r\cdot (b_{ij})_{n\times n}, \\
(rs)\cdot (a_{ij})_{n\times n} &= ((rs)a_{ij})_{n\times n} = r\cdot (sa_{ij})_{n\times n} = r\cdot \left(s\cdot (a_{ij})_{n\times n}\right), \\
\left(r\cdot (a_{ij})_{n\times n}\right)\left(s\cdot (b_{ij})_{n\times n}\right) &= (ra_{ij})_{n\times n}(sb_{ij})_{n\times n} = \left(\sum_{k=1}^{n} (ra_{ik})\,(sb_{kj})\right)_{n\times n} \\
&= \left((rs)\sum_{k=1}^{n} a_{ik}b_{kj}\right)_{n\times n} = (rs)\cdot \left(\sum_{k=1}^{n} a_{ik}b_{kj}\right)_{n\times n} \\
&= (rs)\cdot \left((a_{ij})_{n\times n}\,(b_{ij})_{n\times n}\right).
\end{aligned}$$

Therefore, $\mathcal{M}_n(R)$ is an R-algebra. ■

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 $\mathrm{End}_{R-\mathsf{Mod}}(M)$. [§VI.7.1]

According to Exercise III.5.9, $\mathrm{End}_{R-\mathsf{Mod}}(M)$ has an R-algebra structure, which can induce an $R[x]$-module structure on $\mathrm{End}_{R-\mathsf{Mod}}(M)$. That is, for all $f(x) = r_0 + r_1x + \cdots + r_nx^n \in R[x], \varphi \in \mathrm{End}_{R-\mathsf{Mod}}(M)$,

$$f(x)\cdot \varphi := f(\varphi) = r_0 + r_1\varphi + \cdots + r_n\varphi^n.$$

Given any $\varphi \in \mathrm{End}_{R-\mathsf{Mod}}(M)$, define the following $R[x]$-module structures on M with scalar multiplication $\cdot_\varphi$,

$$f(x) \cdot_\varphi m := (f(\varphi))(m), \qquad \forall f(x) \in R[x], m \in M.$$

What we need is to show that the map $\varphi \mapsto \cdot_\varphi$ is a bijection.

If $\cdot_\varphi = \cdot_\eta$, we have $(f(\varphi))(m) = (f(\eta))(m)$. Take $f(x) = x$ and then we have $\varphi(m) = \eta(m)$ for all $m \in M$, which implies $\varphi = \eta$. Hence the map $\varphi \mapsto \cdot_\varphi$ is injective.

Suppose $\bullet$ is a scalar multiplication which makes M an $R[x]$-module.

- $f(x) \bullet (m+n) = f(x) \bullet m + f(x) \bullet n$
- $(f(x) + g(x)) \bullet m = f(x) \bullet m + g(x) \bullet m$
- $(f(x)g(x)) \bullet m = f(x) \bullet (g(x) \bullet m)$
- $1 \bullet m = m$

■

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

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 $M \cong \ker p \oplus \operatorname{im} p$.

Since $x = p((p - id_M)x) \in M$, p must be an epimorphism and $M \cong \operatorname{im} p \cong M/\ker p$. For all $x \in \ker p \cap \operatorname{im} p$, we can assume $x = py$ and deduce that $0 = px = p^2 y = py = x$. Thus we have $\ker p \cap \operatorname{im} p = \{0\}$ and

$$\frac{\ker p \oplus \operatorname{im} p}{\ker p} \cong \frac{\operatorname{im} p}{\ker p \cap \operatorname{im} p} \cong \operatorname{im} p,$$

which implies

$$\frac{\ker p \oplus \operatorname{im} p}{M} \cong \frac{\ker p \oplus \operatorname{im} p/\ker p}{M/\ker p} \cong \frac{\operatorname{im} p}{\operatorname{im} p} \cong \{0\}.$$

Therefore we show that $M \cong \ker p \oplus \operatorname{im} p$. ■

§7. Complexes and homology

7.1 Assume that the complex

$$\cdots \longrightarrow 0 \longrightarrow M \longrightarrow 0 \longrightarrow \cdots$$

is exact. Prove that $M \cong 0$. [§7.3]

Assume that $f : 0 \to M$ and $g : M \to 0$. Since the the complex is exact, we have

$$\{0\} = \operatorname{im} f = \ker g = M.$$

$\blacksquare$

Chapter V. Irreducibility and factorization in integral domains

Appendix

Lemma II.1 (von Dyck) Given a presentation $(A|\mathscr{R}) = F(A)/R$, where A is the set of generators, $\mathscr{R} \in F(A)$ is the set of relators and R is the smallest normal subgroup of $F(A)$ containing $\mathscr{R}$. Define inclusion mapping $i : A \to F(A)$ and projection $\pi : F(A) \to F(A)/R$. If f is a mapping from A to a group G, and every relations in $\mathscr{R}$ holds in G via f, that is, $\mathscr{R} \subset \ker\varphi$ where φ is the unique homomorphism induced by the universal property of free group, then there exists a unique homomorphism $\psi : F(A)/R \to G$ such that $f = \psi \circ \pi \circ i$. If G is generated by $f(A)$, then ψ is surjective.

$$\begin{tikzcd}
F(A)/R \arrow[dr, dashed, "\exists!\psi"] & \\
F(A) \arrow[u, "\pi"] \arrow[r, dashed, "\varphi"] & G \\
A \arrow[u, "i"] \arrow[ur, "f"'] &
\end{tikzcd}$$

Proof of the lemma. Since R is the smallest normal subgroup of $F(A)$ containing $\mathscr{R}$ and the normal subgroup $\ker\varphi$ contains $\mathscr{R}$, we must have $R \subset \ker\varphi$. Then according to Theorem 7.12, there exists a unique homomorphism $\psi : F(A)/R \to G$ such that $\varphi = \psi \circ \pi$, which means the whole diagram commutes. If there exists a homomorphism $\zeta : F(A)/R \to G$ such that $f = \zeta \circ \pi \circ i$, then we have $\varphi \circ i = \zeta \circ \pi \circ i$, which implies $\varphi(t) = \zeta(\pi(t))$ for all $t \in A$. Note that a homomorphism defined on $F(A)$ can be specified only by its valuation on the set of generators A, we can assert that $\varphi = \zeta \circ \pi$. Since there exists a unique homomorphism $\psi : F(A)/R \to G$ such that $\varphi = \psi \circ \pi$, we have $\zeta = \psi$. Thus we show that there exists a unique homomorphism $\psi : F(A)/R \to G$ such that $f = \psi \circ \pi \circ i$.

Moreover, if G is generated by $f(A)$, then $\mathrm{im}\psi = G$, since $f(A) = \psi(\pi(i(A))) \subset \mathrm{im}\psi$ implies $G \subset \mathrm{im}\psi$. ⌟

References

[1] Paolo Aluffi. *Algebra: chapter 0*, volume 104. American Mathematical Soc., 2009.