Answer to Algebra Chapter 0 - Paolo Aluffi: Exercise Solutions

Hoang Vo Ke

Chapter I. Preliminaries: Set theory and categories

1.3. Categories

Exercise 1
Let C be a category. Consider a structure C^{op} with

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

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.

Proof. For any $f \in \mathrm{Hom}_{C^{op}}(A, B)$ and $g \in \mathrm{Hom}_{C^{op}}(B, C)$, we define the composition $g \circ f$ of C^{op} to be the composition fg of C. (We will denote the composition in C^{op} with "$\circ$" and nothing for the composition in C). With this definition, we have

$$h \circ (g \circ f) = h \circ fg = (fg)h = f(gh) = f(h \circ g) = (h \circ g) \circ f,$$

which says this composition law is associative.

For any object A of C, let the identity of $\mathrm{Hom}_{C^{op}}(A, A)$ equals the identity of $\mathrm{Hom}_C(A, A)$. So for any $f \in \mathrm{Hom}_{C^{op}}(A, B) = \mathrm{Hom}_C(B, A)$, we have $f \circ 1_A = 1_A f = f$. Similarly, we get $1_B \circ f = f1_B = f$. So C^{op} is a category. □

Exercise 3
Formulate precisely what it means to say that 1_a is an identity with respect to composition in Example 3.3, and prove this assertion.

Proof. To show that 1_A is an identity, we must show that for $f \in \mathrm{Hom}(a, b)$, we have $1_b f = f = f1_a$. Indeed, we have $1_b f = (b, b)(a, b) = (a, b) = f$ and $f1_a = (a, b)(a, a) = (a, b) = f$. So 1_a is an identity with respect to the composition in Example 3.3. □

Exercise 4
Can we define a category in the style of Example 3.3 using the relation $<$ on the set $\mathbb{Z}$?

Proof. No we cannot define a category in style of Example 3.3 using the relation $<$ because it is not reflexive. Therefore, there is no identity morphism. □

Exercise 5
Explain in what sense Example 3.4 is an instance of the categories considered in Example 3.3

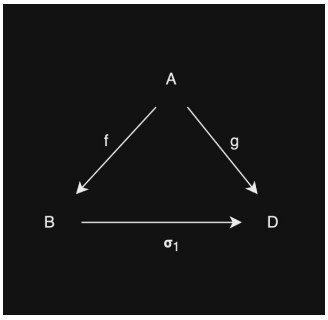
Proof. Because the $\subseteq$ relation is transitive and reflexive, we can define a category out of $P(S)$ similar to Example 3.3. □

Exercise 7
Define carefully objects and morphisms in Example 3.7, and draw the diagram corresponding to composition.

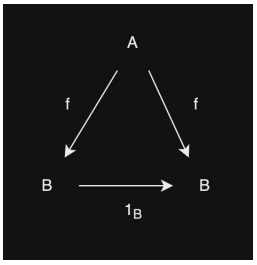
Proof. Let C be a category, we will define C_A as follow

$$\mathrm{Obj}(C_A) = \{f : f \in \mathrm{Hom}(A, B) \text{ for some } B \in \mathrm{Obj}(C)\}.$$

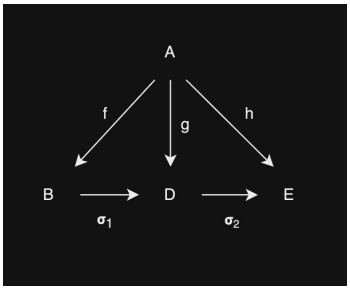
Let $f \in \mathrm{Hom}_C(A, B)$, $g \in \mathrm{Hom}_C(A, D)$, and $h \in \mathrm{Hom}_C(A, E)$, then we will define the morphism $f \to g$ be the commutative diagram.



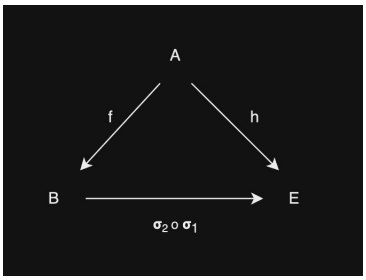
The identity of f would be this diagram.



Similar to Example 3.7, we can define the composition of two diagrams $f \to g$ and $g \to h$ as follow.



Because C is a Category, the previous diagram is the same as this.



And it is not hard to check that is definition satisfies all the properties of a Category. (Trust me, I have done it on paper.) □

4. Morphisms

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

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

Proof.

- Assume that $f \in \mathrm{Hom}_C(A, B)$ has a right inverse, say f', then $f \circ f' = 1_A$. For any β and β' in C such that $\beta \circ f = \beta' \circ f$, then we would have

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

  So f is an epimorphism.

- The converse is not true however. Take the category $\mathbb{Z}$ with the relation $\leq$ as an example. Any morphism is an epimorphism but $(3, 5)$ doesn't have an inverse.

□

5. Universal properties

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

Proof. Let A be a final object of C, so for any $B \in C$, we have $\mathrm{Hom}_{C^{op}}(A, B) = \mathrm{Hom}_C(B, A)$ is a singleton. So A is an initial object in C^{op}. □

Exercise 5.2
Prove that $\varnothing$ is the unique initial object in Set.

Proof. Let $A \neq \varnothing$ be an initial object in Set. Let $\{x, y\} \in Set$ be an object of Set that has two elements. We can define two distinct functions in $\mathrm{Hom}(A, \{x, y\})$, namely $f(a) = x$ and $f(a) = y$ for all $a \in A$. But this is impossible since A is an initial object, thus $\varnothing$ is the unique initial object of Set. □

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

Proof. Let A and B be two final objects of a category C. Notice that the unique element of $\mathrm{Hom}(A, A)$ is 1_A and the same for B. Let $f \in \mathrm{Hom}(A, B)$ and $g \in \mathrm{Hom}(B, A)$. Then $f \circ g \in \mathrm{Hom}(B, B)$, which implies $f \circ g = 1_B$. Similarly we get $g \circ f = 1_A$. So A is isomorphic to B. □

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

Proof. Let $a, b \in \mathbb{Z}^+$, we will show that $d = \gcd(a, b)$ is the product and $m = \mathrm{lcm}(a, b)$ is the coproduct of a and b. Indeed, because $d|a$ and $d|b$, we get $d \to a$ and $d \to b$. For any $c \to a$ and $c \to b$, we get $c|a$ and $c|b$. Therefore $c|\gcd(a, b) = d$. Hence there is a unique morphism $c \to d$. So d is the product of a and b. Similarly, we can show that $m = \mathrm{lcm}(a, b)$ is the coproduct of a and b. □

Exercise 5.8
Show that in every category C the products $A \times B$ and $B \times A$ are isomorphic if they exist.

Proof. Let π_A, π_B be the natural projection from $B \times A$ to A and B respectively. Similarly, let π'_A and π'_B be the natural projection from $A \times B$ to A and B. Because $A \times B$ and $B \times A$ are products, there is a unique $f \in \mathrm{Hom}(A \times B, B \times A)$ and $g \in \mathrm{Hom}(B \times A, A \times B)$ such that 1 commute.

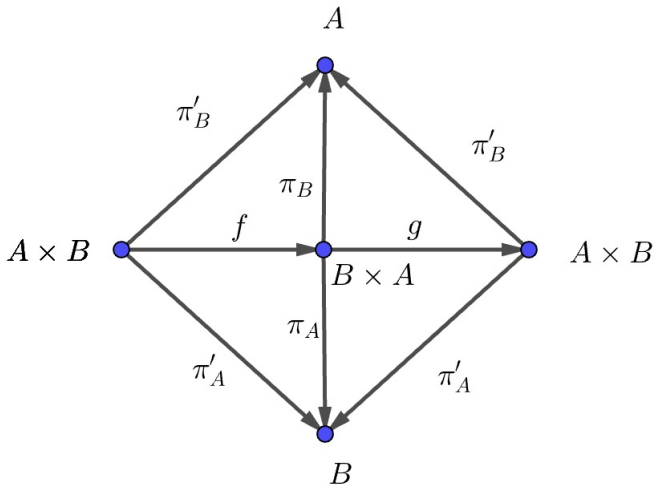


Figure 1: diagram 1

But diagram 1 can be reduced to diagram 2. We can see that by replacing $f \circ g$ by $1_{A \times B}$, the diagram also commute. Using the universal property of the product, we get $f \circ g = 1_{B \times A}$.

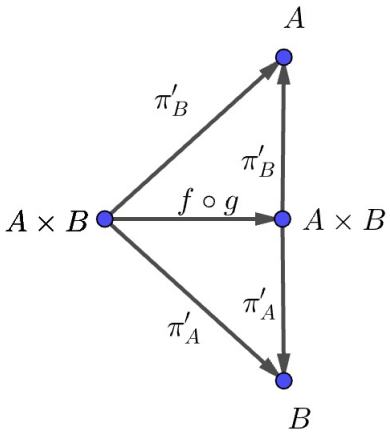


Figure 2: diagram 2

Similarly, we can show that $g \circ f = 1_{A \times B}$. So $A \times B$ and $B \times A$ are isomorphic. $\square$

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

Chapter II. Groups, first encounter

1. Definition of Group.

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

Proof. By considering each element of a group as a morphism, Proposition 4.3 yields the result immediately. □

Exercise 1.5
Prove that every column of the multiplication table of a group contains all elements of the group exactly once.

Proof. Each row of the multiplication table is the image of a group G through an isomorphism f. The epimorphism of f guarantees each column contains all elements of G, and the monomorphism guarantees each element appears exactly once. □

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

Proof. If G has one or two elements, then $\mathrm{Hom}(G)$ has 1! or 2! elements respectively. So G has one multiplication table. Assume that $G = \{e, g, h\}$. Notice that if $gh = g$, then the cancellation law implies $h = e$. Thus $gh = hg = e$. Fill in the table using Exercise 1.5, we get the following unique table.

•	e	g	h
e	e	g	h
g	g	h	e
h	h	e	g

.

After a lot of checking, there are two distinct tables up to reordering as follows

•	e	g	h	k
e	e	g	h	k
g	g	e	k	h
h	h	k	g	e
k	k	h	e	g

, and

•	e	g	h	k
e	e	g	h	k
g	g	e	k	h
h	h	k	e	g
k	k	h	g	e

.

Since all of these tables are symmetric with respect to the main diagonal, groups with less than 4 elements are commutative. □

Exercise 1.7
Prove Corollary 1.11, that is $g^N = e$ if and only if N is a multiple of $|g|$ for an element g of finite order, and $N \in \mathbb{Z}$.

Proof. Let r be the reminder when we divide N by $|g|$. So $r < |g|$. Clearly, we get $g^r = e$. Since $|g|$ is the least nonzero number that satisfies this equation, we get $r = 0$. So N is a multiple of $|g|$. □

Exercise 1.11
Prove that for all g, h in a group G, $|gh| = |hg|$.

Proof. It is sufficient to prove that for any $n \in \mathbb{N}$, $(gh)^n = e$ implies $(hg)^n = e$. Indeed, because if $(gh)^n = e$, then

$$e = heh^{-1} = h(gh)^n h^{-1} = (hg)^n.$$

So $|gh| = |hg|$. □

2. Examples of Group.

Exercise 2.1
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.

Proof. Let $M(i, j)$ be the entry at (i, j) of a matrix M. Because σ is an isomorphism, each row and column of M_σ has exactly one 1. Let $M_{\sigma\tau} := M_\sigma M_\tau$, we have

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

Notice that there is only one t that makes $M_\sigma(i, t) \neq 0$, so $M_{\sigma\tau}(i, j) = 1$ if and only if $M_\sigma(i, t) = M_\tau(t, j) = 1$. This means $t = \sigma(i)$ and $j = \tau(t) = \tau(\sigma(i))$. So $M_{\sigma\tau}$ the matrix represent the permutation $\sigma\tau$. □

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

Proof. We know that $D_8 = \langle r, s \mid r^4 = s^2 = e, rs = sr^{-1} \rangle$. Define $f : D_8 \to S_4$ that maps

$$e \mapsto e, \quad r \mapsto (1234), \quad s \mapsto (24).$$

With brute force, we can check that $(1234)^4 = (24)^2 = e$ and $(1234)(24) = (24)(1234)^{-1}$. So f is a homomorphism. The 8 permutations in the image of f are

$$\{e, (1234), (13)(24), (1432), (13), (24), (12)(34), (14)(23)\}.$$

Since D_8 also has 8 elements and it is not hard to check that f is surjective, we get f is an isomorphism. □

Exercise 2.7
Find all elements of D_{2n} that commute with every other elements.

Proof. We know that

$$D_{2n} = \langle r, s \mid r^n = s^2 = e, rs = sr^{-1} \rangle = \{e, r, \cdots, r^{n-1}, s, rs, \cdots, r^{n-1}s\}.$$

Clearly, e commutes with every element, If $r^j s$ commutes with every element, then it must commute with r. So

$$r^j s = r^{j+1} s r^{-1} = r^j s r^{-2}.$$

This implies $r^2 = e$ or $n = 2$, which is impossible because $n \geq 3$.

If r^j commutes with every element for some j from 1 to $n-1$, then it must commute with s. Thus

$$r^j = s r^j s = r^{-j}.$$

This means $r^{2j} = 2$ or $j = n/2$. So n must be an even number, say $n = 2k$, and r^k commutes with every element of D_{2n}. But this is not hard to check, using the formula $rs = sr^{-1}$. So when n is even, there are exactly two elements, those are e and $r^{n/2}$. Otherwise, e is the only element that commute with everyone. □

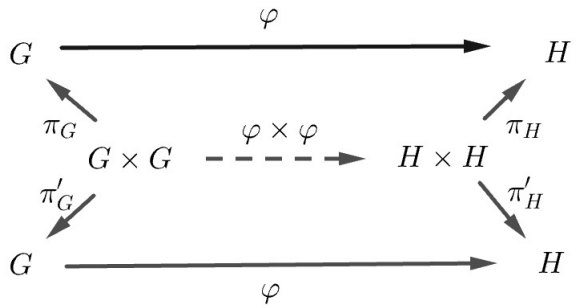
3. The category Grp

Exercise 3.1
Let $\varphi\colon G \to H$ be a morphism in a category C with products. Explain why there is a unique morphism

$$(\varphi \times \varphi)\colon G \times G \to H \times H.$$

(This morphism is defined explicitely for $\mathsf{C} = \mathsf{Set}$ in §3.1.)

Proof. Let $\pi_G\colon G \times G \to G$ be the projection with respect to the first entry and $\pi'_G\colon G \times G \to G$ be the projection with respect to the second entry. Similar for H. Because $\pi_G \circ \varphi$ and $\pi'_G \circ \varphi$ are morphisms of C, the unniversal property of product implies that there exists a unique map $\varphi \times \varphi$ such that the following diagram commutes:



□

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

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

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

Proof. For any $(g_1, g_2) \in G \times G$, we have

$$\begin{aligned}((\psi\varphi) \times (\psi\varphi))(g_1, g_2) &= (\psi\varphi(g_1)) \times (\psi\varphi(g_2)) \\ &= (\psi \times \psi)(\varphi(g_1), \varphi(g_2)) \\ &= (\psi \times \psi)(\varphi \times \varphi)(g_1, g_2).\end{aligned}$$

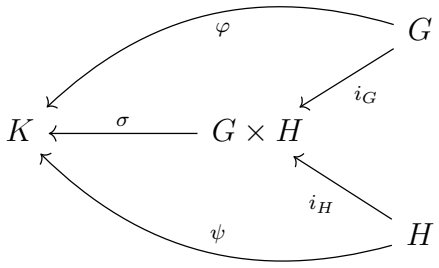
This computation prove the required statement. □

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

Proof. Let $G \times H$ be the group product of G and H. Let $i_G\colon G \to G \times H$ maps $g \mapsto (g, e_H)$ and $i_H\colon H \to G \times H$ maps $h \to (e_G, h)$. Notice that i_G is a homomorphism because for any $g_1, g_2 \in G$, we have

$$i_G(g_1 \cdot g_2) = (g_1 \cdot g_2, e_H) = (g_1, e_H) \cdot (g_2, e_H) = i_G(g_1) \cdot i_G(g_2).$$

Similarly, i_H is a homomorphism.



Let φ and ψ be homomorphism from G and H to K respectively, we will show that there exists a unique homomorphism σ such that the diagram above commutes. Indeed, assume that that diagram commute, then for any $(g, h) \in G \times H$, we get

$$\begin{aligned}\sigma(g, h) &= \sigma((g, e_H) \cdot (e_G, h)) \\ &= \sigma(g, e_H) \cdot \sigma(e_G, h) \\ &= \sigma \circ i_G(g) \cdot \sigma \circ i_H(h) \\ &= \varphi(g) \cdot \psi(h).\end{aligned}$$

Here, the first equality by the operation on $G \times H$, the second equality is because σ is a homomorphism, and the last equality is because this diagram commutes. So if σ exists,

it is unique and $\sigma(g,h) = \varphi(g) \cdot \psi(h)$. Let $\sigma(g,h) := \varphi(g) \cdot \psi(h)$, we show that σ is a homomorphism. Indeed, for $(g_1,h_1),(g_2,h_2) \in G \times H$, we have

$$\sigma((g_1,h_1)\cdot(g_2,h_2)) = \sigma(g_1g_2, h_1h_2) = \varphi(g_1)\varphi(g_2)\psi(h_1)\psi(h_2).$$

But K is commutative, thus the previous equation becomes

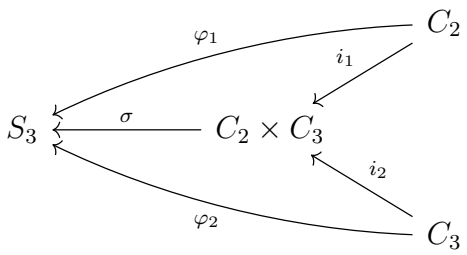
$$\varphi(g_1)\psi(h_1)\varphi(g_2)\psi(h_2) = \sigma(g_1,h_1)\cdot\sigma(g_2,h_2).$$

So σ is a homomorphism, which complete our proof. □

Exercise 3.6
Consider the product of the cyclic groups C_2, C_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 follow:

- 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.

Proof. Let $\varphi_1 \colon C_2 \to \{e, (1,2)\}$ and $\varphi_2 \colon C_3 \to \{e, (123), (132)\}$ be isomorphisms. Assume that $C_2 \times C_3$ is a coproduct of C_2 and C_3, then there exists a $\sigma \colon C_2 \times C_3 \to S_3$ that makes the diagram



commutes. So the image of σ must contain $\{e, (1,2), (123), (132)\}$. Since the image of σ is a subgroup, it equals S_3. But this is impossible because $C_2 \times C_3$ is abelian, whereas S_3 is not. So σ does not exist. □

4. Group homomorphisms

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

Proof. Let G be a group of order n. If $\varphi \colon G \to \mathbb{Z}/n\mathbb{Z}$ is an isomorphism, then $\varphi^{-1}(1)$ has order n by Proposition 4.8. Conversely, if $g \in G$ is an element of order n, then G is a cyclic group generated by n. But any cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, thus we have the conclusion. □

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

Proof. These sets are not isomorphic because $i \in \mathbb{C} \setminus \{0\}$ has order 4, where there is no order 4 element of $\mathbb{R} \setminus \{0\}$. □

Exercise 4.8
Let G be a group, and let $g \in G$. Prove that the function $\gamma_g \colon G \to G$ defined by $(\forall a \in G) : \gamma_g(a) = gag^{-1}$ is an automorphism 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.

Proof. For the first part, it is sufficient to show that γ_g is a homomorphism. Indeed, for any $a, b \in G$, we have

$$\gamma_g(a)\gamma_g(b) = (gag^{-1})(gbg^{-1}) = gabg^{-1} = \gamma_g(ab).$$

For the second part, let $g, h \in G$, then

$$gh \mapsto \gamma_{gh}.$$

But for any $a \in G$, we have

$$\gamma_{gh} = ghah^{-1}g^{-1} = g\gamma_h(a)g^{-1} = \gamma_g \circ \gamma_h(a).$$

Thus $\gamma_{gh} = \gamma_g \circ \gamma_h$, which prove that the function defined by $g \mapsto \gamma_g$ is a homomorphism. For the third part, if G is abelian, then $\gamma_g(a) = gag^{-1} = gg^{-1}a = a$. Thus $g \mapsto \gamma_g = \mathrm{Id}_G$ for all $g \in G$, which is the trivial homomorphism. Conversely, if $g \mapsto \gamma_g$ is trivial, then $\gamma_g(a) = a$ for all for any $g, a \in G$. But this implies that $ga = ag$ for any $a, g \in G$, thus G is abelian. □

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

Proof. Let d be the order of $e \in C_m \times C_n$, it is sufficient to show that $d = mn$. Because there is a natural homomorphism projection from $C_m \times C_n$ to C_m and $e_m \in C_m$ has order m, we get $m|d$. Similarly, we get $n|d$. But $(m, n) = 1$, thus $mn|d$, or $mn \leq d$ (this is because $d > 0$). But $C_m \times C_n$ has mn elements, thus $d \leq mn$. So $d = mn$, which complete our proof. □

Exercise 4.10
Let $p \neq q$ be odd prime integers; show that $(\mathbb{Z}/pq\mathbb{Z})^*$ is not cyclic.

Proof. Let us recall that

$$(\mathbb{Z}/n\mathbb{Z})^* := \{[m]_n \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(m,n) = 1\}.$$

One can easily see that the order of $(\mathbb{Z}/pq\mathbb{Z})^*$ is $\varphi(pq) = (p-1)(q-1)$, where φ is the Euler function. Assume that $(\mathbb{Z}/pq\mathbb{Z})^*$ is cyclic and is generated by t, then $t^{(p-1)(q-1)/2}$ is the only element that has order 2. We will show that $(\mathbb{Z}/pq\mathbb{Z})^*$ has at least 2 order-2 elements, thus contradicting to the cyclic hypothesis.

To find the first element, we consider the isomorphism $\varphi\colon \mathbb{Z}/pq\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$ that maps $[x]_{pq} \mapsto ([x]_p, [x]_q)$. We will claim that $a = \varphi^{-1}([1]_p, [-1]_q)$ has order 2. Indeed, $[a]_p = [1]_p$ implies $[a]_p^2 = [1]_p$ and $[a]_q^2 = [-1]_q^2 = [1]_q$. So $\varphi(a^2) = ([1]_p, [1]_q)$. But $\varphi([1]_{pq}) = ([1]_p, [1]_q)$, the "bijectiveness" of φ implies that $a^2 = [1]_{pq}$. Clearly $a \neq [1]_{pq}$ because $\varphi([1]_{pq}) = ([1]_p, [1]_q)$, we claim that a has order 2.

Similarly, we can point out that the second element is $b = \varphi^{-1}([-1]_p, [1]_q)$. Notice that $a \neq b$ because $p, q > 2$, thus $[1]_p \neq [-1]_p$ and similar for q. □

Exercise 4.11
In due time we will prove the easy fact that if p is a prime integer, then the equation $x^d = 1$ can have at most d solutions in $\mathbb{Z}/p\mathbb{Z}$. Assume this fact, and prove that the multiplicative group $G = (\mathbb{Z}/p\mathbb{Z})^*$ is cyclic.

Proof. Let $g \in G$ be the element of maximal order. Because G is commutative, Exercise 1.15 implies that $h^{|g|} = 1$ for all $h \in G$. It is not hard to check that $|G| = p - 1$, thus the equation $x^{|g|}$ has $p - 1$ zeros. By our hypothesis, $p - 1 \leq |g|$. Thus $|g| = p - 1$ and g is the element that generates G. □

Exercise 4.14
Prove that the order of the group of automorphisms of a cyclic group C_n is the number of positive integers $r < n$ that are relatively prime to n.

Proof. Let $C_n = \langle a \rangle$ be an arbitrary cyclic group. Any isomorphism $\varphi\colon C_n \to C_n$ is determined by where a is mapped to. Notice that φ is a homomorphism implies that $|\varphi(a)| \mid |a| = n$ and φ^{-1} homomorphic implies that $n \mid |\varphi(a)|$. So $|\varphi(a)| = n$. But a^r has order n if and only if $\gcd(r, n) = 1$, so the number of automorphism of C_n equals the number of r such that $\gcd(r, n) = 1$. □

Exercise 4.18
Prove the second part of Proposition 4.8. That is, let $\varphi\colon G \to H$ be an isomorphism. Show that G is commutative if and only if H is commutative.

Proof. For any $h_1, h_2 \in H$, the isomorphic of φ implies that there exists $g_1, g_2 \in G$ such that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. So

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

Therefore, H is commutative. □

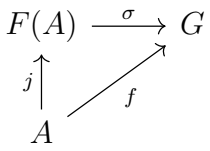
5. Free Group

Exercise 5.3
Use the universal property of free groups to prove that the map $j\colon A \to F(A)$ is injective, for all sets A.

Proof. For any $a, b \in A$ such that $j(a) = j(b)$, we define $G = \mathbb{Z}/2\mathbb{Z}$ and $f\colon A \to G$ as follow:

$$f(t) = \begin{cases} 0 & t \neq b, \\ 1 & t = b. \end{cases}$$

The universal property of free group implies the existence of a homomorphism $\sigma\colon F(A) \to G$ such that the diagram below commutes.

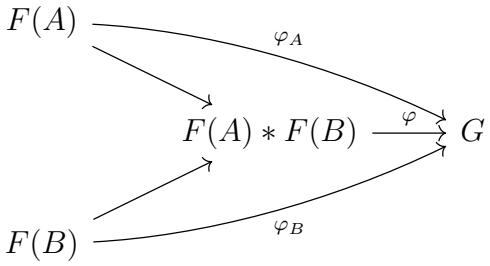


But this means $f(a) = \sigma \circ j(a) = \sigma \circ j(b) = f(b) = 1$. So the definition of f implies that $a = b$. □

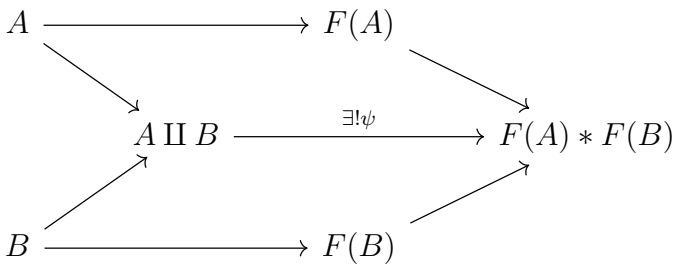
Exercise 5.8
Still more generally, prove that $F(A \amalg B) = F(A) * F(B)$ and that $F^{ab}(A \amalg B) = F^{ab}(A) \oplus F^{ab}(B)$ for all sets A, B.

Proof. We will show that $F(A) * F(B)$ satisfies the universal property of $F(A \amalg B)$. Indeed, for any group G and a set function $f\colon A \coprod B \to G$, the universal properties of $F(A)$ and $F(B)$ imply that there are unique φ_A and φ_B such that the following diagrams commute.

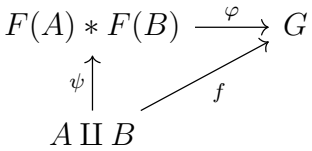
Again, using the universal property of $F(A) * F(B)$, there exists a unique φ such that the following diagram commutes.



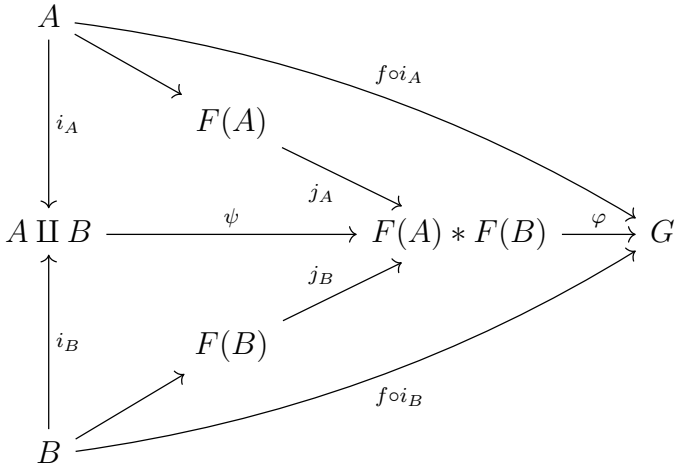
And defining the map from $A \amalg B \to F(A) * F(B)$ to be the unique map ψ such that this diagram commutes,



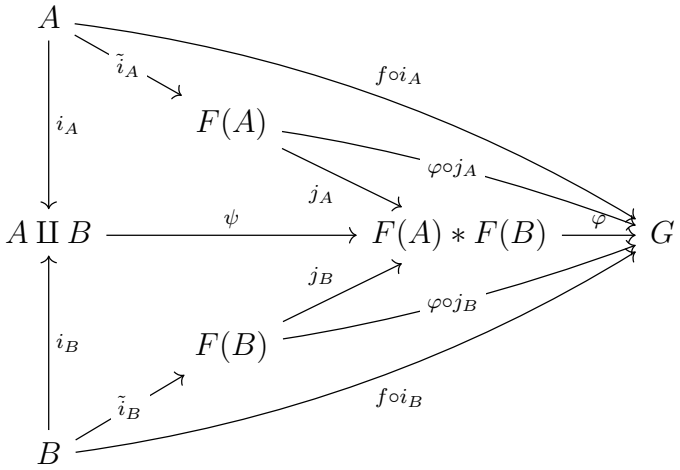
for any $f\colon A \amalg B \to G$, there exists a φ such that this diagram commutes.



Now we prove the uniqueness of φ. Assume that there exists a $\varphi\colon F(A) * F(B) \to G$ such that the diagram above commutes, then this (giant!!!) diagram is commute. (Because $f = \varphi \circ \psi$ and any path from A to G is the same as $\varphi \circ \psi \circ i_A = f \circ i_A$, and the same for B).



And just by composing φ and j_A, j_B, we get this (even bigger) commutative diagram.



A few things to notice here. First, $\varphi \circ j_A$ is a composition of two group homomorphisms, thus it is a group homomorphism. Second, this map $\varphi \circ j_A$ is unique by the universal property of $F(A)$, and the same for $\varphi \circ j_B$. And last, using the universal property of $F(A) * F(B)$, φ must be unique as well.

Since $F(A) * F(B)$ satisfies $F(A \amalg B)$'s universal property, they are isomorphic. The proof for abelian part is similar. □

6. Subgroups

Exercise 6.1
Consider the following sets of matrices:

- $SL_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) \mid \det(M) = 1\}$;
- $SL_n(\mathbb{C}) = \{M \in GL_n(\mathbb{C}) \mid \det(M) = 1\}$;
- $O_n(\mathbb{R}) = \{M \in GL_n(\mathbb{R}) \mid MM^t = M^tM = I_n\}$;
- $SO_n(\mathbb{R}) = \{M \in O_n(\mathbb{R}) \mid \det(M) = 1\}$;
- $U_n(\mathbb{C}) = \{M \in GL_n(\mathbb{C}) \mid MM^\dagger = M^\dagger M = I_n\}$;
- $SU_n(\mathbb{C}) = \{M \in U_n(\mathbb{C}) \mid \det(M) = 1\}$.

Find all possible inclusions among these sets, and prove that in every case the smaller set is a subgroup of the larger one.

Proof. For each of the six sets, say S, we will show that $a, b \in S$ implies $ab \in S$ and $a^{-1} \in S$.

- Let $A, B \in SL_n(\mathbb{R})$ (and equivalently $SL_n(\mathbb{C}), SO_n(\mathbb{R}), SU_n(\mathbb{C})$). We have
$$\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1.$$
Moreover, because $\det(A) = 1$, we get
$$\det(A^{-1}) = \det(A^{-1})\det(A) = \det(I_n) = 1.$$
So $SL_n(\mathbb{R})$ is a subgroup.
- Let $A, B \in U_n(\mathbb{C})$ (and equivalently $U_n(\mathbb{C})$). We have
$$(AB)(AB)^\dagger = ABB^\dagger A^\dagger = AA^\dagger = I_n.$$
Similarly, $(AB)^\dagger(AB) = I_n$. Moreover, clearly $A^\dagger = A^{-1}$, thus $A^{-1} \in U_n(\mathbb{C})$. So $U_n(\mathbb{C})$ (and equivalently $U_n(\mathbb{C})$) is a subgroup.

So in order to find which is a subgroup of which, we only need to check which is a subset of which. It is not hard to see that $SO_n(\mathbb{R}) \subset O_n(\mathbb{R}) \subset U_n(\mathbb{C})$, $SO_n(\mathbb{C}) \subset SL_n(\mathbb{R}) \subset SL_n(\mathbb{C}), SO_n(\mathbb{R}) \subset SU_n(\mathbb{C}) \subset SL_n(\mathbb{C})$. So these are all the possible subgroups among these sets. □

Exercise 6.3
Prove that every matrix in $SU_2(\mathbb{C})$ 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, $SU_2(\mathbb{C})$ may be realized as a three dimensional sphere embedded in $\mathbb{R}^4$.)

Exercise 6.7
Show that inner automorphisms 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. Deduce that if $\mathrm{Aut}(G)$ is cyclic, then G is abelian.

Proof. Let's remind that an inner automorphism of G has the form $\gamma_g : G \to G$ that maps $x \mapsto gag^{-1}$. Let $\mathrm{Inn}(G) = \{\gamma_g : g \in \mathcal{G}\}$, we will prove that $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$. Clearly $\mathrm{Inn}(G) \neq \varnothing$ since G is nonempty. For any $\gamma_g, \gamma_h \in \mathrm{Inn}(G)$, we have

$$\gamma_g \circ \gamma_h^{-1} = \gamma_g \circ \gamma_{h^{-1}} = \gamma_{gh^{-1}} \in \mathrm{Inn}(G).$$

So $\mathrm{Inn}(G)$ is indeed a subgroup of $\mathrm{Aut}(G)$.

Assume that $\mathrm{Inn}(G)$ is cyclic, and is generated by γ_a. Then for any $\gamma_g \in \mathrm{Inn}(G)$, there is an $n \in \mathbb{N}$ such that $\gamma_a^n = \gamma_g$. That is, for any $x \in \mathbb{R}$, we have

$$a^n x a^{-n} = gxg^{-1}.$$

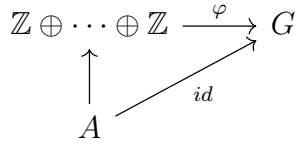
Let $x = a$, we get $a = gag^{-1}$, or g commutes with every element of G. Therefore $\gamma_g(x) = gxg^{-1} = gg^{-1}x = x$ for all $x \in G$. So γ_g is trivial for all $g \in G$. This yields $\mathrm{Inn}(G)$ to be trivial. If $\mathrm{Inn}(G)$ is trivial, then G be abelian by Exercise 4.8. And finally, if G is abelian then $\mathrm{Inn}(G)$ is trivial, thus cyclic. We complete our proof. □

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

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

for some n.

Proof. Assume that G is finitely generated by n elements $A = \{x_1, x_2, \cdots, x_n\}$. Consider the identity set function from A to G that maps $x_i \mapsto x_i$. Since $F(A)$ is the initial object in $\mathcal{F}^A$, there is a group homomorphism $\varphi\colon F(A) \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} \to G$ such that the following diagram commutes



Since $(id) \subset (\varphi)$, we get $A \subset (\varphi)$. But A generates G, thus $(\varphi) = G$. So φ is such surjective homomorphism. □

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

Proof. The proof of the first part is for subgroups generated by 2 fraction. We can deduce the finite case with simple induction. Assume that $G = \langle \frac{p_1}{q_1}, \frac{p_2}{q_2} \rangle = \langle \frac{p_1 q_2}{q_1 q_2}, \frac{p_2 q_1}{q_1 q_2} \rangle$. Let $d = \gcd(p_1 q_2, p_2 q_1)$, then it is not hard to see that $G = \langle \frac{d}{q_1 q_2} \rangle$. So any finitely generated subgroup of $\mathbb{Q}$ is cyclic.

If $\mathbb{Q}$ is finitely generated, then the first part implies that $\mathbb{Q}$ is cyclic. Assume that $\mathbb{Q} = \langle \frac{p}{q} \rangle$ then clearly $\frac{1}{q+1} \notin \mathbb{Q}$, contradiction. So $\mathbb{Q}$ is not finitely generated. □

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

Proof. Because cyclic groups are abelian, coproduct coincides with product. Because $|S_3| = 6$, if S_3 is a product of two cyclic groups, it is either $\mathbb{Z}_6$ or $\mathbb{Z}_3 \times \mathbb{Z}_2$. Notice that S_3 has 3 rank 2 elements, but both $\mathbb{Z}_6$ and $\mathbb{Z}_2 \times \mathbb{Z}_3$ has 1 rank 2 element, thus it is not a coproduct of cyclic groups. □

Exercise 6.15
Prove that if a group homomorphism $\varphi\colon G \to G'$ has a left-inverse, that is, a group homomorphism $\psi\colon G' \to G$ such that $\psi \circ \varphi = id_{G'}$, then φ is a monomorphism.

Proof. For any two group homomorphisms $\alpha, \beta\colon G' \to A$ such that $\varphi \circ \alpha = \varphi \circ \beta$, we have

$$\alpha = id \circ \alpha = \psi \circ \varphi \circ \alpha = \psi \circ (\varphi \circ \beta) = id \circ \beta = \beta.$$

So φ is a monomorphism. □

7. Quotient groups

Exercise 7.1
List all subgroups of S_3 and determine which subgroups are normal and which are not normal.

Proof. Because S_3 has 6 elements, subgroups of S_3 has either $1, 2, 3$, or 6 elements. Let $A \subset S_3$ be a subgroup of S_3. If A has 1 or 6 elements, A is the trivial normal subgroup. If A has 3 elements, then the coset of A has 2 elements. This also implies that A is normal. If A has 2 elements, then without loss of generality, we can assume that $A = \{e, (12)\}$. But $(13)(12)(13) = (23) \notin A$. So A is not normal. In conclusion, S_3 has 3 normal subgroups, which are

$$\{\{e\}; \{e, (123), (132)\}; S_3\}.$$

The rest of subgroups of S_3 include $\{e, (12)\}, \{e, (23)\}, \{e, (13)\}$. □

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

Proof. Well, no. One counter example is $\varphi\colon \mathbb{Z}/2\mathbb{Z} \to S_3$ that maps $e \mapsto e$ and $\bar{1} \mapsto (12)$. It is not hard to check that φ is a group homomorphism, but the image is not a normal subgroup by exercise 7.1. □

Exercise 7.6
Let G be a group, and let n be a positive integer. Consider the relation

$$a \sim b \iff (\exists g \in G) ab^{-1} = g^n.$$

- Show that in general $\sim$ is not an equivalent relation.
- Prove that $\sim$ is an equivalent relation if G is commutative, and determine the corresponding subgroup of G.

Proof. We first show $\sim$ is an equivalent relation if G is commutative. Clearly $a \sim a$ because $aa^{-1} = e = e^n$. If $a \sim b$ then $ab^{-1} = g^n$. Thus $ba^{-1} = (ab^{-1})^{-1} = (g^{-1})^n$. If $a \sim b$ and $b \sim c$ then $ab^{-1} = g_1^n$ and $bc^{-1} = g_2^n$. Thus

$$ac^{-1} = (ab^{-1})(bc^{-1}) = g_1^n g_2^n = (g_1 g_2)^n.$$

Thus $a \sim c$. So when G is commutative, $\sim$ defines an equivalent relation. The corresponding subgroups to this relation is $\{a \in G : a \sim e\}$ or $\{a \in G : a = g^n \text{ for all } g \in G\}$. This group equals $\{g^n : g \in \mathcal{G}\}$. Notice that this is indeed a subgroup because

$$g_1^n (g_2^{-1})^n = (g_1 g_2^{-1})^n.$$

Without the abelian property on G, this is not an equivalent relation however. Take $G = S_3$ and $n = 3$. Then $e \sim (12)$ because $e \cdot (12)^{-1} = (12) = (12)^3$. Moreover, $(12)(123)^{-1} = (12)(132) = (13) = (13)^3$, thus $(12) \sim (123)$. However $e \not\sim (123)$ because I have checked all the possibility. Specifically, $(12)^3 = (12)$ and $(123)^3 = e$. □

Exercise 7.8
Prove Proposition 7.6.

Exercise 7.13
Let A, B be sets and $F(A), F(B)$ the corresponding free groups. Assume $F(A) \cong F(B)$. If A is finite, prove that B is also finite and $A \cong B$.

Proof. Assume that $F(A) \cong F(B)$ then $[F(A), F(A)] \cong [F(B), F(B)]$. Thus

$$\begin{aligned}
\mathbb{Z}^{\oplus A} &\cong F^{ab}(A) \\
&\cong F(A)/[F(A), F(A)] \\
&\cong F(B)/[F(B), F(B)] \\
&\cong F^{ab}(B) \\
&\cong \mathbb{Z}^{\oplus B}.
\end{aligned}$$

So if A is finite, B is finite and $A \cong B$. □

8. Canonical decomposition and Lagrange's theorem

Exercise 8.2
Extend Example 8.6 as follows. Suppose G is a group and $H \subset G$ is a subgroup of index 2, that is, such that there are precisely two cosets of H in G. Prove that H is normal in G.

Proof. If H has index 2, then for some $a \notin H$, we have $G = H \cup aH$. For any $h \in H$ and $g \in G$, if $g \in H$ then obviously $ghg^{-1} \in H$. Otherwise, $g = ah_1$ for some $h_1 \in H$. Thus

$$ghg^{-1} = (ah_1)h(h_1^{-1}a^{-1}) = a(h_1hh_1^{-1})a^{-1}.$$

So all we need to prove is $aha^{-1} \in H$ for all $h \in H$. If $aha^{-1} \notin H$ then

$$aha^{-1} = ah'$$

for some $h' \in H$. Using the cancellation law and moving h over to the right hand side, we get

$$a = (a^{-1})^{-1} = (hh')^{-1} = h'^{-1}h^{-1} \in H,$$

contradiction. So H is indeed a normal subgroup of G. □

Exercise 8.3
Prove that every finite group is finitely presented.

Proof. Assume that G is a group of n elements $\{g_1, g_2, \cdots, g_n\}$. For any real number i, j from 1 to n not necessarily distinct, if $g_ig_j = g_k$, then we let $r_{ij} := g_ig_jg_k^{-1}$. We claim that

$$(g_1, g_2, \cdots, g_n \mid r_{ij}) \cong G. \tag{1}$$

Clearly this is finitely presented because there are n^2 relations and n generators. So we only need to show (1) now. Let $\mathrm{Id} : G \to G$ be the identity from the set G to group G. So by the universal property of the free product, there exist a unique φ such that the following diagram commutes.

$$\begin{array}{ccc} F(g_1, \cdots, g_n) & \xrightarrow{\exists!\varphi} & G \\ \uparrow & \nearrow_{\mathrm{Id}} & \\ \{g_1, \cdots, g_n\} & & \end{array}$$

So we need to check that $\{r_{ij}\}$ generates $\ker\varphi$. Clearly

$$\varphi(r_{ij}) = \varphi(g_ig_jg_k^{-1}) = g_ig_jg_k^{-1} = e,$$

so $r_{ij} \in \ker\varphi$. Conversely, any word in the kernel of φ has the form

$$e = g_{j_1}g_{j_2}\cdots g_{j_m}.$$

Assume that $g_{j_1}g_{j_2} = g_{k_1}$, then we let $r_1 = g_{j_1}g_{j_2}g_{k_1}^{-1}$ and rewrite the word above as

$$g_{j_1}g_{j_2}g_{k_1}^{-1}g_{k_1}g_{j_3}\cdots g_{j_m} = r_1g_{k_1}g_{j_3}\cdots g_{j_m}.$$

Continue this progress for $g_{k_1}g_{j_3}$, we end up with

$$r_1 r_2 \cdots r_{m-1} g$$

for $r_t \in \{r_{ij} : i, j \in \mathbb{N}\}$ and $g \in G$. Because

$$e = \varphi(g_{j_1} g_{j_2} \cdots g_{j_m}) = \varphi(r_1 r_2 \cdots r_{m-1} g) = \varphi(r_1)\varphi(r_2)\cdots\varphi(r_{m-1})\varphi(g) = \varphi(g).$$

But $\varphi(g) = \mathrm{Id}(g)$ thus g is the identity or $r_m := ggg^{-1} \in \{r_{ij} \mid i, j \in \mathbb{N}\}$. So in $F(g_1, \cdots, g_n)$, we have

$$g_{j_1} g_{j_2} \cdots g_{j_m} = r_1 r_2 \cdots r_m \in \ker(\varphi).$$

So G is finitely presented. □

Exercise 8.4
Prove that $(a, b \mid a^2, b^2, (ab)^n)$ is a presentation of the dihedral group D_{2n}.

Proof. By definition, a dihedral group is generated by reflection and rotation. For an n-gon, there matrix would be $f = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$ and $r = \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}$ where $\theta = 2\pi/n$. So $D_{2n} = \langle f, r \rangle \subset GL_2(\mathbb{R})$. We will show that is group has the presentation

$$\langle x, y \mid x^2, y^n, xy = y^{n-1}x \rangle.$$

Let $\psi \colon \{x, y\} \to D_{2n}$ that maps x, y to f, r respectively. The universal property of $F(x, y)$ implies the existence of φ such that the following diagram commutes.

$$\begin{array}{ccc} F(x,y) & \xrightarrow{\varphi} & D_{2n} \\ \uparrow & \nearrow_{\psi} & \\ \{x, y\} & & \end{array}$$

Notice that since $\varphi(x) = f$ and $\varphi(y) = r$ generate D_{2n}, we get φ to be surjective. So we only need to prove $\{x^2, y^n, xyx^{-1}y^{n-1}\}$ generates $\ker\varphi$. Using matrix multiplication, we find that

$$\varphi(x^2) = \varphi(x)^2 = \psi(x)^2 = f^2 = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^2 = \mathrm{Id}\,.$$

Similarly we get

$$\begin{aligned} \varphi(y^n) &= r^n \\ &= \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix}^n \\ &= \begin{pmatrix} \cos(n\theta) & -\sin(n\theta) \\ \sin(n\theta) & \cos(n\theta) \end{pmatrix} \\ &= \begin{pmatrix} \cos(2\pi) & -\sin(2\pi) \\ \sin(2\pi) & \cos(2\pi) \end{pmatrix} \\ &= \mathrm{Id} \end{aligned}$$

and

$$\varphi(y^{n-1}x) = \varphi(y)^{n-1}\varphi(x) = r^{n-1}f\begin{pmatrix} -\cos(\theta) & -\sin(\theta) \\ -\sin(\theta) & \cos(\theta) \end{pmatrix} = rf = \varphi(xy).$$

So these ugly calculations tell us that $x^2, y^n, xyx^{-1}y^{n-1}$ are indeed in $\ker\varphi$. So $D_{2n} \subset \langle x, y \mid x^2, y^n, xy = y^{n-1}x\rangle$. We will now show that $\langle x, y \mid x^2, y^n, xy = y^{n-1}x\rangle$ can have at most $2n$ elements, thus equal D_{2n}.

Indeed, we claim that any element in $\langle x, y \mid x^2, y^n, xy = y^{n-1}x\rangle$ has the form y^ix^j for $0 \le i \le n-1$ and $0 \le j \le 1$. Notice that there are exactly $2n$ elements of that form.

For any word in $F(x, y)$, we can use the relation $xy = y^{n-1}x$ to commute x and y such that all y's are on the left and x's on the right. (This process can be done rigorously but rather tedious, plus this is already clear enough.) So we end up with this word y^cx^d. Next we use the relation $y^n = e$ and $x^2 = e$ to reduce c and d into the form y^ix^j for $0 \le i \le n-1$ and $0 \le j \le 1$. So $D_{2n} = \langle x, y \mid x^2, y^n, xy = y^{n-1}x\rangle$.

Ok, so we have this presentation in our hand, we will prove that

$$D_{2n} = \langle x, y \mid x^2, y^n, xy = y^{n-1}x\rangle \cong \langle a, b \mid a^2, b^2, (ab)^n\rangle.$$

Let

$$f_1 \colon \langle x, y \mid x^2, y^n, xy = y^{n-1}x\rangle \to \langle a, b \mid a^2, b^2, (ab)^n\rangle$$

that maps $x \mapsto a$ and $y \mapsto ab$. Let

$$f_2 \colon \langle a, b \mid a^2, b^2, (ab)^n\rangle \to \langle x, y \mid x^2, y^n, xy = y^{n-1}x\rangle$$

that maps $a \mapsto x$ and $b \mapsto xy$. There are two things we need to check: f_1, f_2 are group homomorphisms, and $f_1 \circ f_2 = f_2 \circ f_1 = \mathrm{Id}$.

For the first point, we have

$$f_1(x^2) = f_1(x)^2 = a^2 = e,$$
$$f_1(y^n) = f_1(y)^n = (ab)^n = e,$$

and finally

$$f_1(xy) = f_1(x)f_1(y) = aab = b,$$

and

$$f_1(y^{n-1}x) = f_1(y)^{n-1}f_1(x) = (ab)^{n-1}a = (ab)^{n-1}ab^2 = (ab)^nb = b = f_1(xy).$$

So f_1 is a group homomorphism. Similarly, we have

$$f_2(a^2) = x^2 = e,$$
$$f_2(b^2) = (xy)^2 = (y^{n-1}x)(xy) = y^{n-1}y = e,$$

and

$$f_2((ab)^n) = (xxy)^n = y^n = e.$$

So f_2 is also a group homomorphism. Lastly, we can easily see that

$$f_2(f_1(x)) = f_2(a) = x, \quad f_2(f_1(y)) = f_2(ab) = xxy = y,$$

and

$$f_1(f_2(a)) = f_1(x) = a, \quad f_1(f_2(b)) = f_1(xy) = aab = b.$$

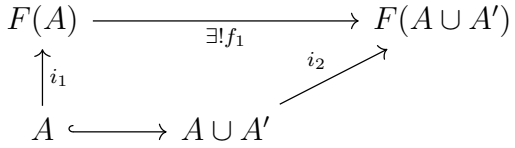
So in the end $f_1 \circ f_2 = f_2 \circ f_1 = \mathrm{Id}$ or f_1 is a group isomorphism. In another words, $D_{2n} = \langle a, b \mid a^2, b^2, (ab)^n\rangle$. □

Exercise 8.7
Let $(A \mid R), (A' \mid R')$ be a presentation for a group G and G' respectively. We may assume that A and A' are disjoint. Prove that the group $G * G'$ presented by

$$(A \cup A' \mid R \cup R')$$

satisfies the universal property for the coproduct of G and G' in Grp

Proof. First, we will construct a group homomorphism from $(A \mid R)$ to $(A \cup A' \mid R \cup R')$. Using the univeral property of $F(A)$, there exists a unique group homomorphism f_1 such that the following diagram commute.



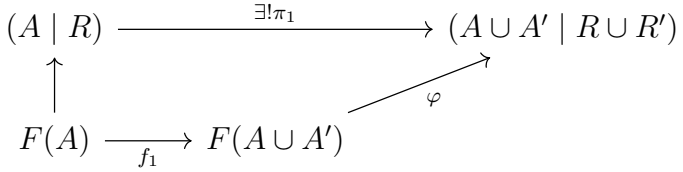
That means for any word $i_1(a_1)i_1(a_2)\cdots i_1(a_n) \in F(A)$ such that $a_i \in A$, then

$$f_1(i_1(a_1)i_1(a_2)\cdots i_1(a_n)) = f_1 \circ i_1(a_1)\cdots f_1 \circ i_1(a_n) = i_2(a_1)i_2(a_2)\cdots i_2(a_n).$$

We can safely omit i_1 and i_2 to get

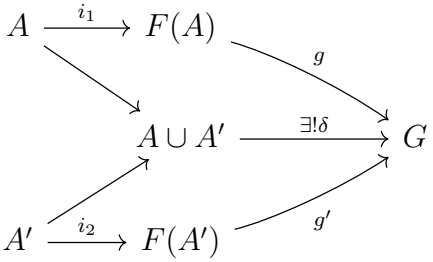
$$f_1(a_1 \cdots a_n) = a_1 \cdots a_2$$

for $a_i \in A \subset F(A)$. So $f_1(a) = a$ for all $a \in F(A)$. Let $\varphi\colon F(A \cup A') \to (A \cup A' \mid R \cup R')$ where $\ker \varphi = (R \cup R')$. For any $r \in R \subset F(A)$, we have $\varphi \circ f_1(r) = \varphi(r) = 0$. Thus $R \subset \ker \varphi \circ f_1$. Using the universal property of the quotient group $(A|R)$, there exists a unique homomorphism $\pi_1\colon (A|R) \to (A \cup A'|R \cup R')$ sucht that the following diagram commutes.

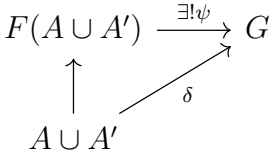


Construct similarly a homomorphism $\pi_2\colon (A'|R') \to (A \cup A'|R \cup R')$.

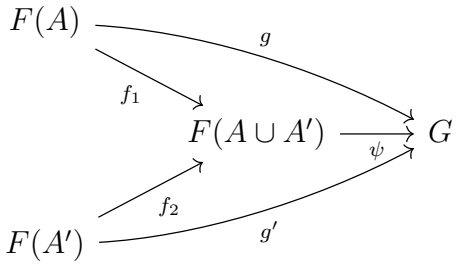
Before continue, we will prove this short and useful result, that is $F(A \cup A')$ satisfies the coproduct universal property of $F(A)$ and $F(A')$. Indeed, for any group G, $g\colon F(A) \to G$, and $g'\colon F(A') \to G$, we get $g \circ i_1\colon A \to G$ and $g \circ i_2\colon A' \to G$. So by the universal property of $A \cup A'$, the coproduct of A and A' in Set, there exists uniquely a function $\delta\colon A \cup A' \to G$ such that the following diagram commute.



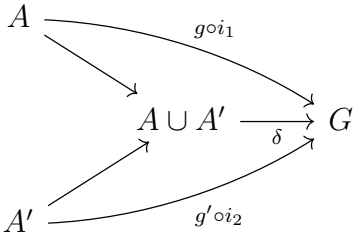
So by the universal property of $F(A \cup A')$, there exists uniquely a function $\psi\colon F(A \cup A') \to G$ such that the following diagram commutes.



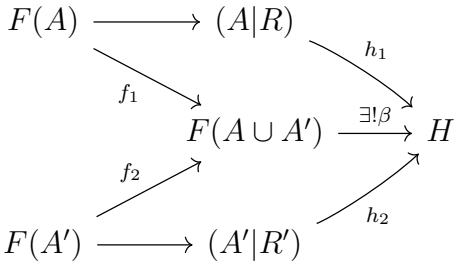
Base on our construction, such ψ that makes the following diagram commutes is unique. Now we show that ψ indeed makes this diagram commutes.



But this is not hard to see since the underling set structure commutes, that is the following diagram.

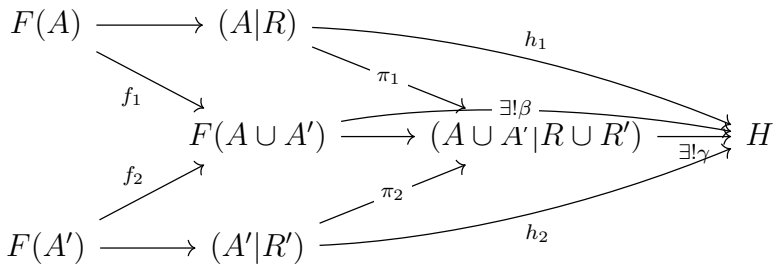


So $F(A \cup A')$ is the coproduct of $F(A)$ and $F(A')$. Back to our problem, assume that H is a group, $h_1\colon (A|R) \to H$ and $(A'|R') \to H$ be group homomorphism, then the universal property of the coproduct $F(A \cup A')$ implies the unique homomorphism β such that the following diagram commute.

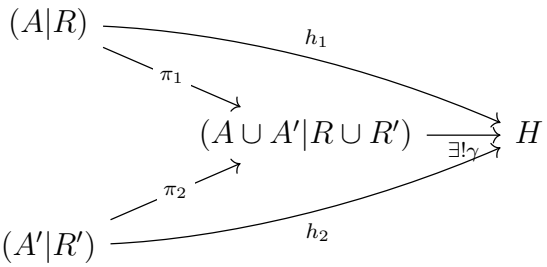


Notice that if $r \in R \cup R'$, then $\beta(r) = \beta \circ f_1(r)$. If $r \in R$ then the branch above implies that $\beta \circ f_1(r) = 0$ and if $r \in R'$ then we use the bottom one. So $R \cup R' \in \ker \beta$, thus the universal property if the quotient space $(A \cup A'|R \cup R')$ implies the unique existence of

$\gamma\colon (A \cup A'|R \cup R')$ such that the following diagram commutes.



Or we can simplify to the following commutative diagram.



So $(A \cup A'|R \cup R')$ satisfy the universal property of the coproduct of $(A|R)$ and $(A'|R')$, which complete our proof. □

Exercise 8.8
Prove that $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$, and 'compute' $GL_n(\mathbb{R})/SL_n(\mathbb{R})$ as a well known group.

Proof. Assume that $A \in SL_n(\mathbb{R})$, then $\det(A) = 1$. For any $B \in GL_n(\mathbb{R})$, we have

$$\det(BAB^{-1}) = \det(B)\det(A)\det(B)^{-1} = \det(A) = 1.$$

So $BAB^{-1} \in SL_n(\mathbb{R})$ for all $B \in GL_n(\mathbb{R})$. Thus $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$.

We will now show that $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong (\mathbb{R}^*, \cdot)$. Clearly $\det\colon GL_n(\mathbb{R}) \to (\mathbb{R}^*, \cdot)$ is a group homomorphism since

$$\det(AB) = \det(A)\det(B).$$

Moreover, $\ker\det = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\} = SL_n(\mathbb{R})$. So by the first homomorphism theorem we get

$$GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong (\mathbb{R}^*, \cdot).$$

□

Exercise 8.9
Prove that $SO_3(\mathbb{R}) \cong SU_2(\mathbb{C})/\{\pm I_2\}$, where I_2 is the identity matrix. Conclude that the fundamental group of $SO_3(\mathbb{R})$ is C_2.

Proof. It is known that any element of $SO_3(\mathbb{R})$ has the form

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

and any element of $SU_2(\mathbb{C})$ has the form

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

such that $a^2+b^2+c^2+d^2=1$. Define a group homomorphism $f\colon SU_2(\mathbb{C}) \to SO_3(\mathbb{R})$ that maps

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

By some brutal calculation that only calculators enjoy doing, we know that f is a homomorphism. If $A = \begin{pmatrix} a+bi & c+di \\ -c+di & a-bi \end{pmatrix} \in \ker f$, then $a^2+b^2-c^2-d^2=1$, thus a and b can't simultaneously be 0. Similarly for a, c and a, d. Notice that

$$f(A)_{12} = f(A)_{21} = 0,$$

thus $ad+bc = -ad+bc$ or $ad=0$. Thus $bc=0$. Similarly, we get $ac=bd=ab=cd=0$. Notice that $bd=cd=bc=0$ implies that one of the b, c, d must be 0. Our observation above implies that $a \neq 0$. Thus $b=c=d=0$. But $a^2+b^2+c^2+d^2=1$, thus $a \in \pm 1$. So $A = \pm 1$. we can easily check that $f(\pm I_2) = I_3$. So by first homomorphism theorem, we get

$$SO_3(\mathbb{R}) \cong SU_2(\mathbb{C})/\{\pm I_2\}.$$

□

Exercise 8.10
View $\mathbb{Z} \times \mathbb{Z}$ as a subgroup of $\mathbb{R} \times \mathbb{R}$. Describe the quotient

$$\frac{\mathbb{R} \times \mathbb{R}}{\mathbb{Z} \times \mathbb{Z}}$$

in terms analogous to those used in Example 8.7.

Proof. Because $\frac{\mathbb{R}}{\mathbb{Z}} \cong \mathbb{S}^1$, thus

$$\frac{\mathbb{R} \times \mathbb{R}}{\mathbb{Z} \times \mathbb{Z}} \cong \frac{\mathbb{R}}{\mathbb{Z}} \times \frac{\mathbb{R}}{\mathbb{Z}} \cong \mathbb{S}^1 \times \mathbb{S}^1 \cong \mathbb{T}^1.$$

So this is a torus. □

Exercise 8.17
Assume G is a finite abelian group, and let p be a prime divisor of $|G|$. Prove that there exists an element in G of order p.

Proof. The proof is on induction of $|G|$. If $|G| = 1$ then $|G|$ has no prime order so we are done. Assume that our claim holds when $|G| \leq k-1$. Let $|G| = k$ and $p|k$. Let $g \in G$ and $g \neq e$, then $n := |\langle g \rangle| > 1$. If $p|n$ then $g^{\frac{n}{p}}$ has order p. If $p \not| n$ then n and p are relatively prime, thus $p|\frac{k}{n}$. Moreover, because G is abelian thus $\langle g \rangle$ is normal. By Lagrange's theorem, $|G/\langle g \rangle| = k/n < k$ and our induction hypothesis implies the existence of $t\langle g \rangle$ of order p. So p is a divisor of $|\langle t \rangle| = n'$. Thus $t^{\frac{n'}{p}}$ has order p. □

Exercise 8.24
Show that epimorphisms in Grp do not necessarily have right-inverses.

Proof. Let $f\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be the group homomorphism reducing module 2. Thus $0 \mapsto 0$ and $2 \mapsto 0$. This is clearly an epimorphism. But there is only one trivial map $g\colon \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z}$. Indeed, because $g(1)+g(1) = g(0) = 0$ thus $g(1) = 2$. But $f \circ g(1) = 0$ thus not the identity. □

9. Group actions

Exercise 9.1
The matrix groups listed in Exercise 6.1 all come with evident actions on a vector space.

- Prove that, through this action, matrices $M \in O_n(\mathbb{R})$ preserve lengths and angles in $\mathbb{R}^n$.
- Find an intersting action of $SU_2(\mathbb{C})$ on $\mathbb{R}^3$.

Proof.

- Let $M \in O_n(\mathbb{R})$, then $M^tM = MM^t = I_n$. We will prove that this action preserve the inner product, thus so is the lengths and angles in $\mathbb{R}^n$. For $v, u \in \mathbb{R}^n$, we have
$$\langle Mv, Mu \rangle = \langle M^tMv, u \rangle = \langle v, u \rangle.$$
So M preserve lengths and angles.

- We have $SU_2(\mathbb{C})/\{\pm I_2\}$ is a quotient of $SU_2(\mathbb{C})$, thus there is a natural quotient homomorphism
$$\varphi\colon SU_2(\mathbb{C}) \to SU_2(\mathbb{C})/\{\pm I_2\} \cong SO_3(\mathbb{R})$$
(by Exercise 8.9). Define an action $*\colon SU_2(\mathbb{C}) \times \mathbb{R}^3 \to \mathbb{R}^3$ by
$$M * v \mapsto \varphi(M)v.$$
Clearly $I_{\mathbb{C}} * v = \varphi(I_{\mathbb{C}})v = Iv = v$ and for any $M, N \in SU_2(\mathbb{C})$, the homomorphism φ implies that
$$M * (N * n) = M * \varphi(N)v = \varphi(M)\varphi(N)v = \varphi(MN)v = MN * v.$$

So $*$ is indeed a group action and it seems interesting to me.

□

Exercise 9.2
The effect of the matrices

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

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

Proof. From Exercise 8.4, we know that

$$D_8 \cong \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \cos(\pi/2) & \sin(\pi/2) \\ -\sin(\pi/2) & \cos(\pi/2) \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle.$$

Since this is a subgroup of $M_2(\mathbb{R})$, there is a natural group action of D_8 on $\mathbb{R}^2$ by matrix multiplication. □

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

Proof. Let G be a group and $g \in G$. If there exists any element $h \in G$ such that $gh = h$ (that is fixing an element h), then the cancelation law implies that $g = e$. So e is the only element that fix any element of G. Thus this is a free action. □

Exercise 9.7
Prove that stabilizers are indeed subgroups.

Proof. Let G be a group that acts on a set A. For any $a \in A$, recall that

$$\mathrm{Stab}_G(a) = \{g \in G : ga = a\}.$$

This is nonempty because by the axioms of group action, $e_G \in \mathrm{Stab}_G(a)$. Moreover, for any $g, h \in \mathrm{Stab}_G(a)$, we have

$$g^{-1}a = g^{-1}(ga) = e_G a = a$$

and

$$(gh)a = g(ha) = ga = a.$$

So $g^{-1}, gh \in \mathrm{Stab}_G(a)$, which implies that $\mathrm{Stab}_G(a)$ is indeed a subgroup. □

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

Proof. Assume that $(A,\varphi_1),(B,\varphi_2),(C,\varphi_3)$, and (D,φ_4) are objects of the category G-Set, where φ_i are group actions. Assume further that $f \in \mathrm{Hom}((A,\varphi_1),(B,\varphi_2))$, $g \in \mathrm{Hom}((B\varphi_2),(C,\varphi_3))$, and $h \in \mathrm{Hom}((C,\varphi_3),(D,\varphi_4))$. We first show that $g \circ f \in \mathrm{Hom}((A,\varphi_1),(C,\varphi_3))$. Indeed, for any $a \in A$, we have

$$g \circ f(\varphi_1(a)) = g(\varphi_1(f(a))) = \varphi_1(g(f(a)) = \varphi_1(g \circ f(a)).$$

Clearly we have $h \circ (g \circ f) = (h \circ g) \circ f$ since these are just compositions of set functions. Lastly, we show that $\mathrm{Id}\colon B \to B$ is the identity homomorphism of $\mathrm{Hom}((B,\varphi_2),(B,\varphi_2))$. Because for any $b \in B$, we have

$$\mathrm{Id}(\varphi_2(b)) = \varphi_2(b) = \varphi_2(\mathrm{Id}(b)).$$

So $\mathrm{Id} \in \mathrm{Hom}((B,\varphi_2),(B,\varphi_2))$. Moreover, $Id \circ f = f$ and $g \circ \mathrm{Id} = g$ because, again, these are just set functions. So G-Set is indeed a category.

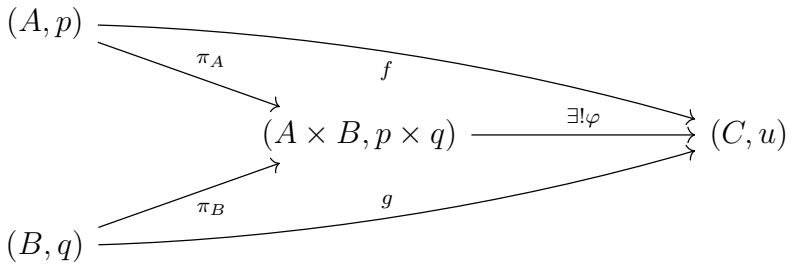
If $f \in \mathrm{Hom}((A,\varphi_1),(B,\varphi_2))$ is a bijective equivariant, then $f\colon A \to B$ is a bijection under Set. Let f^{-1} be the inverse of f under set, then for any $b \in B$, there is some $a \in A$ such that $f(a) = b$. In this case, we have

$$f^{-1}(\varphi_2(b)) = f^{-1}(\varphi_2(f(a))) = f^{-1}(f(\varphi_1(a))) = \varphi_1(a) = \varphi_1(f^{-1}(b)).$$

So $f^{-1} \in \mathrm{Hom}((B,\varphi_2),(A,\varphi_1))$. Clearly $f^{-1} \circ f = \mathrm{Id}_A$ and $f \circ f^{-1} = \mathrm{Id}_B$, we conclude that f is an isomorphism. Conversely, if $f \in \mathrm{Hom}((A,\varphi_1),(B,\varphi_2))$ is an isomorphism, then it is an isomorphism under set, thus bijective. So the isomorphisms in G-Set are precisely the equivariant bijections. □

Exercise 9.9
Prove that G-set has products and coproducts and that every finite object of G-Set is a coproduct of objects of the type $G/H = \{\text{left-cosets of } H\}$, where H is a subgroup of G and G acts on G/H by left-multiplication.

Proof. For (A,p) and (B,q) in the category of G-set, we define the product $(A,p)\times(B,p)$ by $(A \times B, p \times q)$. For any $(C,u) \in G$-Set, we will prove that $(A \times B, p \times q)$ satisfy the universal property of product.



Let $f \in \mathrm{Hom}((A,p),(C,u))$ and $g \in \mathrm{Hom}((B,q),(C,u))$, then by the universal property of set product, there exists uniquely a $\varphi\colon A \times B \to C$. For any $a \in A$ and $b \in B$, we have

$$\varphi((p\times q)(a,b)) = \varphi(p(a),q(b)) = (\varphi(p(a)),\varphi(q(b))) = (p(\varphi(a)),q(\varphi(b))) = (p\times q)(\varphi(a\times b)).$$

So $\varphi \in \mathrm{Hom}((A \times B, p \times q), (C, u))$, which shows that $(A \times B, p \times q)$ is the product of (A, p) and (B, q).

Similarly, we can check that $(A \coprod B, p \coprod q)$ is the coproduct of (A, p) and (B, q). Here

$$p \coprod q(x) = \begin{cases} p(x) & \text{if } x \in A, \\ q(x) & \text{if } x \in B. \end{cases}$$

For the second part, let $(A, p) \in G$-Set. Let $A_1, \cdots, A_n$ be the partition of orbits of G acts on A. For $a_1 \in A_1$, let $H = \mathrm{Stab}(a_1)$, then Proposition 9.9 implies that (A_1, p) isomorphic to the left-multiplicaiton of G on G/H_1. Clearly

$$(A, P) = \coprod_{i=1}^{n} (A_i, p),$$

thus finish our proof. □

Exercise 9.10
Let H by any subgroup of a group G. Prove that there is a bijection between the set G/H of left-cosets of H and the set H/G of rigth-cosets of H in G.

Proof. Let $\sigma \colon G/H \to H/G$ that maps $gH \mapsto Hg^{-1}$. This map is well defined because if $gH = g'H$ then $gg'^{-1} \in H$. Thus $g^{-1}g' \in H$ so $Hg^{-1} = Hg$. For any right coset Hg of G, we have $\sigma(g^{-1}H) = H(g^{-1})^{-1} = Hg$, so σ is surjective. If $\sigma(gH) = \sigma(g'H)$ then $Hg^{-1} = Hg'^{-1}$ or $g^{-1}g' \in H$. Therefore $gH = g'H$, which prove that σ is injective. So σ is a bijection from the left cosets and the right cosets. □

Exercise 9.11
Let G be a finite group, and let H be a subgroup of index p, where p is the smallest prime dividing $|G|$. Prove that H is normal in G, as follows:

- Interpret the action of G on G/H by left-multiplicaition as a homomorphism $\sigma \colon G \to S_p$.
- Then $G/\ker\sigma$ is (isomorphic to) a subgroup of S_p. What does this say about the index of $\ker\sigma$ in G?
- Show that $\ker\sigma \subset H$.
- Conclude that $H = \ker\sigma$, by index considerations.

Thus H is a kernel, proving that it is normal.

Proof. Assume that H has index p, let $g_1H = H, g_2H, \cdots, g_pH$ be left cosets of H. For any $g \in G$, the left action of g on the cosets of H is a permutation of $\{g_1H, \cdots, g_pH\}$, thus can be viewed as an element of S_p. Let this action be $\sigma \colon G \to S_p$, (i.e. $\sigma(g)(g_iH) = (gg_i)H$), then for any $g, g' \in G$, we have

$$\sigma(gg')(g_iH) = gg'g_iH = g(g'g_iH) = g\sigma(g') = \sigma(g)\sigma(g').$$

So σ is indeed a group homomorphism. By the first isomorphism theorem, we get $G/\ker\sigma \cong \mathrm{Im}(\sigma)$, which is a subgroup of S_p. So

$$|G|/|\ker\sigma| \mid |S_p| = p!.$$

Since p is the smallest prime divisor of $|G|$, either $|G|/|\ker\sigma|$ equals 1 or p. The first case implies σ is the trivial homomorphism, thus H has one coset or $H = G$. This contradicts to the hypothesis that H has prime index. So $|G|/|\ker\sigma| = p$.

Notice that if $h \in H$, then $(hg_i)g_i^{-1} = h \in H$. Thus $hgH = gH$ or h stabilizes every cosets. This means $h \in \ker\sigma$ or $H \subset \ker\sigma$. If $H \neq \ker\sigma$, then

$$p = \frac{|G|}{\ker\sigma} < \frac{|G|}{|H|} = p,$$

contradiction. So $H = \ker\sigma$ or H is a normal subgroup. □

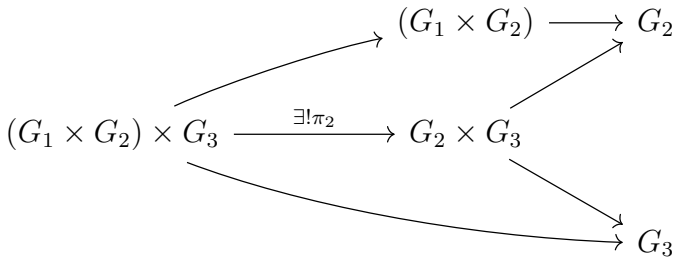
10. Group objects in categories

Exercise 10.1
Define all the unnamed maps appearing in the diagrams in the definition of group object, and prove they are indeed isomorphisms when so indicated.

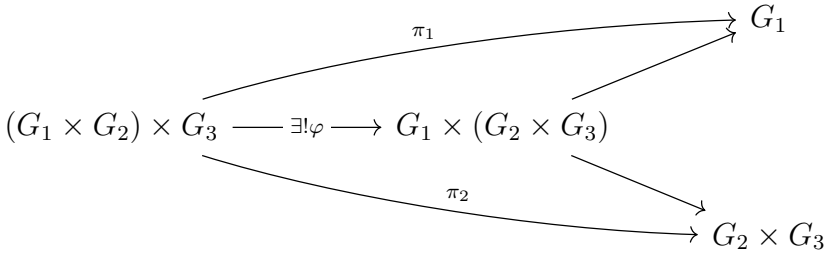
Proof. Let $G_1 \cong G_2 \cong G_3 \cong G$. For the first homomorphism from $(G_1 \times G_2) \times G_3$ to $G_1 \times (G_2 \times G_3)$, we first let π_1 be the projection from $(G_1 \times G_2) \times G_3$ to G_1 to be the composition of two projections as follow.

$$(G_1 \times G_2) \times G_3 \xrightarrow{\quad} (G_1 \times G_2) \xrightarrow{\pi_1} G_1$$

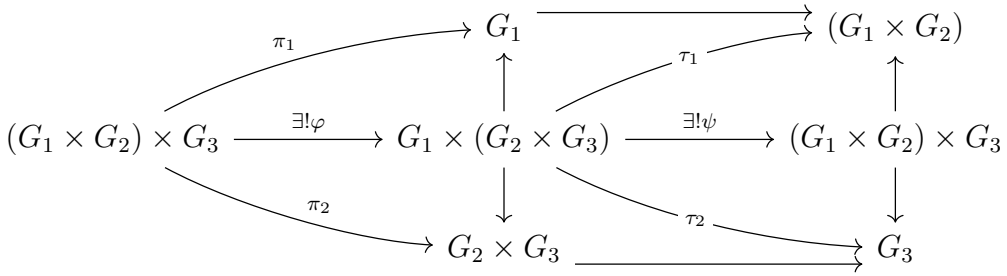
Next we define a homomorphism π_2 from $(G_1 \times G_2) \times G_3$ to $(G_2 \times G_3)$ using the universal property of $G_2 \times G_3$ such that the following diagram commutes.



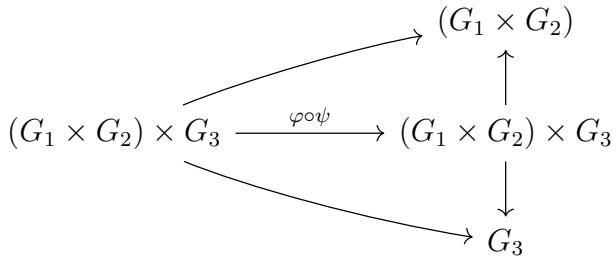
Using the universal property of $G_1 \times (G_2 \times G_3)$, we can define a homomorphism $\varphi\colon (G_1 \times G_2) \times G_3 \to G_1 \times (G_2 \times G_3)$ such that the following diagram commutes.



Using the same technique, we can construct a homomorphism $\psi\colon G_1 \times (G_2 \times G_3) \to (G_1 \times G_2) \times G_3$. We will prove that $\psi \circ \varphi\colon (G_1 \times G_2) \times G_3 \to (G_1 \times G_2) \times G_3$ is the identity homomorphism. Notice that in our process of defining ψ, τ_1 and τ_2 are maps that make the following diagram commutes.



By cleaning up some arrows and combine some obvious ones, we get the following commutative diagram that defines ψ.

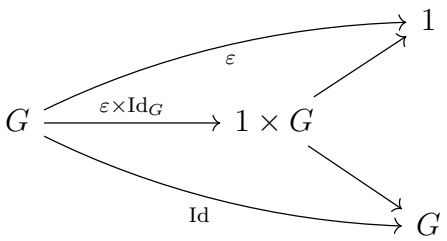


But all arrows beside $\varphi\circ\psi$ are natural projections, thus the universal property of product implies that $\varphi \circ \psi = \mathrm{Id}$. Similarly, we get $\psi \circ \varphi = \mathrm{Id}$, thus φ is an isomorphism.

For the homomorphism from $1 \times G \to G$, we only need to prove that the composition

$$G \xrightarrow{\varepsilon\times \mathrm{Id}_G} 1 \times G \longrightarrow G$$

is the identity. But this is clear by the construction of $\varepsilon \times \mathrm{Id}$, that is, the following diagram commutes.



□

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

Proof. Let G be a group as in §1.2, $m\colon G \times G \to G$ that maps $(g_1, g_2) \mapsto g_1 g_2$, $\varepsilon\colon 1 \to G$ maps $1 \mapsto e_g$, and $\iota\colon G \to G$ maps $g \mapsto g^{-1}$. We will check that these maps generate the following commutative diagrams. Because multiplication is associative, we get the following commutative diagram.

$$\begin{array}{ccccc} (G \times G) \times G & \xrightarrow{m \times \mathrm{Id}_G} & G \times G & \xrightarrow{m} & G \\ \downarrow{\scriptstyle \cong} & & & & \| \\ G \times (G \times G) & \xrightarrow{\mathrm{Id}_G \times m} & G \times G & \xrightarrow{m} & G \end{array}$$

Moreover, because e_g is the identity of G, we get the following commutative diagrams.

$$\begin{array}{ccc} 1 \times G & \xrightarrow{\varepsilon \times \mathrm{Id}_G} & G \times G \\ & \searrow^{\cong} & \downarrow{\scriptstyle m} \\ & & G \end{array} \qquad \begin{array}{ccc} G \times 1 & \xrightarrow{\mathrm{Id}_G \times \varepsilon} & G \times G \\ & \searrow^{\cong} & \downarrow{\scriptstyle m} \\ & & G \end{array}$$

Lastly, the inverse of G implies these commutative diagrams.

$$\begin{array}{ccccc} G & \xrightarrow{\Delta} & G \times G & \xrightarrow{\mathrm{Id}_G \times \iota} & G \times G \\ \downarrow & & & & \downarrow{\scriptstyle m} \\ 1 & & \xrightarrow[\varepsilon]{} & & G \end{array} \qquad \begin{array}{ccccc} G & \xrightarrow{\Delta} & G \times G & \xrightarrow{\iota \times \mathrm{Id}_G} & G \times G \\ \downarrow & & & & \downarrow{\scriptstyle m} \\ 1 & & \xrightarrow[\varepsilon]{} & & G \end{array}$$

So G is a group object in the category of sets. □

Exercise 10.3
Let $(G, \cdot)$ be a group, and suppose $\circ\colon G \times G \to G$ is a group homomorphism such that $(G, \circ)$ is also a group. Prove that $\circ$ and $\cdot$ coincide.

Proof. Because $\circ$ is a homomorphism, for any $g_i \in G$, we have

$$g_1 g_2 \circ g_3 g_4 = (g_1 \circ g_3)(g_2 \circ g_4). \tag{2}$$

Let $g_i = e$, then (2) becomes

$$e \circ e = (e \circ e)(e \circ e).$$

So $e \circ e = e$. But $(G, \circ)$ has group structure, thus the cancelation law implies that e is the identity element of $(G, \circ)$. For any $g_1, g_2 \in G$, by (2), we have

$$g_1 \circ g_2 = (g_1 \cdot e) \circ (e \cdot g_2) = (g_1 \circ e)(e \circ g_2) = g_1 g_2.$$

So $\circ$ and $\cdot$ coincide. □

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

Proof. A group object in the category Ab consists of an abelian group $G \in \mathrm{Obj}(\mathsf{Ab})$ and group homomorphisms $m\colon G \times G \to G$, $e\colon 1 \to G$, and $\iota\colon G \to G$. But by Exercise 10.3, m coincides with the mulitiplication on G. Thus for $g_1, g_2 \in G$, we have

$$m(g_1, g_2) = g_1 g_2 = g_2 g_1 = m(g_2, g_1).$$

So the group object in the category Ab is just the abelian group itself. □

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

Proof. Let $G \in \mathsf{Grp}$, $m\colon G \times G \to G$, $e\colon 1 \to G$ and $\iota\colon G \to G$ be a group object in the category of Grp. Since m is a group homomorphism, Exericse 10.3 implies that m is just the multiplication in G. It is not hard to see that e is also a group homomorphism (that maps $1 \mapsto e_G$). But ι being a group homomorphism means for any $g_1, g_2 \in G$, we have

$$g_1 g_2 = (g_2^{-1} g_1^{-1})^{-1} = \iota(g_2^{-1} g_1^{-1}) = \iota(g_2^{-1})\iota(g_1^{-1}) = g_2 g_1.$$

So this groups is abelian. And when G is non abelian, there is no group object for G. □

Chapter III. Rings and modules

1. Definition of ring

Exercise 1.1
Prove that if $0 = 1$ in a ring R, then R is a zero-ring.

Proof. Let R be a ring and $r \in R$, then we have

$$r = r \cdot 1 = r \cdot 0 = 0.$$

So R has one element, which is 0. □

Exercise 1.2
Let S be a set, and define operations on the power set $\mathscr{P}(S)$ of S be setting $\forall A, B \in \mathscr{P}(S)$

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

Prove that $(\mathscr{P}(S), +, \cdot)$ is a commutative ring.

Proof. Let $0 := \varnothing$ and $1 := S$. For $A, B, C \in \mathscr{P}(S)$, using set arguments, we can get

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

Moreover

$$A + B = (A \cup B) \setminus (A \cap B) = (B \cup A) \setminus (B \cap A) = B + A$$

and

$$A + \varnothing A \cup \varnothing \setminus A \cap \varnothing = A \setminus \varnothing = A.$$

So $\varnothing$ is the zero element. Lastly,

$$A + A = A \cup A \setminus A \cap A = A \setminus A = \varnothing = 0.$$

So $\mathscr{P}(S)$ is indeed an abelian group with addition.

What is more,

$$A \cdot (B \cdot C) = A \cap (B \cap C) = (A \cap B) \cap C = (A \cdot B) \cdot C,$$

and

$$A \cdot B = A \cap B = B \cap A = B \cdot A.$$

Moreover,

$$A \cdot 1 = S \cap A = A,$$

so S is the one element of $\mathscr{P}(S)$. Finally,

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

So with these operations, $\mathscr{P}(S)$ is a commutative ring.

□

Exercise 1.3
Let R be a ring, and let S be any set. Explain how to endow the set R^S of set-functions $S \to R$ of two operations $+, \cdot$ so as to make R^S into a ring, such that R^S is just a copy of R if S is a singleton.

Proof. Let $f, g, h \colon S \to R$. We define addition and multiplication on R^S by $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x) \cdot g(x)$ for any $x \in S$. Because addition is associative in R, it is not hard to see that $f + (g + h) = (f + g) + h$. Moreover, $(f + g)(x) = f(x) + g(x) = g(x) + f(x) = (g + f)(x)$ thus addition is commutative. The zero function $0(x) = 0$ is the identity function because $(0 + f)(x) = 0(x) + f(x) = 0 + f(x) = f(x)$. Lastly, for any $f \colon S \to R$, we have $(-f)(x) = -f(x)$ since $(f + (-f))(x) = f(x) + (-f)(x) = f(x) - f(x) = 0 = 0(x)$. So $(R^S, +)$ is a commutative group. Clearly $f \cdot (g \cdot h)(x) = f(x) \cdot (g(x) \cdot h(x)) = (f(x) \cdot g(x)) \cdot h(x) = (f \cdot g) \cdot h(x)$. So multiplication is associative in R^S. What is more,

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

Similarly we get $f \cdot (g + h) = f \cdot g + f \cdot h$. Let $1(x) = 1$ for all $x \in S$, then $f \cdot 1(x) = f(x) \cdot 1(x) = f(x)$ and similarly $1 \cdot f = f$. So $(R^S, +, \cdot)$ is a ring.

If S is a singleton, then a function from S to R is determined by its image, that is an element of R. We can easily check that the multiplication and addition of these functions in this case is identical to these of R. So R^S is just a copy of R in this case. □

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

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

Proof.
- Assume that $a^n = b^m = 0$, then we will show that $(a+b)^{m+n} = 0$. Indeed, any term of the expansion has $m+n$ terms of either a or b. By the pigeonhole principle, there are at least m terms a or n terms b. In either case, its product is 0 since a and b are commute. So $(a+b)^{m+n} = 0$ or $a+b$ is nilpotent.
- Yes it is. For a counter example, let $A = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, and $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ in the ring $M_2(\mathbb{R})$. It is not hard to see that A and B are nilpotent because $A^2 = B^2 = 0$. But $A+B$ is not because $(A+B)^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$. That is, for any $n \in \mathbb{N}$, $(A+B)^{2n} \neq 0$ thus $(A+B)^n \neq 0$.

□

Exercise 1.7
Prove that $[m]$ is nilpotent in $\mathbb{Z}/n\mathbb{Z}$ if and only if m is divisible by all prime factors of n.

Proof. Let $n = p_1^{t_1} \cdots p_k^{t_k}$ be the factorization for n. If p_i divides m for each i from 1 to k, then

$$m^{\max\{t_i : 1 \leq i \leq k\}} = 0$$

in $\mathbb{Z}/n\mathbb{Z}$. So m is nilpotent. Conversely, if m is nilpotent, then there is some t such that $n | m^t$. For any i from 1 to n, because $p_i | m^t$, we deduce that $p_i | m$. So m is divisible by all prime factors of n. □

Exercise 1.8
Prove that $x = \pm 1$ are the only solutions to the equation $x^2 = 1$ in an intergral domain. Find a ring in which the equation $x^2 = 1$ has more than 2 solutions.

Proof. If $x^{=}1$ then $x^2 - 1 = 0$ or $(x-1)(x+1) = 0$. Since this is an integral domain, either $x - 1 = 0$ or $x + 1 = 0$, which is synonymous with $x = 1$ or $x = -1$.

This is not the case however for general ring. For example in $\mathbb{Z}/8\mathbb{Z}$, we have $[1]^2 = [3]^2 = [7]^2 = 1$. So $x^2 = 1$ has more than 2 solutions in $\mathbb{Z}/8\mathbb{Z}$. □

Exercise 1.9
Prove Proposition 1.12. That is to check that

- the inverse of a two-sided unit is unique;
- two-sided units form a group under multiplication.

Proof. • Let v_1 and v_2 be two-side units of $u \in R$, then we have

$$v_1 = v_1 \cdot 1 = v_1 \cdot u \cdot v_2 = 1 \cdot v_2 = v_2.$$

So the two-sided unit of u is unique.

- Let R be a ring and $U(R)$ be the set of units of R. Then $1 \in U(R)$, thus this group is nonempty. If $u, v \in U(R)$, then let $u', v' \in R$ be the inverse of u and v. So $(uv)(v'u') = 1$ and $(v'u')(uv) = 1$. So uv has $v'u'$ as its inverse, thus $uv \in U(R)$. Moreover, clearly v is the inverse of v', thus $v' \in U(R)$. In the end, $U(R)$ is a subgroup under multiplication.

□

Exercise 1.16
Let R be a ring, and consider the ring of power series $R[[x]]$.

- Prove that a power series $a_0 + a_1x + a_2x^2 + \cdots$ 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 $R[[x]]$?
- Prove that $R[[x]]$ is an integral domain if any only if R is.

Proof. • Evidently the polynomial 1 is the one element of this ring $R[[x]]$. Let $a(x) = a_0 + a_1x + \cdots$ be an invertible element of $R[[x]]$, then there exists $a'(x) = a'_0 + a'_1x + \cdots$ such that $a(x) \cdot a'(x) = 1$. But the constant coefficient of this product is $a_0a'_0$, thus $a_0a'_0 = 1$ and similarly $a'_0a_0 = 1$. So a_0 is a unit in R.

Conversely, if a_0 is a unit in R, we can multiply $a(x)$ to a'_0. Because a'_0 is invertible, thus if $a(x) \cdot a'_0$ invertible, then so is $a(x)$. This new polynomial has the form $1 + x \cdot q(x)$ for some $q(x) \in R[[x]]$. And it is invertible by the formula

$$\frac{1}{1 + xq(x)} = 1 - xq(x) + x^2q^2(x) - x^3q^3(x) + \cdots \in R[[x]].$$

So $a(x)$ is invertible if a_0 is invertible. Specifically,

$$(1 - x)^{-1} = 1 + x + x^2 + \cdots.$$

- Assume that R is an integral domain. Let $a(x)$ and $b(x)$ in $R[[x]]$ such that $a(x)b(x) = 0$. Because $\mathbb{N}$ is well-ordered, there are the smallest nonzero coefficients of $a(x)$ and $b(x)$, say a_k and b_h. Then the $k + h$ degree term in $a(x)b(x)$ is $a_kb_hx^{k+h}$. Since $a(x)b(x) = 0$, we get $a_kb_h = 0$. But both of them are nonzero, which contradicts to the hypothesis that R is an integral domain. So $R[[x]]$ is an integral domain.

  The converse is obvious because we can embed R into $R[[x]]$.

□

Exercise 1.17
Explain in what sense $R[x]$ agrees with the monoid ring $R[\mathbb{N}]$.

Proof. We know that $1, x, x^2, \cdots$ span $R[X]$ (whatever span means). Let $f\colon R[x] \to R[\mathbb{N}]$ maps $x^n \mapsto n$, then this give rise to a ring isomorphism from $R[x]$ to $R[\mathbb{N}]$. I guess we don't need no proof, cause the exercise asks for an explanation that's all. □

2. The category Ring

Exercise 2.1
Prove that if there is a homomorphism from a zero-ring to a ring R, then R is a zero-ring.

Proof. Recall that a homomorphism maps 0 to 0 and 1 to 1, and $0 = 1$ in the zero ring. For a ring R such that there exists a ring homomorphism $f\colon 0 \to R$, we have

$$0_R = f(0) = f(1) = 1_R.$$

Thus R is the zero ring. □

Exercise 2.2
Let R and S be rings, and let $\varphi\colon R \to S$ be a function preserving both operations $+, \cdot$.

- Prove that if φ is surjective, then necessarily $\varphi(1_R) = 1_S$.
- Prove that if $\varphi \neq 0$ and S is an integral domain, then $\varphi(1_R) = 1_S$.

Proof.
- Because φ is surjective, we can assume that $\varphi(r) = 1$ and $\varphi(1) = s$ for some r and s in R and S respectively. Then

  $$1 = \varphi(r) = \varphi(r \cdot 1) = \varphi(r) \cdot \varphi(1) = 1 \cdot s = s.$$

  Thus $\varphi(1) = s = 1$.

- Let $\varphi(1) = s$. If $s = 0$ then $\varphi = 0$. Conversely, if $s \neq 0$, then we have

  $$0 = \varphi(1) - \varphi(1 \cdot 1) = \varphi(1) - \varphi(1)^2 = s - s^2 = s(1 - s).$$

  But S is an integral domain, thus $1 - s = 0$ or $s = 1$. So $\varphi(1) = 1$.

□

Exercise 2.3
Let S be a set, and consider the power set ring $\mathscr{P}(S)$ and the ring $(\mathbb{Z}/2\mathbb{Z})^S$ you constructed in Exercise 1.3. Prove that these two rings are isomorphic.

Proof. Let $\varphi\colon \mathscr{P}(S) \to (\mathbb{Z}/2\mathbb{Z})^S$ that map $A \mapsto \varphi(A)$ such that $\pi_i \circ \varphi(A) = \begin{cases} 1, & i \in A, \\ 0, & i \notin A. \end{cases}$ Notice that this is enough to define an element of $(\mathbb{Z}/2\mathbb{Z})^S$ by the universal property of the product of rings. Let $\psi\colon (\mathbb{Z}/2\mathbb{Z})^S \to \mathscr{P}(S)$ that maps $(s_i)_{i\in S} \mapsto \{i \in S : s_i = 1\}$. We first check that these are ring isomorphisms and after that $\varphi \circ \psi = 1$ and $\psi \circ \varphi = 1$.

The 1 element in $\mathscr{P}(S)$ is S, and $\varphi(S) = (1, \cdots, 1)$, which is the identity of $(\mathbb{Z}/2\mathbb{Z})^S$. What is more, for $A, B \subset S$, we have

$$\varphi(A + B) = \varphi((A \cup B) \setminus (A \cap B)) = (u_i)$$

such that $u_i = 1$ iff $i \in (A \cup B) \setminus (A \cap B)$. Moreover, let

$$\varphi(A) + \varphi(B) = (r_i) + (s_i) = (t_i),$$

then $t_i = 0$ iff both $r_i = s_i = 1$ or both $r_i = s_i = 0$. The first case is when $i \in A \cap B$ and the second is when $i \notin A \cup B$. Thus $t_i = 1$ iff $i \in (A \cup B) \setminus (A \cap B)$, or equivalently $t_i = u_i$, which yields $\varphi(A+B) = \varphi(A)+\varphi(B)$. Similarly, we can check that $\varphi(A \cap B) = \varphi(A) \cdot \varphi(B)$ (it is not at all similar but I get lazy eventually). With a similar technique, one can check that ψ is also a ring homomorphism.

One can easily check from the definition of φ and ψ that $\varphi \circ \psi$ and $\psi \circ \varphi$ are the identity maps. Thus φ is indeed an isomorphism. □

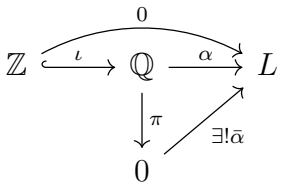
Exercise 2.8
Prove that every subring of a field is an integral domain.

Proof. Assume that R is a subring of a field F. Then obviously R is a ring. Assume that $r, s \in R$, $r \cdot s = 0$, and $r \neq 0$, then because a field is an integral domain, we get $s = 0$. So R is an integral domain. □

Exercise 2.12
Consider the inclusion map $\iota\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$. Describe the cokernel of ι in Ab and its cokernel in Ring.

Proof. From §8.6, we know that $\operatorname{coker}\varphi = \mathbb{Q}/\operatorname{Im}(\iota) = \mathbb{Q}/\mathbb{Z}$. Let $\sim$ be a relation on $\mathbb{Q}$ such that $q \sim p$ if and only if $q - p \in \mathbb{Z}$. So so we can view $\mathbb{Q}/\mathbb{Z} = \{\bar{q} \in \mathbb{Q} : 0 \leq q < 1\}$, which is the $\operatorname{coker}\iota$ in Ab.

Let $\pi\colon \mathbb{Q} \to 0$ be the zero map, and α and L are ring homomorphism and ring respectively such that $\alpha \circ \iota = 0$. We will show that there exists uniquely an $\bar{\alpha}$ such that the following diagram commutes.



Because ι is an epimorphism, and $\alpha \circ \iota = 0 \circ \iota = 0$, we get $\alpha = 0$. But α is a ring homomorphism, thus it maps $1 \mapsto 1_L = 0$. So $L = 0$. And because $\bar{\alpha}\colon 0 \to 0$, it exists and is unique. So 0 satisfy the universal property of a cokernel in the category of Ring. □

Exercise 2.13
Verify that the componentwise product $R_1 \times R_2$ of two rings satisfies the universal property for products in a category, given in §I.5.4.

Proof. Let $\pi_i\colon R_1 \times R_2 \to R_i$ be the group product projections. We will check that these are ring homomorphisms. Clearly $\pi_1(1,1) = 1$ and for any $(r_i, s_i) \in R_1 \times R_2$, we have

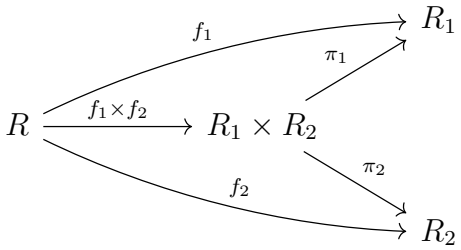
$$\pi_1((r_1,s_1) + (r_2,s_2)) = \pi_1(r_1 + r_2, s_1 + s_2) = r_1 + r_2 = \pi_1(r_1,s_1) + \pi_1(r_2,s_2).$$

Moreover,

$$\pi_1((r_1,s_1) \cdot (r_2,s_2)) = \pi_1(r_1 \cdot r_2, s_1 \cdot s_2) = r_1 \cdot r_2 = \pi_1(r_1,s_1) \cdot \pi_1(r_2,s_2).$$

So π_1 is a ring homomorphism, and so is π_2 for similar reason.

Now we prove that $R_1 \times R_2$ satisfies the universal property of product in the category of Rings. Let R be a ring, $f_i\colon R \to R_i$ are ring homomorphisms. By the underling group structure, there exists uniquely an $f_1 \times f_2$ such that the following diagram is commute in Gr.



So if such $f_1 \times f_2$ exists in Ring such that the diagram above commutes, it is unique. It is sufficient now to check that $f_1 \times f_2$ is a ring homomorphism. Indeed, because f_1, f_2 are ring homomorphisms, we get

$$(f_1 \times f_2)(1) = (f_1(1), f_2(1)) = (1, 1).$$

For any $r_1, r_2 \in R$, we get

$$\begin{aligned}(f_1 \times f_2)(r_1 + r_2) &= (f_1(r_1 + r_2), f_2(r_1 + r_2)) \\ &= (f_1(r_1) + f_1(r_2), f_2(r_1) + f_2(r_2)) \\ &= (f_1(r_1), f_2(r_1)) + (f_1(r_2), f_2(r_2)) \\ &= (f_1 \times f_2)(r_1) + (f_1 \times f_2)(r_2),\end{aligned}$$

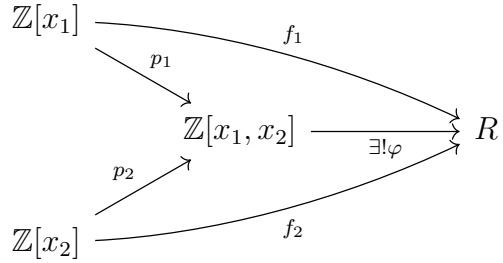
and

$$\begin{aligned}(f_1 \times f_2)(r_1 \cdot r_2) &= (f_1(r_1 \cdot r_2), f_2(r_1 \cdot r_2)) \\ &= (f_1(r_1) \cdot f_1(r_2), f_2(r_1) \cdot f_2(r_2)) \\ &= (f_1(r_1), f_2(r_1)) \cdot (f_1(r_2), f_2(r_2)) \\ &= (f_1 \times f_2)(r_1) \cdot (f_1 \times f_2)(r_2).\end{aligned}$$

So with this ring structure, $R_1 \times R_2$ is a product in the category of Ring. □

Exercise 2.14
Verify that $\mathbb{Z}[x_1, x_2]$ (along with the evident morphisms) satisfies the universal property for the coproduct of two copies of $\mathbb{Z}[x]$ in the category of commutative rings. Explain why it does not satisfy it in Ring.

Proof. Let $p_i \colon \mathbb{Z}[x_i] \to \mathbb{Z}[x_1, x_2]$ maps $x_i \mapsto x_i$. This is enough to define p_i due to its universal property. Now let f_1 and f_2 be ring homomorphisms from $\mathbb{Z}[x_1]$ and $\mathbb{Z}[x_2]$ to R repsectively, we prove that there exists uniquely a φ such that the following diagram commutes.



Notice that in oder for this diagram to commute, we have $\varphi(x_i) = \varphi \circ p_i(x_i) = f_i(x_i)$. And again by the universal property of polynomial rings, φ is uniquely defined. Let φ be defined such that $\varphi(x_i) = f_i(x_i)$, we will show that this diagram is actually commutes. Indeed, for any polynomial $a0 + a_1x_1 + \cdots + a_nx_1^n \in \mathbb{Z}[x_1]$, we have

$$\begin{aligned}
\varphi \circ p_1(a_0 + a_1x_1 + \cdots + a_nx_1^n) &= \varphi(a_0 + a_1x_1 + \cdots + a_nx_1^n) \\
&= a_0 + a_1\varphi(x_1) + \cdots + a_n\varphi(x_1)^n \\
&= a_0 + a_1f_1(x_1) + \cdots + a_nf_1(x_1)^n \\
&= f_1(a_0 + a_1x_1 + \cdots + a_nx_1^n).
\end{aligned}$$

So $\varphi \circ p_1 = f_1$, and similarly $phi \circ p_2 = f_2$. So this in indeed a coproduct. Notice that this is not true in Ring in general because without the commutativity, φ is not a ring homomorphism. □

Exercise 2.15
For $m > 1$, the abelian groups $(\mathbb{Z}, +)$ and $(m\mathbb{Z}, +)$ are anifestly isomorphic: the function $\varphi\colon \mathbb{Z} \to m\mathbb{Z}$, $n \mapsto mn$ 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 explicite formula for the "multiplication" $\bullet$ this defines on $\mathbb{Z}$ (that is, such that $\varphi(a \bullet b) = \varphi(a) \cdot \varphi(b)$). Explain why structures induced by different positive integers m are nonisomorphic as 'rings without 1'.

Proof. Let $a \bullet b = m \cdot a \cdot b$ for $a, b \in \mathbb{Z}$. Then

$$\varphi(a \bullet b) = \varphi(m \cdot a \cdot b) = m^2 \cdot a \cdot b = (ma)(mb) = \varphi(a) \cdot \varphi(b).$$

Notice that φ is a group isomorphism and preserve multiplication. Therefore it is a ring homomorphism from $(\mathbb{Z}, +, \bullet) \to (m\mathbb{Z}, +, \cdot)$. Similarly, one can check that $\psi\colon (m\mathbb{Z}, +, \cdot) \to (\mathbb{Z}, +, \bullet)$ that maps $mz \mapsto z$ is a ring homomorphism, and $\varphi \circ \psi = 1$, and so is $\psi \circ \varphi$. So $(\mathbb{Z}, +, \bullet) \cong (m\mathbb{Z}, +, \cdot)$.

For the next part, we show that for $n \neq m$, the rings $(m\mathbb{Z}, +, \cdot)$ is not isomorphic to $(n\mathbb{Z}, +, \cdot)$. Assume the converse, that there exists an isomorphism from $(m\mathbb{Z}, +, \cdot)$ to $(n\mathbb{Z}, +, \cdot)$. Then we have

$$m\varphi(m) = \varphi(m \cdot m) = \varphi(m)\varphi(m),$$

where the first equality is $\varphi(m) + \varphi(m) + \cdots + \varphi(m)$ m times. And the second equality is the multiplication of m's. Notice that $\varphi(m) \neq 0$ (or else this is the zero function) and that $n\mathbb{Z}$ is an integral domain, we conclude that $\varphi(m) = m$. Similarly, we get $\varphi(n) = n$. Without loss of generality, assume that $n > m$, then there is no m in $n\mathbb{Z}$, which contradict to the fact that $\varphi(m) = m$. □

Exercise 2.16
Prove that there is (up to isomorphism) only one structure of ring with identity on the abelian group $(\mathbb{Z}, +)$.

Proof. Let $(Z, +, \bullet)$ be a ring structure with identity, and assume n be the identity. Then

$$1 = 1 \bullet n = 1 \bullet (1 + 1 + \cdots + 1) = 1 \bullet 1 + \cdot + 1 \bullet 1,$$

where these are addition of n terms. But this means $1 \bullet 1 = \frac{1}{n}$. Therefore $n = 1$ and we get the unique normal ring structure. □

3. Ideals and quotient rings

Exercise 3.1
Prove that the image of the ring homomorphism $\varphi\colon R \to S$ 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?

Proof. We can decompose φ into the following diagram.

$$R \xrightarrow{\quad\varphi\quad} \xrightarrow{\quad} R/\ker\varphi \xrightarrow{\ \sim\ } \operatorname{Im}\varphi \hookrightarrow S$$

Since $\mathbb{R}/\ker\varphi$ is a ring, so is $\operatorname{Im}\varphi$. So $\operatorname{Im}\varphi$ is a subring of S. If $\operatorname{Im}\varphi$ is an ideal, then it equals S since it contains 1. Therefore, if $\ker\varphi$ is a subring of R, then $\ker\varphi = R$ or φ is the zero homomorphism. □

Exercise 3.2
Let $\varphi\colon R \to S$ be a ring homomorphism, and let J be an ideal of S. Prove that $I = \varphi^{-1}(J)$ is an ideal of R.

Proof. If J is an ideal of S then there is a function $\psi\colon S \to S/J$. Then $\psi \circ \varphi\colon R \to S/J$ is a ring homomorphism with its kernel being $\varphi^{-1}(J)$. Therefore $\varphi^{-1}(J)$ is an ideal of R.

$$R \xrightarrow{\ \varphi\ } S \xrightarrow{\ \psi\ } S/J \qquad (\psi\circ\varphi)$$

□

Exercise 3.3
Let $\varphi\colon R \to S$ 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 $\bar{J} = \varphi(J)$, an ideal of R/I be the previous point. Prove that

$$\frac{R/I}{\bar{J}} \cong \frac{R}{I+J}.$$

Proof.

- Let $\varphi\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$ be the inclusion ring homomorphism. Clearly $\mathbb{Z}$ is an ideal of $\mathbb{Z}$, but $\varphi(\mathbb{Z}) = \mathbb{Z}$ is not an ideal of $\mathbb{Q}$ because it is strictly smaller than $\mathbb{Q}$ and it has the identity element 1 in it.
- Because φ is surjective, any element of S has the form $\varphi(r)$ for some $r \in R$. For any $\varphi(j) \in \varphi(J)$, we have

$$\varphi(r)^{-1}\varphi(j)\varphi(r) = \varphi(r^{-1}jr) \in \varphi(J).$$

So $\varphi(J)$ is an ideal of S.

- Let φ and ψ be ring homomorphisms as the following diagram.

$$R \xrightarrow{\varphi} R/I \xrightarrow{\psi} \frac{R/I}{J}, \qquad R \xrightarrow[\psi\circ\varphi]{} \frac{R/I}{J}$$

  It is sufficient to show that $I + J$ is the kernel of $\psi \circ \varphi$. Because $I \in \ker \varphi$, thus $\psi \circ \varphi(I) = \psi(0) = 0$. Moreover notice that $\varphi(J) \in \ker \psi$, thus $\psi \circ \varphi(J) = 0$. So $I + J \subset \ker(\psi \circ \varphi)$. Conversely, if $x \in \ker(\psi \circ \varphi)$, then $\varphi(x) \in \varphi(J)$ or equivalently $x \in I + J$. So $I + J = \ker(\psi \circ \varphi)$, which complete our proof.

□

Exercise 3.4
Let R be a ring such that every subgroup of $(R, +)$ is in fact an ideal of R. Prove that $R \cong \mathbb{Z}/n\mathbb{Z}$, where n is the characteristic of R.

Proof. Let $f\colon \mathbb{Z} \to R$ be the unique ring homomorphism. Notice that f is a group homomorphism with addition, thus $f(\mathbb{Z})$ is a subgroup of $(R, +)$. Using the hypothesis of every subgroup of $(R, +)$ being ideal of R, we get $f(\mathbb{Z})$ to be an ideal of R that contains 1. Thus $R \cong f(\mathbb{Z}) \cong \mathbb{Z}/\ker f \cong \mathbb{Z}/n\mathbb{Z}$ where n is the characteristic of R. □

Exercise 3.7
Let R be a ring, and let $a \in R$. Prove that Ra is a left-ideal of R and aR is a right-ideal of R. Prove that a is left-, resp. right-, unit if and only if $R = aR$, resp. $R = Ra$.

Proof. Any element of Ra has the form r_0a for some $r_0 \in R$. For any $r \in R$, we have $r(r_0a) = (rr_0)a \in Ra$. So it is sufficient to check that Ra is a group under addition. Indeed, for $r_1a, r_2a \in R$, we have

$$r_1a - r_2a = (r_1 - r_2)a \in Ra.$$

So Ra is a left ideal of R. If a is a right unit, then there is $r_0 \in R$ such that $r_0a = 1$. So for any $r \in R$, we have $r = r \cdot 1 = r(r_0a) = (rr_0)a \in Ra$. So $R \subset Ra$ or $R = Ra$. Conversely, assume that $Ra = R$, then obviously there exists some $r_0 \in R$ such that $r_0a = 1$. So a is a right unit. The proof for left unit and right ideal is done similarly. □

Exercise 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.

Proof. If R is a division ring, then any nonzero element is a unit. Thus there are two right ideals, which are $0R$ and $aR = R$ for any $a \neq 0$. Similarly, there are only two left ideals which are $\{0\}$ and R. Conversely, if $\{0\}$ and R are the only right ideals there are, then for any nonzero element $r \in R$, we have $rR \neq \{0\}$ thus $rR = R$. By Exercise 3.7, we claim that r is a left unit. Similarly, we get r to be a right, thus a two sided unit. If R is also commutative, we get a field obviously. □

Exercise 3.10
Let $\varphi\colon K \to R$ be a ring homomorphism, where K is a field and R is a nonzero ring. Prove that φ is injective.

Proof. For any nonzero $k \in K$, if $\varphi(k) = 0$ then

$$1_R = \varphi(1) = \varphi(k \cdot k^{-1}) = \varphi(k) \cdot \varphi(k)^{-1} = 0 \cdot 0 = 0.$$

This contradicts to the hypothesis of R being nonzero ring. So $\ker \varphi = 0$ or φ is injective. □

Exercise 3.12
Let R be a commutative ring. Prove that the set of nilpotent elements of R is an ideal of R.

Find a noncommutative ring in which the set of nilpotent elements is not an ideal.

Proof. Let $I = \{r \in R : r^n = 0 \text{ for some } n \in \mathbb{N}\}$ be the set of nilpotent elements of R. For any $r \in R$, and $x \in I$ such that $x^n = 0$, we show that rx is nilpotent. Indeed, we have

$$(rx)^n = r^n x^n = r^n \cdot 0 = 0.$$

So it is sufficient to show that I is a group under addition. For any $x, y \in I$, and $x^n = y^m = 0$, because R is commutative, we can see that $(x - y)^{m+n} = 0$. Thus I is a group under addition and therefore an ideal of R.

One can check that the set of nilpotent elements of $M_2(\mathbb{R})$ is not even a group under addition. Let $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, and $B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Then $A^2 = B^2 = 0$ but $A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is not nilpotent. So when R is noncommutative, nothing can we say. □

Exercise 3.13
Let R be a commutative ring, and let N be its nilradical. Prove that R/N contains no nonzero nilpotent elements.

Proof. Let $\varphi\colon R \to R/N$ be the For any element $\varphi(r)$ the is nilpotent in R/N there exists some $n \in \mathbb{N}$ such that $\varphi(r^n) = \varphi(r)^n = 0$. Thus $r^n \in N$. So there is some $m \in \mathbb{N}$ such that $r^{nm} = 0$ or $r \in N$. So $\varphi(r) = 0$ or there is no nonzero nilpotent elements. □

Exercise 3.14
Prove that the characteristic of an integral domain is either 0 or a prime integer. Do you know any ring of characteristic 1?

Proof. Let R be an integral domain. If the characteristic of R is neither a prime or infinity, then it equals $n \cdot m$ for $n, m > 1$. But this implies

$$(m1_R) \cdot (n1_R) = mn1_R = 0.$$

Since R is an integral domain thus either $m1_R$ or $n1_R$ is 0. But this is impossible since m and n is strictly less then mn, the order of 1_R, contradiction. □

Exercise 3.15
A ring R is Boolean if $a^2 = a$ for all $a \in R$. Prove that $\mathscr{P}(S)$ is Boolean, for ever set S. Prove that every Boolean ring is commutative, and has characteristic 2. Prove that if an integral domain R is Boolean, then $R \cong \mathbb{Z}/2\mathbb{Z}$.

Proof. For any $A \subset S$, we have $A \cdot A = A \cap A = A$. So R is Boolean. Assume R is a Boolean ring, then for any $r, s \in R$, we have $-r = (-r)^2 = r^2 = r$. Moreover,

$$r + s = (r + s)^2 = r^2 + rs + sr + s^2 = r + rs + sr + s = r + s + rs - sr.$$

Subtract both sides for $r + s$, we get $rs = sr$, or R is commutative. Also by the previous remark, $1_R = -1_R$. Thus R has characteristic 2. Assume moreover that R is an integral domain, then for any $r \in R$, we have $r^2 = r$ or $r(r - 1) = 0$. This implies that $r = 0$ or $r = 1$. So R has two elements 0 and 1. One can check with ease that $R \cong \mathbb{Z}/2\mathbb{Z}$ in this case. □

Exercise 3.16
Let S be a set and $T \subset S$ a subset. Prove that the subsets of S contained in T form an ideal of the power set ring $\mathscr{P}(S)$. Prove that if S is finite, then every ideal of $\mathscr{P}(S)$ is of this form. For S infinite, find an ideal of $\mathscr{P}(S)$ that is not of this form.

Proof. Let $I = \{U \subset T\}$, we will prove that I is an ideal of the power ring $\mathscr{P}(S)$. For $U_1, U_2 \in I$, we have $U_1 - U_2 = U_1 + U_2 \subset U_1 \cup U_2 \subset T$. So I is a group under addition. For any subset K of S and $U \in I$, we have $K \cdot U = K \cap U \subset U \subset T$. So I is indeed an ideal of $\mathscr{P}(S)$.

If S is finite and I is an ideal of $\mathscr{P}(S)$, we first prove that if $A, B \in I$, then so is $A \cup B$. Indeed, because I is an ideal, we have

$$A \setminus B = A \cap B^c = A \cdot B^c \in I.$$

Mover, because I is a group under addition, we get

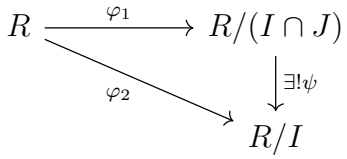
$$A \cup B = A + (A \setminus B) \in I.$$

With a simple induction, we can deduce that $V = \bigcup_{U \in I} U \in I$. So the ideal I consists of subsets of V. Moreover, because $V \in I$, $\mathscr{P}(S) \cdot V$ the set of all subsets of V is also in I. So I is the set of all subsets of V.

For the counterexample part, set $S = \mathbb{N}$ and $I = \{U \subset S : |U| < \infty\}$ is the set of finite subsets of S. If $A, B \in I$ then $|A + B| \leq |A| + |B| < \infty$ and $|-A| = |A| < \infty$. So I is a group under addition. Moreover, for any $U \subset S$ and $A \in I$, we have $|U \cdot A| = |U \cap A| \leq |A| < \infty$. So I is an ideal of $\mathscr{P}(\mathbb{N})$. But for any $T \subset \mathbb{N}$, if $T = \mathbb{N}$ then clearly $\mathbb{N}$ is a subset of T, but $\mathbb{N} \notin I$. If T is strictly smaller than $\mathbb{N}$, then we can choose $n \notin T$. Clearly $\{n\} \in I$ because it is a subgroup of order 1. So I is an ideal not of the form of subsets of T. □

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

Proof. Let φ_1 and φ_2 be quotient maps from R to $R/(I \cap J)$ and to R/I respectively. Because $I \cap J \in I$, using the universal property of quotient space, there exists uniquely a ring homomorphism ψ such that the following diagram commutes.



Consider the ideal $I+J$ of R, we have $\varphi_2(I+J) = (I+J)/I$ and $\varphi_1(J) = J/(I \cap J)$. We will show that $\psi\colon \varphi_1(J) \to \varphi_2(I+J)$ is an isomorphism (no relabeling is required). This is well defined because any element of $\varphi_1(J)$ has the form $\varphi_1(j)$ for some $j \in J \subset I+J$. So $\psi \circ \varphi_1(j) \in \psi \circ \varphi_1(I+J) = \varphi_2(I+J)$. If $v \in \ker \psi$, then there is some $j \in J$ such that $\varphi_1(j) = v$.

$$\varphi_2(j) = \psi \circ \varphi_1(j) = \psi(v) = 0.$$

So $j \in I$ or $j \in I \cap J$. But this implies that $v = \varphi_1(j) = 0$. So ψ is injective. Moreover, ψ is surjective because φ_2 is surjective. Indeed, any element of R/I has the form $\varphi_2(r)$ for some $r \in R$. But

$$\varphi_2(r) = \psi(\varphi_1(r)).$$

So ψ is surjective. This ψ is a ring isomorphism or $(I+J)/I$ is isomorphic to $J/(I \cap J)$. □

4. Ideals and quotients: Remarks and examples

Exercise 4.1
Let R be a ring, and let $\{I_a\}_{a \in A}$ be a family of ideals of R. We let

$$\sum_{a \in A} I_a := \left\{ \sum_{a \in A} r_a \text{ such that } r_a \in I_a \text{ and } r_a = 0 \text{ for all but finitely many } a \right\}.$$

Prove that $\sum_a I_a$ is an ideal of R and that it is the smallest ideal containing all of the ideals I_a.

Proof. Let $r_1 + \cdots + r_n, s_1 + \cdots + s_m \in \sum I_a$. Because each I_i is a group under addition, we get $r_i - s_i \in I_i$. Since there are finitely many r_i and s_j, one can check that

$$r_1 + \cdots + r_n - s_1 - \cdots - s_m \in \sum I_a.$$

So I_a is a subgroup under addition. For any $r \in R$, since each I_i is an ideal, we get $rr_i \in I_i$. Using the distribution law, one can check that

$$r(r_1 + \cdots + r_n) \in \sum I_a.$$

So $\sum_a I_a$ is an ideal of R. Clearly this ideal contains each I_a (by letting this finite sum to be the sum of 1 element). Moreover, if I contains I_α for all α, then because I is a subgroup under addition, $\sum_a I_a \subset I$. So $\sum_a I_a$ is the smallest ideal containing all of the ideals I_a. □

Exercise 4.2
Prove that the homomorphic image of a Noetherian ring is Noetherian. That is, prove that if $\varphi\colon R \to S$ is a surjective ring homomorphism and R is Noetherian, then S is Noetherian.

Proof. Assume that R is Noetherian, and $\varphi\colon R \to S$ be surjective. For any ideal J of S, we have $\varphi^{-1}(J)$ to be an ideal of R. But R is Noetherian, thus $\varphi^{-1}(J)$ is finitely generated, which yields $\varphi(\varphi^{-1}(J))$ to be finitely generated. But φ is surjective, thus $\varphi \circ \varphi^{-1}(J) = J$. So J is finitely generated, or S is Noetherian. □

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

Proof. The proof is by mathematical contradiction. Assume that $(2, x)$ is generated by a single polynomial $f(x)$, then $2 \in \{f(x) \cdot g(x) : g(x) \in \mathbb{Z}[x]\}$. But $\mathbb{Z}$ is an integral domain, thus

$$\deg(f) \leq \deg(f) + \deg(g) = \deg(f \cdot g) = \det(2) = 0.$$

Thus $\deg(f) = 0$ or $f(x)$ is a constant, say, c. Because $2 \in (c)$, c has to be a divisor of 2. If $c = \pm 2$, then one can see that $x \notin (c)$. If $c = \pm 1$, then $(c) = \mathbb{Z}[x]$. But this is not the case because $1 \notin (2, x) = \{2 \cdot r + x \cdot s : r, s \in \mathbb{Z}[x]\}$. So $\mathbb{Z}[x]$ is not principal. □

Exercise 4.4
Prove that if k is a field, then $k[x]$ is a PID.

Proof. Assume that I is an ideal of $k[x]$. If $I = \{0\}$, then $I = (0)$ a principle ideal. If $I \neq \{0\}$, then there is $f(x) \in I$ of minimal degree. Clearly $(f(x)) \subset I$, we show that $I \subset (f(x))$. Because k is a field, we can rewrite any polynomial $q(x)$ of I as $q(x) = f(x) \cdot g(x) + r(x)$ where $\deg(r) < \deg(f)$. Because I is a group under addition, and $f(x) \cdot g(x) \in I$, we get $r(x) \in I$. But f is the polynomial of minimal degree, we get $r(x) = 0$. So $q(x) = f(x) \cdot g(x) \in (f(x))$. Therefore any ideal of $k[x]$ is principal or equivalently $k[x]$ is PID. □

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

Proof. Because $IJ \subset IR = I$ and similarly $IJ \subset J$, we get $IJ \subset I \cap J$. Conversely, assume that $x \in I \cap J$. Because $I + J = (1) = R$, there is some $i \in I$ and $j \in J$ such that $i + j = 1$. So $x = x \cdot 1 = xi + xj$. But $x \in I \cap J$, thus both xi, xj are in IJ. Since IJ is a group under addition, we get $x = xi + xj \in IJ$. So $IJ = I \cap J$. □

Exercise 4.7
Let $R = k$ be a field. Prove that every nonzero (pricipal) ideal in $k[x]$ is generated by a unique monic polynomial.

Proof. From Exercise 4.4, we know that $k[x]$ is a PID. So any ideal of $k[x]$ has the form $(f(x))$, where $f(x) = a_n x^n + \cdots + a_0$. Because k is a field, a_n^{-1} exists. Clearly $a_n^{-1} f(x) \in (f(x))$. Moreover, $f(x) = a_n(a_n^{-1} f(x)) \in (a_n^{-1} f(x))$. Thus $(f(x)) = (a_n^{-1} f(x))$. Since $a_n^{-1} f(x)$ is monic.

Assume that $f(x)$ and $g(x)$ are different monic functions such that $(f(x)) = (g(x))$. Because $f(x) \in g(x)$, we have $f(x) = q(x) \cdot g(x)$ and conversely $g(x) = p(x) \cdot f(x)$. Therefore

$$f(x) = q(x) \cdot g(x) = q(x) \cdot p(x) \cdot f(x).$$

So $\deg p(x) = \deg q(x) = 0$, or both of them are constant. Notice that $f(x)$ and $g(x)$ are monic, thus the formula $f(x) = q(x) \cdot g(x)$ implies that $q(x) = 1$. So $f(x) = g(x)$, contradiction. □

Exercise 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 $N \colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Z}$ by $N(a + b\sqrt{d}) := a^2 - b^2 d$. Prove that $N(zw) = N(z)N(w)$ and that $N(z) \neq 0$ 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.

- Prove that $\mathbb{Q}(\sqrt{d})$ is a field and in fact the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$.
- Prove that $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(t^2 - d)$.

Proof.

- We have $1 = 1 + 0\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. For $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, we have

  $$(a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{d} \in \mathbb{Q}(\sqrt{d}),$$

  and

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

  So $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$.

- Let $N \colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Z}$ defined by $N(a + b\sqrt{d}) = a^2 - b^2 d$. Let $a_1 + b_1\sqrt{d}, a_2 + b_2\sqrt{d} \in$

$\mathbb{Q}(\sqrt{d})$, we have

$$\begin{aligned}
N((a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d})) &= N(a_1a_2 + b_1b_2d + (a_1b_2 + a_2b_1)\sqrt{d}) \\
&= (a_1a_2 + b_1b_2d)^2 - (a_1b_2 + a_2b_1)^2d \\
&= a_1^2a_2^2 + b_1^2b_2^2d^2 + 2a_1a_2b_1b_2d - 2a_1b_2a_2b_1d - a_1^2b_2^2d - a_2^2b_1^2d \\
&= a_1^2a_2^2 - a_1^2b_2^2d + b_1^2b_2^2d + b_1^2b_2^2d^2 - a_2^2b_1^2d \\
&= (a_1^2 - b_1^2d)(a_2^2 - b_2^2d) \\
&= N(a_1 + b_1\sqrt{d})N(a_2 + b_2\sqrt{d}).
\end{aligned}$$

So $N(zw) = N(z)N(w)$. If $N(a + b\sqrt{d}) = a^2 - b^2d = 0$, we consider 2 cases. First, if $b = 0$, then so is a, and thus so is $a + b\sqrt{d}$. If $b \neq 0$, then $d = (a/b)^2$. So d is either not an integer or a square of an integer, say a/b. Both contradict to the hypothesis on d. So $N(z) = 0$ implies $z = 0$.

- Let $x + y\sqrt{d}$ be a nonzero element of $\mathbb{Q}(\sqrt{d})$, we need to find $z + t\sqrt{d}$ such that

$$1 = (x + y\sqrt{d})(z + t\sqrt{d}) = xz + tyd + (xt + yz)\sqrt{d}.$$

This is synonymous with

$$\begin{pmatrix} x & yd \\ y & x \end{pmatrix} \begin{pmatrix} z \\ t \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

But

$$\det \begin{pmatrix} x & yd \\ y & x \end{pmatrix} = x^2 - y^2d = N(x + y\sqrt{d}) \neq 0,$$

we can always find $z, t \in \mathbb{Q}$ satisfying the above equation. So $\mathbb{Q}(\sqrt{d})$ is a field. For any subfield F of $\mathbb{C}$ that contains both $\mathbb{Q}$ and $\sqrt{d}$, since a subring is closed under addition and multiplication, clearly $\mathbb{Q}(\sqrt{d}) \subset F$. So $\mathbb{Q}(\sqrt{d})$ is the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$.

- We know that $\mathbb{Q}[t]/(t^2-d)$ consists of polynomials of degree 1 or less. Let $\varphi\colon \mathbb{Q}[t]/(t^2-d) \to \mathbb{Q}(\sqrt{d})$ that maps $a_0 + a_1x \mapsto a_0 + a_1\sqrt{d}$. Clearly this is a bijection, we only need to show that it is a ring homomorphism. Ideed, first, $1 + 0x \mapsto 1 + 0\sqrt{d}$. Second, for any $a_0 + a_1x, b_0 + b_1x \in \mathbb{Q}[t]/(t^2 - d)$, we have

$$\begin{aligned}
\varphi((a_0 + a_1x) + (b_0 + b_1x)) &= \varphi((a_0 + b_0) + (a_1 + b_1)x) \\
&= (a_0 + b_0) + (a_1 + b_1)\sqrt{d} \\
&= a_0 + a_1\sqrt{d} + b_0 + b_1\sqrt{d} \\
&= \varphi(a_0 + a_1x) + \varphi(b_0 + b_1x).
\end{aligned}$$

And lastly

$$\begin{aligned}
\varphi((a_0 + a_1x) + (b_0 + b_1x)) &= \varphi(a_1b_1x^2 + (a_0b_1 + a_1b_0)x + a_0b_0) \\
&= \varphi(a_1b_1(x^2 - d) + (a_0b_1 + a_1b_0)x + a_0b_0 + a_1b_1d) \\
&= (a_0b_1 + a_1b_0)\sqrt{d} + a_0b_0 + a_1b_1d \\
&= (a_0 + a_1\sqrt{d})(b_0 + b_1\sqrt{d}) \\
&= \varphi(a_0 + a_1x).\varphi(b_0 + b_1x).
\end{aligned}$$

So φ is a ring isomorphism, which proves that $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[t]/(t^2 - d)$.

□

Exercise 4.11
Let R be a commutative ring, $a \in R$, and $f_1(x), \cdots, f_r(x) \in R[x]$

- Prove that equality of ideals

$$(f_1(x), \cdots, f_r(x), x - a) = (f_1(a), \cdots, f_r(a), x - a).$$

- Prove the useful substitution trick

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

Proof.

- For any i from 1 to r, we divide $f_i(x)$ to $x - a$ to get

$$f_i(x) = g_i(x)(x - a) + r_i.$$

Substitute $x = a$, we get $r_i = f_i(a)$. So

$$f_i(a) = f_i(x) - g_i(x)(x - a) \in (f_1(x), \cdots, f_r(x), x - a).$$

So $(f_1(a), \cdots, f_r(a), x - a) \subset (f_1(x), \cdots, f_r(x), x - a)$. Conversely, using the same formula as above, we get

$$f_i(x) = g_i(x)(x - a) + f_i(a) \in (f_1(a), \cdots, f_r(a), x - a).$$

Thus $(f_1(a), \cdots, f_r(a), x - a) = (f_1(x), \cdots, f_r(x), x - a)$.

- We have

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

□

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

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

Proof. Let $f\colon R[x_1, \cdots, x_n] \to R$ be the ring homomorphism that maps $x_i \mapsto a_i$. Clearly $f(x_i - a_i) = a_i - a_i = 0$, thus $(x_1 - a_1, \cdots, x_n - a_n) \subset \ker f$. □

Exercise 4.13
Let R be an integral domain. For all $k = 1, \cdots, n$ prove that $(x_1, \cdots, x_k)$ is prime in $R[x_1, \cdots, x_n]$.

Exercise 4.15
Let $\varphi\colon R \to S$ be a homomorphism of commutative rings, and let $I \subset S$ be an ideal. Prove that if I is a prime ideal in S, then $\varphi^{-1}(I)$ is a prime ideal in R. Show that $\varphi^{-1}(I)$ is not necessarily maximal if I is maximal.

Exercise 4.17
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 $f_1, \cdots, f_r \in R$ have no common zeros, then $(f_1, \cdots, f_r) = (1)$.

(iii) Prove that every maximal ideal M in R is of the form M_p for some $p \in K$.

Conclude that $p \mapsto M_p$ defines a bijection from K to the set of maximal ideals of R.

Exercise 4.21
Let k be an algebraically closed field, and let $I \subset k[x]$ be an ideal. Prove that I is maximal if and only if $I = (x - c)$ for some $c \in k$.

Exercise 4.22
Prove that $(x^2 + 1)$ is maximal in $\mathbb{R}[x]$.

Exercise 4.23
A ring R has Krull dimension 0 if every prime ideal in R is maximal. Prove that fields and Boolean rings have Kull dimension 0.

Exercise 4.24
Prove that the ring $\mathbb{Z}[x]$ has Krull dimension ≥ 2. (It is in fact exactly 2; thus it corresponds to a surface from the point of view of algebraic geometry.)

5. Modules over a ring

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

7. Complexes and homology