Definition of Group

1.1

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

Proof. Let G be a group, we define a category $\mathbf{C}$ as follows:

- $\mathrm{Obj}(\mathbf{C}) = \{*\}$
- $\mathrm{Hom}(*, *) = \{g \mid g \in G\}$

We prove the fore-defined structure does form a category:

- **Composition of Morphisms** There is a function as follows:

$$\mathrm{Hom}(*, *) \times \mathrm{Hom}(*, *) \to \mathrm{Hom}(*, *)$$
$$(g, h) \mapsto gh$$

  This composition law explicitly satisfies associativity.

- **Identity** $1_G \in \mathrm{Hom}(*, *)$ is the identity.

Also, for any $g \in \mathrm{Hom}(*, *)$, there exists $g^{-1} \in \mathrm{Hom}(*, *)$ such that $gg^{-1} = g^{-1}g = 1_G$. Thus, every morphism in $\mathrm{Hom}(*, *)$ is an isomorphism and $\mathbf{C}$ is a groupoid. □

1.4

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

Proof. For any $g, h \in G$, we have:

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

Which indicates G is commutative □

1.7

Prove Corollary 1.11:

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

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

Proof. ($\Rightarrow$) According to Lemma1.10

($\Leftarrow$)

$$g^N = (g^{|g|})^{\frac{N}{|g|}} = (e_G)^{\frac{N}{|g|}} = e_G$$

□

1.8

Let G be a finite **abelian** group, with exactly one element f of order 2. Prove that $\prod_{g \in G} g = f$

Proof. Since G is abelian, the product of all elements of G is well-defined, that is to say, the results is irrelevant to the multiplication order.

Thus, we have:

$$\prod_{g \in G} g = (a_1 a_1^{-1})(a_2 a_2^{-1}) \cdots (a_n a_n^{-1}) f e_G = f$$

□

Note The original problem has no abelian condition, which is a false proposition: Consider $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, which is a non-commutative group and only -1 has an order of 2. However, the product of all elements in Q_8 may generate different results:

$$1ijk(-1)(-i)(-j)(-k) = 1$$

$$1i(-i)j(-j)k(-k)(-1) = -1$$

1.9

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

Proof. All elements can be make pair with its inverse, thus:

$$G = \bigcup\{a_i, a_i^{-1}\}$$

For those elements which have order greater than 2, a_i and a_i^{-1} are different. Thus we have: $n = m + 2k + 1$ where k is the number of pair where element has order greate than 2.

This shows that $n - m = 2k + 1$ is an odd value. If n is even, then m is certainly greater than 0, meaning there are elements has order equals to 2. □

1.11

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

Proof. We prove that for $n \in \mathbb{N}^+$, $(gh)^n = e \iff (hg)^n = e$

$$\begin{aligned}(gh)^n = e &\iff (gh)(gh)\cdots(gh) = e \\ &\iff g(hg)^{n-1}h = e \\ &\iff (hg)^{n-1}h = g^{-1} \\ &\iff (hg)^n = e\end{aligned}$$

Thus we have: $|hg| \mid |gh|$ and $|gh| \mid |hg|$, indicating $|gh| = |hg|$ □

1.12

In the group of invertible 2×2 matrices, consider

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

Verify that $|g| = 4, |h| = 3$, and $|gh| = \infty$

Proof. It is easy to show that $g^2 = -I$, thus $|g| = 4$. For h we have:

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

Thus, $|h| = 3$. $gh = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, it's not hard to verify that $(gh)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$(By induction), which indicates gh has no finite order. □

Note If g and h are commutative, then $|gh| \leq lcm(|g|, |h|)$. However, for a non-commutative group, there is no general result for the order of gh.

1.14

prove that if g and h commute, and $gcd(|g|,|h|)=1$, then $|gh|=|g||h|$

Proof. If $(gh)^t=e, t\in\mathbb{N}^+$ then: $g^t=h^{-t}$. We have:

$$g^{t|h|}=h^{-t|h|}=e\Rightarrow |g|\mid t|h|\Rightarrow |g|\mid t$$

since $gcd(|g|,|h|)=1$. Also, $|h|\mid t$ and $|g||h|\mid t$ because $gcd(|g|,|h|)=1$. Note that $(gh)^{|g||h|}=e$ we have: $|gh|\mid |g||h|$. By the above fact, we have $|g||h|\mid |gh|$. Thus we have: $|gh|=|g||h|$. □

Examples of groups

2.1

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

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

would be

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

Prove that, with this notation,

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

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

Proof.

$$\begin{aligned}M_\sigma M_\tau(i,j)&=\sum_{k=1}^{n}M_\sigma(i,k)M_\tau(k,j)\\&=\sum_{\substack{1\le k\le n\\ \sigma(i)=k,\tau(k)=j}}1\end{aligned}$$

Only when $\tau\circ\sigma(i)=j$ would makes this item equals to 1, thus $M_\sigma M_\tau(i,j)=M_{\sigma\tau}(i,j)$. It's done. □

2.2

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

Proof. The permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & d-1 & d & d+1 & \cdots & n \\ 2 & 3 & 4 & \cdots & d & 1 & d+1 & \cdots & n \end{pmatrix}$$

is obviously an element has an order of d. □

2.6

For every positive integer n construct a group containing two elements g, h such that $|g| = 2$, $|h| = 2$, and $|gh| = n$.

Proof. D_{2n} satisfies this condition. □

2.7

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

2.12

Prove that there are no integers a, b, c such that $a^2 + b^2 = 3c^2$.

Proof. Let (a, b, c) be the smallest tuple that satisfies $a^2 + b^2 = 3c^2$ then we have:

$$a^2 + b^2 = [0]_3$$

There is only one possible way to achive this: $a = [0]_3, b = [0]_3$. Let $a = 3a^{'}, b = 3b^{'}$ then we have: $3(a'^2 + b'^2) = c^2$, indicating $c = [0]_3$. Let $c = 3c'$ would incur $a'^2 + b'^2 = 3c'^2$ and we have a solution (a', b', c') which is smaller than (a, b, c), a contradiction.

□

2.13

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

$$am + bn = 1$$

Conversely, prove that if $am + bn = 1$ for some integers a and b, then $\gcd(m, n) = 1$

Proof. $[m]_n$ is an generator of $\mathbb{Z}/n\mathbb{Z}$. Thus, there exists some positive integer a such that: $a[m]_n = [1]_n$, i.e $[am]_n = [1]_n$. Further, we have: $am - 1 = b'n$ for some $b' \in \mathbb{N}$. which is: $am - b'n = 1$, Let $b = -b'$, the equation holds.

If there are a, b such that $am + bn = 1$ then $\gcd(m, n)$ is a divisor of left side, thus a divisor of 1. Then $\gcd(m, n)$ has to be 1. □

2.15

Let $n > 0$ be an odd integer.

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

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

Proof. (1) Let $d = \gcd(2m + n, 2n)$ then $d \mid 2(2m + n) - 2n$, which is $d \mid 4m$. Thus: $d \mid \gcd(4m, 2n)$. Note that $\gcd(m, n) = 1$, then $\gcd(4m, 2n) = 2\gcd(2m, n) = 2$. Thus $d = 1$ or $d = 2$. Note that $2m + n$ is odd, then $d = 1$.

(2) Let $d = \gcd(\frac{r+n}{2}, n)$, then $d \mid 2 \times \frac{r+n}{2} - n$, that is $d \mid r$. Then $d \mid n$ indicates $d \mid$ r,n. Thus $d = 1$.

(3) According to (1), $\gcd(m, n) = 1$ indicates $mboxgcd(2m + n, 2n) = 1$, thus the element $[2m + n]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^*$. Next we will verify that this function is well-defined.

If $[m_1]_n = [m_2]_n$ then $n \mid (m_2 - m_1) \Rightarrow 2n \mid (2m_2 - 2m_1) \Rightarrow 2n \mid ((2m_2 + n) - (2m_1 + n))$. Thus, $[2m_2 + n]_{2n} = [2m_1 + n]_{2n}$. This indicates the function is well-defined.

If $[2m_1 + n]_{2n} = [2m_2 + n]_{2n}$ then we have $2n \mid ((2m_2 + n) - (2m_1 + n))$, which is $2n \mid 2(m_2 - m_1)$, and further $n \mid (m_2 - m_1)$, indicating $[m_2]_n = [m_1]_n$. Thus, this function is injective.

For any $[2m + n]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^*$, we have $f([m]_n) = [2m + n]_{2n}$. According to (2), $\gcd(\frac{2m+n+n}{2}, n) = 1$, which is $\gcd(m + n, n) = 1 \Rightarrow \gcd(m, n) = 1$. Thus, $[m]_n \in (\mathbb{Z}/n\mathbb{Z})^*$ and f is surjective.

In conclusion, f is both injective and surjective, thus bijective.

□

The Category Grp

3.3

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

Proof. Let τ_G and τ_H satisfies $\tau_G(g) = (g, 0_H)$ and $\tau_H(h) = (0_G, h)$. We have to show that the following commutative graph exists:

$$\begin{tikzcd}
 & A & \\
G \arrow[ur, "f_G"] \arrow[r, "\tau_G"] & G \times H \arrow[u, dashed, "\exists! f"] & H \arrow[ul, "f_H"'] \arrow[l, "\tau_H"]
\end{tikzcd}$$

We define f as follows:

$$f : G \times H \to A, \quad (g, h) \mapsto f_G(g) + f_H(h)$$

We show that f is an homomorphism:

$$\begin{aligned}
f((g_1, h_1) + (g_2, h_2)) = f((g_1 + g_2, h_1 + h_2)) &= f_G(g_1 + g_2) + f_H(h_1 + h_2) \\
&= f_G(g_1) + f_G(g_2) + f_H(h_1) + f_H(h_2) \\
&= (f_G g_1 + f_H(h_1)) + (f_G g_2 + f_H(h_2)) \\
&= f(g_1, h_1) + f(g_2, h_2)
\end{aligned}$$

And we show that f is unique. if f' satisfies the above commutative diagram, then we have:

$$\begin{aligned}
f'(g, h) = f'(g, 0_H) + f'(0_G, h) &= f'(\tau_G(g)) + f'(\tau_H(h)) \\
&= (f'\tau_G)(g) + (f'\tau_H)(h) \\
&= f_G(g) + f_H(h) = f(g, h)
\end{aligned}$$

Thus, f is unique. And by the definition of coproduct, $G \times H$ is the coproduct of G and H in category **Ab**.

□

3.4

Let G, H be groups, and assume that $G \cong H \times G$. Can you conclude that H is trivial.

Solution No, H might be non-trivial group. The following example:

$$2\mathbb{Z} \times \mathbb{Z}_2 \cong \mathbb{Z} \cong \mathbb{Z}_2$$

indicates that $H = \mathbb{Z}_2$ is not a trivial group. We construct homomorphims as follows:

$$f : 2\mathbb{Z} \times \mathbb{Z}_2 \longrightarrow \mathbb{Z}$$

$$([a], 2k) \mapsto 2k + a, a = 0, 1$$

Then it is easy to verify that f is bijective. $\forall x = ([a], 2k_1), y = ([b], 2k_2)$.

$$f(x + y) = f([a + b], 2k_1 + 2k_2) = 2k_1 + 2k_2 + (a + b) = f(x) + f(y)$$

Thus, f is an homomorphim, therefore, $2\mathbb{Z} \times \mathbb{Z}_2 \cong \mathbb{Z}$. The right part, $2\mathbb{Z} \cong \mathbb{Z}$ is trivial.

3.5

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

Proof. Proof by contradiction, say $\mathbb{Q}$ is the direct product of two groups $\mathbb{Q} \cong G \times H$, say that G is nontrivial. We prove that π_G is injective by proving no other element is mapped to be 0_G except for $0 \in \mathbb{Q}$

Suppose that $\pi_G\left(\dfrac{m}{n}\right) = 0_G$. We have: $\pi_G(m) = n\pi_G(m) = nm\pi_G(1) = 0_G$. Thus $\pi_G(1) = 0_G$. Which means $\pi_G(\mathbb{Z}) = \{0_G\}$.

Thus, for any $\dfrac{a}{b} \in \mathbb{Q}$, we have: $0_G = \pi_G(a) = b\pi_G(\frac{a}{b}) \Rightarrow \pi_G(\frac{a}{b}) = 0_G$, which means $\pi_G(\mathbb{Q}) = \{0_G\}$. Note that π_G is surjective and G is nontrivial, we have above assumption failed, that is to say, no element $\dfrac{a}{b}$ satisfies $\pi_G(\frac{a}{b}) = 0_G$, which means π_G is injective.

Thus H must be trivial, otherwise, $\pi_G(g_1, h_1) = g_1 = \pi_G(g_1, h_2)$ indicates that π_G is not injective. □

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 follows:

- find injective homomorphisms $C_2 \to S_3$, $C_3 \to S_3$;

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

Proof. The injective homomorphism is:

$$f_{C_2} : C_2 \to S_3$$
$$[0]_2 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, [1]_2 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

and

$$f_{C_3} : C_3 \to S_3$$
$$[0]_3 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, [1]_3 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, [2]_3 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

According to the definition of coproduct, the following diagram holds

$$\begin{tikzcd} & S_3 & \\ C_2 \arrow[ur, "f_{C_2}"] \arrow[r, "\tau_{C_2}"'] & C_2 \times C_3 \arrow[u, dashed, "\exists! f"] & C_3 \arrow[ul, "f_{C_3}"'] \arrow[l, "\tau_{C_3}"] \end{tikzcd}$$

The homomorphism $f : C_2 \times C_3 \to S_3$ satisfies $f\tau_{C_2} = f_{C_2}$ and $f\tau_{C_3} = f_{C_3}$. We prove that such f does not exist: We write $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ as a and b for simplicity: thus we must have:

$$f([0]_2, [0]_3) = \mathbf{1}_{S_3}, f([1]_2, [0]_3) = a, f([0]_2, [1]_3) = b, f([0]_2, [1]_3) = b^2$$

And we have:

$$ab = f([1]_2, [0]_3) + f([0]_2, [1]_3) = f([1]_2, [1]_3)$$

and

$$(ab)(ab) = f([1]_2, [1]_3)f([1]_2, [1]_3) = f([0]_2, [2]_3) = b^2$$

This indicates $abab = b^2 \Rightarrow ba = a^{-1}b = ab$. However, $ab = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $ba = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ thus $ab \neq ba$. Then such f does not exist. We assert that $C_2 \times C_3$ is not the coproduct of C_2 and C_3 in category **Grp**. $\square$

Group Homomorphisms

4.1

Check that the function π^n_m defined in 4.1 is well-defined, and makes the diagram commute.Verify that it is a group homomorphism.Why is the hypothesis $m \mid n$ necessary?

Proof. π^n_m is well-defined: if $[a_1]_n = [a_2]_n$ then $n \mid a_1 - a_2$, thus $m \mid a_1 - a_2$ as $m \mid n$. We have $[a_1]_m = [a_2]_m$ and $\pi^n_m([a_1]_n) = \pi^n_m([a_2]_n)$. The function has nothing to do with the representators. This is a homomorphism becuase:

$$\pi^n_m([a]_n + [b]_n) = \pi^n_m([a+b]_n) = [a+b]_m = [a]_m + [b]_m = \pi^n_m([a]_n) + \pi^n_m([b]_n)$$

The hypothesis $m \mid n$ is necessary because if $m \nmid n$ we may fail to show that pi^n_m is well-defined. One example is to use $m = 4, n = 3$. Then π^n_m is not well-defined, we have:

$$\pi^4_3([12]_4) = [12]_3 = [0]_3;$$

$$\pi^4_3([8]_4) = [8]_3 = [2]_3 \neq [0]_3$$

□

4.2

Show that the homomorphism $\pi^4_2 \times \pi^4_2 : C_4 \to C_2 \times C_2$ is not an isomorphism. In fact, is there any nontrivial isomorphism $C_4 \to C_2 \times C_2$?

Solution No, there is no such isomorphism between C_4 and $C_2 \times C_2$. The reason is that C_4 has one element of order 4, which is $[1]_4$, however, each element of $C_2 \times C_2$ has order 1 or 2.

4.3

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

Proof. ($\Rightarrow$) If group G with order of n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ then G must have an element of order n, which is $f^{-1}([1]_n)$. Here f is the isomorphism from G to $\mathbb{Z}/n\mathbb{Z}$.
($\Leftarrow$) If group G with order n has an element with order of n,say g Then $\langle g \rangle = G$. We define the homomorphism $f\colon G \to \mathbb{Z}/n\mathbb{Z}$ as follows: $g^k \mapsto [k]_n$. It is obvious to see that f is an isomorphism. □

4.4

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

Proof. $(\mathbb{Z},+)$ and $(\mathbb{Q},+)$ are not isomorphic to $(\mathbb{R},+)$ because they even do not have the same cardinality.

$(\mathbb{Z},+)\ncong(\mathbb{Q},+)$:
Suppose f is an isomorphism from $(\mathbb{Z},+)$ to $(\mathbb{Q},+)$, let $f(1)=g\in\mathbb{Q}$. Then we have $\mathbb{Q}$ is generated by g as $\frac{a}{b}=f(n)=nf(1)=ng$ for some n. Let $g=\frac{a}{b}$ and a,b relatively prime, then have: $\frac{na}{b}=\frac{1}{p}$. We have: $pna=b$. note that $\gcd(a,b)=1$, then we must have $a=1$. And $np=b$. We pick p a prime that is relatively prime to b. Then $np=b$ can not be true. $\square$

4.5

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

Proof. If $(\mathbb{R}\setminus\{0\},\times)$ is isomorphic to $(\mathbb{C}\setminus\{0\},\times)$ let the isomorphism be f. and let $f(1)=1$ and let $f(\mathbf{i})=g$ Consider $f(-1)$, we have:

$$f(-1)^2=f((-1)^2)=f(1)=1$$

Then we have $f(-1)=1$ or $f(-1)=-1$, note that f is an isomorphism, we must have $f(-1)=-1$. Further we have:$f(\mathbf{i})^2=f(\mathbf{i}^2)=f(-1)=-1$. However, no such element in $\mathbb{R}$ makes this true. Thus, we have show that $(\mathbb{R}\setminus\{0\},\times)\ncong(\mathbb{C}\setminus\{0\},\times)$. $\square$

4.6

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

Solution

4.7

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

Proof. $g \mapsto g^{-1}$ is an homomorphism iff $f(ab) = f(a)f(b)$ holds for any $a, b \in G$. This is true if and only if $a^{-1}b^{-1} = b^{-1}a^{-1}$ for any $a, b \in G$. And $a^{-1}b^{-1} = b^{-1}a^{-1} \iff ba = ab$ by taking inverse at both sides. Thus we have $g \mapsto g^{-1}$ if and only if G is abelian.

$g \mapsto g^2$ is an homomorphism iff $f(ab) = f(a)f(b)$ holds for any $a, b \in G$. This is true if and only if $(ab)(ab) = a^2b^2 \iff ab = ba$ for any $a, b \in G$. $\square$

4.8

Let G be a group, and $g \in G$. Prove that the function $\gamma_g : G \to G$ defined by $(\forall a \in G) : \gamma_g(a) = gag^{-1}$ is an automorphism of G. (The automorphisms γ_g are called 'inner' automorphisms of G.) Prove that the function $G \to \mathrm{Aut}(G)$ defined by $g \to \gamma_g$ is a homomorphism. Prove that this homomorphism is trivial if and only if G is abelian.

Proof. First we show that γ_g is an homomorphism: for any $a, b \in G$ we have:

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

Thus γ_g is an homomorphism. γ_g has an inverse: $\gamma_{g^{-1}}$. We have:$\gamma_g\gamma_{g^{-1}}(a) = \gamma_g(g^{-1}ag) = g(g^{-1}ag)g^{-1} = a$ for any $a \in G$. Thus, $\gamma_g\gamma_{g^{-1}} = I_G$. Similarly, $\gamma_{g^{-1}}\gamma_g = I_G$. Thus γ_g has inverse and therefore a bijection, this indicates γ_g is an isomorphism.

Let $f : G \to \mathrm{Aut}(G), g \to \gamma_g$ be the function mentioned above. We shall prove that this function is actually an homomorphism: $f(ab) = \gamma_{ab}$ and we have:$\gamma_{ab}(g) = (ab)^{-1}gab = b^{-1}(a^{-1}ga)b = \gamma_a \circ \gamma_b(g)$ for all $g \in G$. Thus we have $f(ab) = \gamma_{ab} = \gamma_a \circ \gamma_b = f(a)f(b)$. Therefore f is an homomorphism. If G is abelian then all $f(g) = \gamma_g = I_G$, thus is trivial. $\square$

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. The homomorphism $\pi_m^{mn} \times \pi_n^{mn} : C_{mn} \to C_m \times C_n$ is defined as follows:

$$[a]_{mn} \mapsto ([a]_m, [a]_n)$$

and is an homomorphism as π_m^{mn} and π_n^{mn} are homomorphisms. We shall show that this function is bijection. First it is injective: if $f([a]_{mn}) = f([b]_{mn})$ then $([a]_m, [a]_n) = ([b]_m, [b]_n)$ which means: $m \mid a - b$ and $n \mid a - b$. Further we have $mn \mid a - b$ because $\gcd(m, n) = 1$. Thus $[a]_{mn} = [b]_{mn}$ and this indicates f is injective.

For surjective property, note that $\gcd(m, n) = 1$ indicates there exist some x, y such that $xm - ny = 1$. Then we have x satisfies $xm = ny + 1$, we call $\mathbf{x} = [xm]_{mn}$, we have $f(\mathbf{x}) = ([0]_m, [1]_n)$. Similarly, we will have such $\mathbf{y}$ satisfying $f(\mathbf{y}) = ([1]_m, [0]_n)$. For any $([a]_m, [b]_n) \in C_m \times C_n$ we have: $([a]_m, [b]_n) = ([a]_m, [0]_n) + ([0]_m, [b]_n) = af(\mathbf{x}) + bf(\mathbf{y}) = f(a\mathbf{x} + b\mathbf{y})$. Thus f is surjective and f is bijective.

In conclusion, we have f to be group homomorphism and bijection. Thus f is a group isomorphism. □

4.10

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

Proof. Suppose that $(\mathbb{Z}/pq\mathbb{Z})^*$ is cyclic. Then we have the order of □

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 the maximum order of elements in $(\mathbb{Z}/p\mathbb{Z})^*$ be d, we show that d must be p.

If $d \leq p - 2$, say g has order d, then for every element $h \in (\mathbb{Z}/p\mathbb{Z})^*$ we have $|h| \mid d$. Otherwise, the element gh will have order of $\mathrm{lcm}(|h|, d) > d$, contradicts the assumption that d is the maximum order.

Thus we have $g^d = 1$ for every element in $\mathbb{Z}/p\mathbb{Z}$, which means $x^d = 1$ has $p - 1$ solutions, controdicts the assumption. Thus, we have $d = p - 1$ and $\mathbb{Z}/p\mathbb{Z}$ is cyclic. □

NOTE This proof can not be used to proof a general $(\mathbb{Z}/n\mathbb{Z})^*, n \in \mathbb{N}^+$ is cyclic(though this proposition is false). The assumption $x^d = 1$ has at most d solutions is constrainted within $\mathbb{Z}/p\mathbb{Z}$, not generalized group.

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. C_n is generated by $[1]_n$, so any automorphism from C_n to C_n is determined by the image of $[1]_n$. To make this homomorphim f bijective, we must make $f([1]_n)$ also be a generator. Thus the number of elements in $\mathrm{Aut}_{\mathbf{Grp}}(C_n)$ is determined by the number of generators in C_n, which is the number of positive number that is relatively prime to n. We formally prove this as followed:

Let $f \in \mathrm{Aut}_{\mathbf{Grp}}(C_n)$, consider $f([1]_n)$. Notice that f is isomorphism, thus we have $|f([1]_n)|$ has order n(proposition4.8), thus $|f([1]_n)|$ is relatively prime to n(The representator of $f([1]_n)$).

On the contrary, if $[m]_n, \gcd(m,n) = 1$, we define $f([1]_n) = [m]_n$, it derives an isomorphism from C_n to C_n. Thus, we have established a map from $\mathrm{Aut}_{\mathbf{Grp}}(C_n)$ to the set of numbers that are relatively prime to n, denoted as S. This map is injective as each f maps $[1]_n$ to different elements in S, and is surjective by the construction described above. Thus, it is bijection and they have the same cardinality. □

4.15

Compute the group of automorphisms of $(\mathbb{Z}, +)$. Prove that if p is prime, then $\mathrm{Aut}_{\mathbf{Grp}}(C_p) \cong C_{p-1}$. (Use Exercise 4.11.)

Proof. There are only two elements in $\mathrm{Aut}_{\mathbf{Grp}}(\mathbb{Z}, +)$: The identity and the isomorphism that maps 1 to -1.
To prove $\mathrm{Aut}_{\mathbf{Grp}}(C_p) \cong C_{p-1}$, we show that $\mathrm{Aut}_{\mathbf{Grp}}(C_p) \cong (\mathbb{Z}/p\mathbb{Z})^*$ and leverage the result of exercise 4.11.

The proof of exercise 4.14 shows that there is a bijection from $\mathrm{Aut}_{\mathbf{Grp}}(C_p)$ to $(\mathbb{Z}/p\mathbb{Z})^*$ by $[m]_n \mapsto f_{[m]_n}, \gcd(m,n) = 1$, where $f_{[m]_n}$ is the automorphism derived by $f_{[m]_n}([1]_n) = [m]_n$. We show that this map, namely ϕ is an homomorphim:

$$\phi([m_1]_n \times [m_2]_n) = \phi([m_1 m_2]_n) = f_{[m_1 m_2]_n} = f_{[m_1]_n} \circ f_{[m_2]_n}$$

The last = is true by checking the image of $[1]_n$ under $f_{[m_1 m_2]_n}$ and $f_{[m_1]_n} \circ f_{[m_2]_n}$ In conclusion, we have the map ϕ is both a homomorphim and bijection. Thus, $\mathrm{Aut}_{\mathbf{Grp}}(C_p) \cong (\mathbb{Z}/p\mathbb{Z})^* \cong C_{p-1}$. □

4.16

Prove *Wilson's theorem*: a positive integer p is prime if and only if

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

Proof. ($\Rightarrow$) If p is a prime, then $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic, let $g \in \mathbb{Z}/p\mathbb{Z})^*$ be the elements with order $p-1$, then we have:

$$(p-1)! \equiv gg^2 \dots g^{p-1} \equiv g^{\frac{p(p-1)}{2}} \mod p$$

Note that we have $g^{p-1} \equiv 1 \mod p$ and $g^{\frac{p-1}{2}} \equiv -1 \mod n$ because the order of g is exactly $p-1$. We have:

$$g^{\frac{p(p-1)}{2}} = g^{\frac{(p-1)^2}{2}} g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \equiv -1 \mod p$$

The proof is done.

($\Leftarrow$) Suppose p is not a prime and d is a divisor of p. Then we have:$(p-1)! \equiv -1 \mod d$. However, $d < p$ indicates $d \mid d!$ and $d! \mid (p-1)!$, thus we have:$(p-1)! \equiv 0 \mod d$, a contradiction. □

5. Free Group

5.1

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

Solution It has, the object (G, j) where G is trivial group and j is a set-function satisfies: $a \mapsto 1_G, \forall a \in A$ is a final object in $\mathscr{F}^A$. It's obvious that any other object in this category has a morphism to this object, namely the trivial homomorphim. Note that final object in a category is the same up to isomorphism, thus, these are all possible final objects.

5.2

5.3

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

Proof. The universal property indicates that the following commutative diagram holds for any objects (G, j_2):

$$\begin{tikzcd}
F(A) \arrow[r, "\varphi"] & G \\
A \arrow[u, "j"] \arrow[ur, "j_1"] &
\end{tikzcd}$$

Specifically, let j_1 be injective set-function, we must have $j_1 = \varphi \circ j$, the fact that j_1 is injective indicates j is injective. The difficulty is to show that such j_1 and G exists.

$\square$

5.5

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

Proof. $H^{\oplus A}$ is a subset of H^A that consists of set-functions only has finitely many "non-zero" images. For $\alpha_1, \alpha_2 \in H^{\oplus A}$, we have $\alpha_1 + \alpha_2 \in H^A$ by defining:

$$(\alpha_1 + \alpha_2)(a) = \alpha_1(a) + \alpha_2(a)$$

Note that α_1 and α_2 has at most finitely many non-zero images, thus $\alpha_1 + \alpha_2$ has only finitely many non-zero images. Further, we have the zero element: $\mathbf{0} : a \mapsto 0_H$ and addition inverse:$-\alpha : a \mapsto -\alpha(a)$. Thus $H^{\oplus A}$ is a group. The commutativaty of H also indicates that $H^{\oplus A}$ is an abelian group. $\square$

5.6

Prove that the group $F(\{x, y\})$ (visualized in Example 5.3) is a coproduct $\mathbb{Z} * \mathbb{Z}$ of $\mathbb{Z}$ by itself in the category **Grp**.

Proof. There is a explicit proof to show that $F(\{x, y\})$ is the coproduct of $\mathbb{Z}$ and $\mathbb{Z}$: We have the following diagram:

$$\begin{tikzcd}
\mathbb{Z} \arrow[dr, "\iota_1"] & \\
& F(\{x,y\}) \\
\mathbb{Z} \arrow[ur, "\iota_2"] &
\end{tikzcd}$$

ι_1 and ι_2 are homomorphims derived by defining $\iota_1(1) = x$ and $\iota_2(1) = y$. Then for any other group G and f_1, f_2 we have to prove the next diagram holds:

$$\begin{tikzcd}
 & G & \\
\mathbb{Z} \arrow[ur, "f_1"] \arrow[r, "\iota_1"] & F(\{x,y\}) \arrow[u, dashed, "\exists!\varphi"] & \mathbb{Z} \arrow[ul, "f_2"'] \arrow[l, "\iota_2"]
\end{tikzcd}$$

Define φ such that $\varphi(x) = f_1(1)$ and $\varphi(y) = f_2(1)$. Then we have such φ is a homomorphim and is unique. Thus, the free group on $\{x, y\}$ is a coproduct of $\mathbb{Z}$ and $\mathbb{Z}$. $\square$

5.7

Extend the result of Exercise 5.6 to free groups $F(\{x_1, \dots, x_n\})$ and to free abelian groups $F^{ab}(\{x_1, \dots, x_n\})$

Solution The Extended result is that: $F(\{x_1, \dots, x_n\})$ is the coproduct of n $\mathbb{Z}$ in category **Grp** and is a coproduct of n $\mathbb{Z}$ in category Ab.

5.8

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

Proof. We will only prove the fact that $F(A \sqcup B) = F(A) * F(B)$. In this question, we can only use the universal property. To prove that $F(A \sqcup B)$ is the coproduct of $F(A)$ and $F(B)$, we first construct the "injection" homomorphim: Here is the diagram:

$$\begin{tikzcd}
A \arrow[r, "i_A"] \arrow[d, "\iota_A"] & F(A) \arrow[d, dashed, "I_{F(A)}"] \\
A \sqcup B \arrow[r, "i_{A \sqcup B}"] & F(A \sqcup B) \\
B \arrow[r, "i_B"] \arrow[u, "\iota_B"] & F(B) \arrow[u, dashed, "I_{F(B)}"']
\end{tikzcd}$$

Note that the set-function $i_{A \sqcup B} \circ \iota_A$(or $i_{A \sqcup B} \iota_B$) is a function from A(or B) to $F(A \sqcup B)$, according to the universal property of $F(A)$, there exists a unique homomorphim $I_{F(A)}$(or $I_{F(B)}$) such that $I_{F(A)} \circ i_A = i_{A \sqcup B} \circ \iota_A$ and $I_{F(B)} \circ i_B = i_{A \sqcup B} \circ \iota_B$. We prove that $(F(A \sqcup B), I_{F(A)}, I_{F(B)})$ is a coproduct of $F(A)$ and $F(B)$.

Say G is another group with homomorphim$f_{F(A)} : F(A) \to G$ and $f_{F(B)} : F(B) \to G$. Then we have:

$$\begin{tikzcd}
A \arrow[r, "i_A"] \arrow[d, "\iota_A"] & F(A) \arrow[d, "f_{F(A)}"] \\
A \sqcup B \arrow[r, dashed, "f"] & G \\
B \arrow[r, "i_B"] \arrow[u, "\iota_B"] & F(B) \arrow[u, "f_{F(B)}"']
\end{tikzcd}$$

Note that $A \sqcup B$ is a coproduct of A and B, then there is a set function f such that $f \circ \iota_A = f_{F(A)} \circ i_A$ and $f \circ \iota_B = f_{F(B)} \circ i_B$.

According to the universal property of $F(A \sqcup B)$, there exists some φ such that the following diagram commutes:

$$\begin{tikzcd}
A \sqcup B \arrow[r, "i_{A \sqcup B}"] \arrow[dr, "f"'] & F(A \sqcup B) \arrow[d, dashed, "\varphi"] \\
& G
\end{tikzcd}$$

We have to prove that $f_{F(A)} = \varphi \circ I_{F(A)}$ and $f_{F(A)} = \varphi \circ I_{F(B)}$ and such φ is unique. We only prove that $f_{F(A)} = \varphi \circ I_{F(A)}$ due to similarity.

Note that $I_{F(A)} \circ i_A = i_{A \sqcup B} \circ \iota_A$, we have:$\varphi \circ I_{F(A)} \circ i_A = \varphi \circ i_{A \sqcup B} \circ \iota_A = (\varphi \circ i_{A \sqcup B}) \circ \iota_A = f \circ \iota_A = f_{F(A)} \circ i_A$ that is $(\varphi \circ I_{F(A)}) \circ i_A = f_{F(A)} \circ i_A$.

In the following diagram:

$$\begin{tikzcd}
& F(A) \arrow[dl, dashed, "\varphi \circ I_{F(A)}"'] \arrow[dr, "f_{F(A)}"] & \\
G & A \arrow[l, "(\varphi \circ I_{F(A)}) \circ i_A"] \arrow[u, "i_A"] \arrow[r, "f_{F(A)} \circ i_A"] & G
\end{tikzcd}$$

According to the universal property of $F(A)$, we must have:$\varphi \circ I_{F(A)} = f_{F(A)}$ due to the uniqueness. To prove the uniqueness of φ, we assume that φ' satisfies $\varphi' \circ I_{F(A)} = f_{F(A)}$(same for B), we have $\varphi' \circ I_{F(A)} \circ i_A = f_{F(A)} \circ i_A$. The left side equals to $\varphi' \circ (i_{A \sqcup B} \circ \iota_A)$, thus we have:$(\varphi' \circ i_{A \sqcup B}) \circ \iota_A = f_{F(A)} \circ i_A$. According to the universal property of $A \sqcup B$, we have $f = \varphi' \circ i_{A \sqcup B} \Rightarrow \varphi \circ i_{A \sqcup B} = \varphi' \circ i_{A \sqcup B}$. And we are done.

$\square$

6. Subgroups

6.2

Prove that the set of 2×2 matrices

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

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

Proof. Let A denote the set compries matrix described in this question, then for any $a, b \in A$, we have:

$$ab^{-1} = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \times \frac{1}{ad} \begin{pmatrix} d_2 & -b_2 \\ 0 & a_2 \end{pmatrix} = \frac{1}{ad} \begin{pmatrix} a_1 d_2 & b_1 a_2 - a_1 b_2 \\ 0 & d_1 a_2 \end{pmatrix}$$

And $(a_1 d_2)(d_1 a_2) = (a_1 d_1)(a_2 d_2) \neq 0$. Thus we have $ab^{-1} \in A$ and A is a subgroup of $\mathrm{GL}_2(\mathbb{C})$.

For a more general case, we show that the multiplication of two 'upper triangular' matrix is still 'upper triangular' and the inverse of an 'upper trivial' matrix is still upper trivial.

If A and B are 'upper triangular' matrixes, then for AB we have:

$$(AB)_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}$$

For $i > j$, note that:

$$a_{ik} b_{kj} = \begin{cases} 0, a_{ik} = 0, i > k \\ 0, b_{kj} = 0, k \geq i > j \end{cases}$$

Thus, we have $(AB)_{ij} = 0$ for $i > j$. This indicates that AB is still 'upper triangular'.

For the second proposition, we induct on n: for $n = 2$, the case is proved above; Let's assume this proposition is held for $n = k$, and for $n = k + 1$, for any 'upper triangular' matrix, it could be written as:

$$B = \begin{pmatrix} a_{11} & B_{1\times k} \\ \mathbf{0}_{k\times 1} & T_{k\times k} \end{pmatrix}$$

where $a_{11} \neq 0$ and $T_{k\times k}$ is an 'upper triangular' matrix of order n. We have its inverse as:

$$B^{-1} = \begin{pmatrix} a_{11}^{-1} & -a_{11}^{-1}B_{1\times k}T_{k\times k}^{-1} \\ \mathbf{0}_{k\times 1} & T_{k\times k}^{-1} \end{pmatrix}$$

According to the assumption that $T_{k\times k}^{-1}$ is an 'upper triangular', we have B^{-1} is also 'upper triangular'.

With above two propositions, for any $a, b \in A_n$, we have ab^{-1} is still an 'upper triangular' matrix, thus $ab^{-1} \in A_n$ and the proof is done. $\square$

6.3

Prove that every matrix in $\mathrm{SU}_2(\mathbb{C})$ 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, $\mathrm{SU}_2(\mathbb{C})$ may be realized as a three-dimensional sphere embedded in $\mathbb{R}^4$; in particular, it is simply connected.)

Proof. Let $M \in \mathrm{SU}_2(\mathbb{C})$ and

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

. We have

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} \overline{x} & \overline{z} \\ \overline{y} & \overline{w} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \overline{x} & \overline{z} \\ \overline{y} & \overline{w} \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}$$

That means:

$$\begin{cases} x\overline{z} + y\overline{w} = 0 \\ z\overline{x} + w\overline{y} = 0 \\ \overline{x}y + \overline{z}w = 0 \\ \overline{y}x + \overline{w}z = 0 \end{cases}$$

$\square$

6.5

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

Proof. For any $a, b \in G$, we have $a = g^n, b = h^n$ for some $g, h \in G$, and $b^{-1} = (h^{-1})^n$. Thus:

$$ab^{-1} = g^n(h^{-1})^n = (gh^{-1})^n$$

Note that $gh^{-1} \in G$, thus $ab^{-1} \in \{g^n \mid g \in G\}$, which means this group is a subgroup of G. An counter example of the latter assertion would be the permutation group S_4 and let $n = 2$. □

6.7

Show that inner automorphisms (cf. Exercise 4.8) form a subgroup of $\mathrm{Aut}(G)$; this subgroup is denoted $\mathrm{Inn}(G)$. Prove that $\mathrm{Inn}(G)$ is cyclic if and only if $\mathrm{Inn}(G)$ is trivial if and only if G is abelian

Proof. For $\gamma_a, \gamma_b \in \mathrm{Inn}(G)$, we have $\gamma_a\gamma_b^{-1} = \gamma_{ab^{-1}} \in \mathrm{Inn}(G)$. Thus it is a subgroup of $\mathrm{Aut}(G)$.

$\mathrm{Inn}(G)$ is trivial is obviously equavialent to the fact that G is abelian. If $\mathrm{Inn}(G)$ is cyclic, then there exists some $a \in G$ such that for any $g \in G$, there exists some $n \in \mathbb{N}^+$ such that $\gamma_{a^n} = \gamma_g$, this indicates $gag^{-1} = a^n a a^{-n} = a$ and thus $ga = ag, \forall g \in G$. Thus we have $\forall \gamma_g \in \mathrm{Inn}(G)$, $\gamma_g = \gamma_{a^m}$ and $\forall x \in G, \gamma_{a^m}(x) = x$, thus $\gamma_g = \mathrm{Id}_G$. The proof is done. □

6.9

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

Proof. Let $H < G$ be a finitely generated subgroup and $H = \langle a_1, a_2, ..., a_n \rangle$. We induct on n to prove that H is cyclic:
(1) If $n = 1$ then we have $F(\{a_1\})$ to be cyclic, thus $H = \varphi(F(\{a_1\}))$ is also cyclic
(2) Assume for n this holds, consider $n + 1$. Since $H^{'} = \langle a_1, a_2, ..., a_n \rangle$ is cyclic, there exits some $q \in \mathbb{Q}$ such that $H^{'} = \langle q \rangle$, Consider a_{n+1} and q, let's say a_{n+1} and q both has the form: $q = \frac{s}{t}, a_{n+1} = \frac{s^{'}}{t}$. Consider $q^{'} = \gcd(s, s^{'})$ and we will have both q and a_{n+1} be multiple $\frac{q^{'}}{t}$. Note that $\gcd(\frac{s}{q^{'}}, \frac{s^{'}}{q^{'}}) = 1$. We will have $x, y \in \mathbb{N}$ such that $\frac{xs}{q^{'}} + \frac{ys^{'}}{q^{'}} = 1$, by multiplying $\frac{q^{'}}{t}$ at both sides:

$$\frac{q^{'}}{t} = \frac{xs}{t} + \frac{ys^{'}}{t}$$

This means: $\dfrac{q^{'}}{t} \in \langle a_1, a_2, ..., a_{n+1} \rangle$ and it's obviously that each element can be expressed as multiple of $\dfrac{q^{'}}{t}$. Thus the proposition is true for the case of $n+1$.

In conclusion, we have proved that any finitely generated subgroup of $\mathbb{Q}$ is cyclic.

$\mathbb{Q}$ is not finitely generated as $\mathbb{Q}$ is not cyclic. □

6.10

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

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

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

$$s = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Proof. Using induction, we have $t^a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, a \in \mathbb{N}$ and $s^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, s^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ □

6.12

Let m, n be positive integers, and consider the subgroup $\langle m, n \rangle$ of $\mathbb{Z}$ they generate. By Proposition 6.9, $\langle m, n \rangle = d\mathbb{Z}$ for some positive integer d. What is d, in relation to m, n?

Proof. Since $\langle m, n \rangle = d\mathbb{Z}$, there exits some $x, y \in \mathbb{N}$ such that $xm + yn = d$. Thus we have $\gcd(m, n) \mid d$. On the contrary, note that $m \in d\mathbb{Z}$ and $n \in d\mathbb{Z}$, thus we have $d \mid m$ and $d \mid n$, which indicates $d \mid \gcd(m, n)$. Thus we have $\gcd(m, n) = d\mathbb{Z}$. □

6.16

Counterpoint to Exercise 6.15: the homomorphism $\varphi : \mathbb{Z}/3\mathbb{Z} \to S_3$ given by

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

is a monomorphism; show that it has no left-inverse in **Grp**

Proof. If there the left-inverse of φ exits, denoted as φ^{-1}, then we must have: $\varphi^{-1}\left(\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right) = [1], \varphi^{-1}\left(\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\right) = [2]$, Consider $\varphi^{-1}((1\ 2)), \varphi^{-1}((1\ 3))$, $\varphi^{-1}((2\ 3))$. We have $\varphi^{-1}(\mathrm{id}) = \varphi^{-1}((1\ 2)^2) = \varphi^{-1}((1\ 2))^2$ That is: $\varphi^{-1}((1\ 2))^2 = [0]$. Thus we must have $\varphi^{-1}((1\ 2)) = [0]$. Similarly we have $\varphi^{-1}((2\ 3)) = [0], \varphi^{-1}((1\ 3)) = [0]$. However, note that $[2] = \varphi^{-1}\left(\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}\right) = \varphi^{-1}((1\ 2)(1\ 3))$ $= \varphi^{-1}((1\ 2)) + \varphi^{-1}((1\ 3)) = [0]$. a contradiction. This means φ^{-1} does not exits in **Grp**. □

1 Quotient groups

7.1

List all subgroups of S_3 and determine which subgroups are normal and which are not normal.
Solution All subgroups of S_3 are as follows:

- Order of 1: $\{\mathrm{id}\}$
- Order of 2: $\{\mathrm{id}, (1\ 2)\}$, $\{\mathrm{id}, (1\ 3)\}$, $\{\mathrm{id}, (2\ 3)\}$
- Order of 3: $\left\{\mathrm{id}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right\}$

The normal subgroups are $\{\mathrm{id}\}$ and $\left\{\mathrm{id}, \begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}\right\}$

7.2

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

Solution For abelian group, the proposition is true as any subgroup of an abelian group is normal. Generally speaking, the proposition is not true. The counterpoint would be

$$\varphi : \mathbb{Z}/2\mathbb{Z} \to S_3$$
$$\varphi([0]) = \mathrm{id}, \quad \varphi([1]) = \begin{pmatrix}1 & 2 & 3\\ 1 & 3 & 2\end{pmatrix}$$

And obviously $\mathrm{Im}(\varphi)$ is not a normal subgroup as Exercise7.1 claims the only normal subgroup is the subgroup of order 3.

7.6

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

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

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

Proof. Note this relation naturaly satisfies *symmetricity* and *reflexity*: $\forall g \in G, gg^{-1} = \mathrm{id} = \mathrm{id}^n$ and if $a \sim b$ then $ab^{-1} = g^n$ for some g, indicates $ba^{-1} = (ab^{-1})^{-1} = (g^n)^{-1} = (g^{-1})^n \Rightarrow b \sim a$

To show that $\sim$ is not an equavialent relation in general, we need to consider a counterpoint of *transitivity*.

If G is commutative, then *transitivity* is true as: If $a \sim b, b \sim c$ then $ab^{-1} = g^n$ and $bc^{-1} = h^n$, as a result $ab^{-1}bc^{-1} = ac^{-1} = g^n h^n = (gh)^n$, indicating $a \sim c$. □

7.7

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

Proof. If h is an element of order n, then for any $g \in G$, we have $ghg^{-1} = \gamma_g(h)$ also has an order of n as γ_g is an isomorphism.

Thus, for any elements of H, it can be denoted as $g_1 g_2 \dots g_n$ where $g_i, i = 1, 2 \dots n$ is an element of order n. Then $\forall g \in G$ we have: $g(g_1 g_2 \dots g_n)g^{-1} = (gg_1g^{-1})(gg_2g^{-1}) \dots (gg_ng^{-1}) \in H$ as gg_ig^{-1} is an element of order n. Thus we have proved that H is normal. □

7.8

Prove that If H is any subgroup of a group G, the relation $\sim_L$ defined by

$$(\forall a, b \in G) : a \sim_L b \Longleftrightarrow a^{-1}b \in H$$

is an equivalence relation satisfying (†)

Proof. We only need to prove $\sim_L$ is an equavialent relation and the remaining part is done by the author:

- *reflexity*: $\forall g \in G$ we have $g^{-1}g = e \in H \Rightarrow g \sim_L g$

- *symmetricity*: If $a \sim_L b$ then $a^{-1}b \in H \Rightarrow b^{-1}a = (a^{-1}b)^{-1} \in H \Rightarrow b \sim_L a$
- *transitivity*: If $a \sim_L b$ and $b \sim_L c$ then $a^{-1}b, b^{-1}c \in H \Rightarrow a^{-1}c = (a^{-1}b)(b^{-1}c) \in H \Rightarrow a \sim_L c$

In conclusion, $\sim_L$ is an equavialent relation. And it satisfies the following property:

$$a \sim_L b \Rightarrow (\forall g \in G) ga \sim_L gb$$

as:

$$a \sim_L b \Rightarrow a^{-1}b \in H \Rightarrow a^{-1}g^{-1}gb \in H \Rightarrow (ga)^{-1}(gb) \in H \Rightarrow ga \sim_L gb$$

□

7.9

State and prove the 'mirror' statements of Proposition 7.4 and 7.6, leading to the description of relations satisfying (††)
The mirror statement of Proposition 7.4 is:

Mirror of Proposition7.4 *Let $\sim$ be an equivalence relation on a group G, satisfying (††). Then:*

- *the equivalence class of e_G is a subgroup H of G; and*
- $a \sim b \iff ab^{-1} \in H \iff Ha = Hb$

Proof. Let H be the equavialence class of e_G. If $a \in H, b \in H, b \in H$. Then $a \sim b$. By (††) we have $ab^{-1} \sim bb^{-1}$, which is $ab^{-1} \sim e_G$. Thus $ab^{-1} \in H$. And H is a subgroup of G.

$a \sim b \iff ab^{-1} \sim e_G \iff ab^{-1} \in H$. Then we prove that the equavialence class of a is Ha. Let the equavialence class of a be $[a]$, then $(\forall b \in [a]) : a \sim b \Rightarrow ab^{-1} \sim e_G \Rightarrow ab^{-1} \in H \Rightarrow ab^{-1} = h, h \in H$. Thus $b = h^{-1}a \in Ha$. Thus $[a] \subseteq Ha$. Conversely, for any $ha \in Ha, h \in H$, we have $h \sim e_G$ and $ha \sim e_G a \Rightarrow ha \sim a$. Thus $ha \in [a]$. This indicates $Ha \subseteq [a]$. So we have $[a] = Ha$.

Thus we have $a \sim b \iff [a] = [b] \iff Ha = Hb$. □

Mirror of Proposition7.4 *If H is any subgroup of a group G, the relation $\sim_R$ defined by*

$$(\forall a, b \in G) : a \sim_R b \iff ab^{-1} \in H$$

is an equavialence relation satisfying (††).

Proof. We do not prove that this relation is an equavialence relation but only to prove it satisfies (††).

If $a \sim b$ then for any $g \in G$, we have $a \sim b \Rightarrow ab^{-1} \in H \Rightarrow a(gg^{-1})b^{-1} \in H \Rightarrow (ag)(g^{-1}b^{-1}) \in H \Rightarrow (ag)(bg)^{-1} \in H \Rightarrow ag \sim bg$. Thus this equavialence relation satisfies (††). □

7.10

Let G be a group, and $H \subseteq G$ a subgroup. With notation as in Exercise 6.7, show that H is normal in G if and only if $\forall \gamma \in \text{Inn}(G), \gamma(H) \subseteq H$. Conclude that if H is normal in G then there is an interesting homomorphism $\text{Inn(G)} \longrightarrow \text{Aut}(H)$

Proof. H is normal in G if and only if $(\forall g \in G) : gH \subseteq Hg \iff (\forall g \in G) : gHg^{-1} \subseteq H \Longleftarrow (\forall g \in G) : \gamma_g(H) \subseteq H$. The proof is done.

Note that γ_g constrainted on H is actually an automorphism of H as $\gamma_g(H) \subseteq H$. Define function $\varphi : \text{Inn}(G) \longrightarrow \text{Aut}(H), \gamma_g \mapsto \gamma_g \mid_H$ Is actually an homomorphim. But why is it interesting? □

7.11

Let G be a group, and let $[G, G]$ be the subgroup of G generated by all elements of the form $aba^{-1}b^{-1}$. (This is the commutator subgroup of G; we will return to it in §IV.3.3.) Prove that $[G, G]$ is normal in G.

Proof. Note for any $aba^{-1}b^{-1} \in [G, G]$ and for any $g \in G$, we have: $gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}$. Note that $gag^{-1}, gbg^{-1} \in G$. Thus $gaba^{-1}b^{-1}g^{-1} \in [G, G]$. Note that $\forall t \in [G, G]$, it can be written as $t = g_1g_2 \cdots g_n$ where each g_i has form $aba^{-1}b^{-1}$. Thus for any $g \in G$, $gtg^{-1} = (gg_1g^{-1})(gg_2g^{-1}) \cdots (gg_ng^{-1})$. Note that each gg_ig^{-1} still has form $aba^{-1}b^{-1}$. Thus $gtg^{-1} \in [G, G]$. Indicates $[G, G]$ is normal. □

7.12

Let $F = F(A)$ be a free group, and let $f : A \longrightarrow G$ be a set-function from the set A to a commutative group G. Prove that f induces a unique homomorphism $F/[F, F] \to G$, where $[F, F]$ is the commutator subgroup of F defined in Exercise 7.11. (Use Theorem 7.12.) Conclude that $F/[F, F] \cong F^{ab}(A)$.

Proof. We first need to prove that $F/[F, F]$ is abelian. By exercise 7.11, we have $[F, F]$ is a normal subgroup of F and $F/[F, F]$ the quotient group. We need to prove that for any $a, b \in F$, we have $ab[F, F] = ba[F, F]$ to indicate commutativaty.

For any $t \in [F, F]$, let $t = g_1 g_2 \cdots g_n$ where each g_i has form $aba^{-1}b^{-1}$. Then we have $abt = baa^{-1}b^{-1}abt = (ba)(a^{-1}b^{-1}abt)$, note that $a^{-1}b^{-1}ab \in [F, F]$. Thus $abt \in ba[F, F]$ and $ab[F, F] \subseteq ba[F, F]$. Similarly $ba[F, F] \subseteq ab[F, F]$. Thus we have

$$(\forall a, b \in G) : (a[F, F])(b[F, F]) = ab[F, F] = ba[F, F] = (b[F, F])(a[F, F])$$

This indicates $F/[F, F]$ is commutative.

According to the universal property of $F(A)$, the following diagram holds:

$$\begin{tikzcd} A \arrow[r, "\iota_A"] \arrow[dr, "f"'] & F \arrow[d, dashed, "\exists ! \varphi"] \\ & G \end{tikzcd}$$

Note that φ we have $\forall t \in [F, F]$, we have $\varphi(t) = \varphi(g_1 g_2 \cdots g_n) = e_G$, thus $[F, F] \subseteq \ker \varphi$. Thus according to theorem 7.12, we have:

$$\begin{tikzcd} F \arrow[r, "\varphi"] \arrow[dr, "\pi"'] & G \\ & F/[F, F] \arrow[u, dashed, "\exists ! \widetilde{\varphi}"] \end{tikzcd}$$

Put these two diagram together:

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

This indicates that $F/[F, F] \cong F^{ab}(A)$. $\square$