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:

$$\prod_{g\in G} g = (a_1a_1^{-1})(a_2a_2^{-1})\cdots(a_na_n^{-1})fe_G = f$$

□

Note The original problem has no abelian condition, which is a false proposition: Consider $Q_8 = \{\pm1, \pm i, \pm j, \pm k\}$, 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. $\square$

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 $|gh| = |hg|$ $\square$

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. $\square$

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: $0_G = \pi_G(a) = b\pi_G(\dfrac{a}{b}) \Rightarrow \pi_G(\dfrac{a}{b}) = 0_G$, 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 $\pi_G(\dfrac{a}{b}) = 0_G$, 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**. $\square$