

1. **Intersections and unions of subgroups.** Prove that if H and K are subgroups of G , then so is $H \cap K$. On the other hand, prove $H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.

Proof. Suppose $H, K \leq G$. Consider $H \cap K$.

Note that $1 \in H, K$ by the definition of groups, so $1 \in H \cap K$. Hence, $H \cap K \neq \emptyset$

Now let $x, y \in H \cap K$. Then $x, y \in H$ and $x, y \in K$, both of which are groups. Hence, $y^{-1} \in H$ and $y^{-1} \in K$, which implies $xy^{-1} \in H$ and $xy^{-1} \in K$. Thus, $xy^{-1} \in H \cap K$.

As a result, $H \cap K$ satisfies the subgroup criterion and is hence a subgroup of G .

Now consider $H \cup K$. Suppose for contraposition that $H \not\subseteq K$ and $K \not\subseteq H$. Then $\exists x \in H$ such that $x \notin K$ and $\exists y \in K$ such that $y \notin H$.

Then we have $y^{-1} \notin H$ and $x \notin K$, so $xy^{-1} \notin H, K$. Hence $xy^{-1} \notin H \cup K$ and so $H \cup K$ does not satisfy the subgroup criterion.

As a result, we have that $H \cup K$ subgroup of G implies that $H \subset K$ or $K \subset H$.

Now for the other direction of the proof. Suppose $H \subset K$.

Then $\forall x \in H$ we have $x \in K$. Hence, $H \cup K = K$. Since $K \leq G$, we have $H \cup K \leq G$ as well. \square

2. **Homomorphisms and isomorphisms.**

(a) Show that the map

$$\varphi : G \rightarrow G \quad \text{defined by} \quad \varphi : g \mapsto g^{-1}$$

is a homomorphism if and only if G is abelian. Give an example of a (non-abelian) group G , and verify by example that this map is not a homomorphism.

Proof. Suppose φ is a homomorphism. Then $\varphi(xy) = \varphi(x)\varphi(y)$ for every $x, y \in G$. By the definition of φ we have

$$\begin{aligned} \varphi(xy) &= y^{-1}x^{-1} \\ &= \varphi(x)\varphi(y) \\ &= x^{-1}y^{-1} \end{aligned}$$

Hence $y^{-1}x^{-1} = x^{-1}y^{-1}$ for every $x, y \in G$. Thus, G is abelian.

Now suppose G is abelian. Then for every $x, y \in G$, we have that

$$xy = yx$$

Define the map $\varphi : G \rightarrow G$ by $\varphi : g \rightarrow g^{-1}$

Then we have,

$$\begin{aligned}\varphi(xy) &= (xy)^{-1} \\ &= y^{-1}x^{-1}\end{aligned}$$

and

$$\varphi(x)\varphi(y) = x^{-1}y^{-1}$$

Since G abelian, we can rewrite

$$\begin{aligned}\varphi(x)\varphi(y) &= x^{-1}y^{-1} \\ &= y^{-1}x^{-1}\end{aligned}$$

Hence we have that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$, so φ is a homomorphism. \square

- (b) Let $\varphi : G \rightarrow H$ be an isomorphism of groups. For the following, you may use the facts that (1) a function is a bijection if and only if it has an inverse, and (2) an invertible function is a homomorphism if and only if its inverse is a homomorphism (which implies that $G \cong H$ if and only if $H \cong G$).

- (i) Show $|G| = |H|$.

Proof. Since $\varphi : G \rightarrow H$ is an isomorphism, we know that it is a bijection from G to H . Suppose $|G| < |H|$. Since φ is injective, then each element of G is mapped to exactly one element of H .

Since $|H| > |G|$, there exists $y \in H$ such that there is no $x \in G$ with $\varphi(x) = y$. However, we assumed φ was bijective, so this cannot be the case. So $|G| \geq |H|$.

However, now assume that $|G| > |H|$. Since φ is a bijection, we can take the inverse bijection φ^{-1} and apply the same argument as above. Thus, $|H|$ cannot be greater than $|G|$.

As a result, the only remaining option is that $|G| = |H|$. \square

- (ii) Show G is abelian if and only if H is also abelian.

Proof. Suppose G is abelian. Then $\forall x, y \in G$, we have $xy = yx$. Thus, we have

$$\varphi(xy) = \varphi(yx) \tag{1}$$

In addition, by the definition of φ as an isomorphism, we have that $\varphi(xy) = \varphi(x)\varphi(y)$ and $\varphi(yx) = \varphi(y)\varphi(x)$.

Hence, from (1) and the above, we get

$$\varphi(x)\varphi(y) = \varphi(y)\varphi(x)$$

for every $x, y \in G$. Since φ is a bijection, for every element $y \in H$, $\exists x_y \in G$ such that $\varphi(x_y) = y$. Hence, this shows that H is an abelian group as well.

Now suppose H is abelian. Consider φ^{-1} , which is a bijection from $H \rightarrow G$ and a homomorphism (hence an isomorphism). Then we can apply the same argument as above, just swapping the H and G .

Hence, H abelian $\implies G$ abelian, and we get G abelian $\iff H$ abelian.

□

(iii) Show that for any $g \in G$, $|g| = |\varphi(g)|$. [Show $g^n = 1$ if and only if $\varphi(g)^n = 1$.]

Proof. Suppose $g^n = 1$.

Then $\varphi(g^n) = \varphi(1)$.

Note that for every $x \in G$, we have

$$\begin{aligned}\varphi(1x) &= \varphi(1)\varphi(x) \\ &= \varphi(x)\end{aligned}$$

Hence $\varphi(g^n) = \varphi(1)$ must map to the identity in H (ie. 1).

In addition, we have

$$\begin{aligned}\varphi(g^n) &= \varphi(g \cdot g \cdots g) \\ &= \varphi(g) \cdot \varphi(g) \cdots \varphi(g) \\ &= \varphi(g)^n \\ &= 1\end{aligned}$$

as required.

Now suppose $\varphi(g)^n = 1$. Then

$$\begin{aligned}\varphi(g)^n &= \varphi(g) \cdot \varphi(g) \cdots \varphi(g) \\ &= \varphi(g^n) = 1\end{aligned}$$

So $g^n = 1$ if and only if $\varphi(g)^n = 1$.

Thus, if $g^m \neq 1$ for some m , then $\varphi(g)^m \neq 1$ as well. So if $|g| = n$, then every power g^k with $k \in \{1, \dots, n-1\}$ is such that $g^k \neq 1$ and $\varphi(g)^k \neq 1$

In addition, from what we have proved above, we have $g^n = 1 \implies \varphi(g)^n = 1$. Since we showed that neither g^k nor φ^k are 1 for any $k \in \{1, \dots, n-1\}$, we have that $|g| = |\varphi(g)| = n$ \square

(c) Show that the following groups are *not* isomorphic. [If you use the previous part, these will all be short answers.]

(i) The multiplicative groups \mathbb{R}^\times and \mathbb{C}^\times ;

Answer. There are only 2 elements in \mathbb{R}^\times with order less than ∞ : $|1| = 1$ and $|-1| = 2$. However, there are 4 in \mathbb{C}^\times : $|1| = 1$, $|-1| = 2$, $|i| = 4$, $|-i| = 4$.

Since there are no elements in \mathbb{R}^\times with order 4, these two groups cannot be isomorphic.

.....

(ii) $\mathbb{Z}/24\mathbb{Z}$ and S_4 ;

Answer. We know that $\mathbb{Z}/24\mathbb{Z}$ is abelian since

$$\begin{aligned}\bar{x} + \bar{y} &= \overline{x + y} \\ &= \overline{y + x} \\ &= \bar{y} + \bar{x}\end{aligned}$$

for every $\bar{x}, \bar{y} \in \mathbb{Z}/24\mathbb{Z}$. However, S_4 is not abelian because

$$(23)(13) = (123)$$

but

$$(13)(23) = (132)$$

.....

(iii) $D_{2 \cdot 12}$ and S_4 ;

Answer. The order of $r \in D_{2 \cdot 12}$ is 12. However, there is no element in S_4 with order 12.

.....

(iv) S_m and S_n , with $m \neq n$.

Answer. We have $|S_m| = m!$ and $|S_n| = n!$. Since $n \neq m$, we have $|S_m| \neq |S_n|$

.....

3. **Direct Products.** As defined in Example 6 on page 18, if (A, \star) and (B, \diamond) are groups, we can form a new group $A \times B$, called their *direct product*, whose elements are those in the Cartesian Product

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

and whose operation is defined component-wise:

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2).$$

For example, if $A = B = \mathbb{R}$ and $\star = \diamond = +$, then $\mathbb{R} \times \mathbb{R}$ is the familiar \mathbb{R}^2 .

(a) Verify the group axioms for $A \times B$.

Proof. Let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B$. Then,

$$\begin{aligned} [(a_1, b_1) \cdot (a_2, b_2)] \cdot (a_3, b_3) &= (a_1 a_2, b_1 b_2) \cdot (a_3, b_3) \\ &= (a_1 a_2 a_3, b_1 b_2 b_3) \\ &= (a_1, b_1) \cdot (a_2 a_3, b_2 b_3) \\ &= (a_1, b_1) \cdot [(a_2, b_2) \cdot (a_3, b_3)] \end{aligned}$$

Now let $1 = (1, 1)$. Then,

$$\begin{aligned} (a_1, b_1) \cdot (1, 1) &= (a_1 \cdot 1, b_1 \cdot 1) \\ &= (a_1, b_1) \end{aligned}$$

and

$$\begin{aligned} (1, 1) \cdot (a_1, b_1) &= (1 \cdot a_1, 1 \cdot b_1) \\ &= (a_1, b_1) \end{aligned}$$

Finally, we know that if $a_1, b_1 \in \mathbb{R}$, then $a_1^{-1}, b_1^{-1} \in \mathbb{R}$. Let $(a_1, b_1)^{-1} = (a_1^{-1}, b_1^{-1})$. Then,

$$\begin{aligned} (a_1, b_1)^{-1} \cdot (a_1, b_1) &= (a_1^{-1}, b_1^{-1}) \cdot (a_1, b_1) \\ &= (a_1^{-1} a_1, b_1^{-1} b_1) \\ &= (1, 1) \end{aligned}$$

and,

$$\begin{aligned} (a_1, b_1) \cdot (a_1, b_1)^{-1} &= (a_1, b_1) \cdot (a_1^{-1}, b_1^{-1}) \\ &= (a_1 a_1^{-1}, b_1 b_1^{-1}) \\ &= (1, 1) \end{aligned}$$

Hence, $A \times B$ is a group. □

- (b) Verify that $\pi : A \times B \rightarrow A$ defined by $(a, b) \mapsto a$ is a homomorphism, and compute its kernel. (Note: A similar proof would show that the projection $\pi_B : A \times B \rightarrow B$ defined by $(a, b) \mapsto b$ is a homomorphism, with a corresponding kernel.)

Proof. Let $(a_1, b_1), (a_2, b_2) \in A \times B$. Then,

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

Hence, φ is a homomorphism. □

- (c) Verify that $A \times 1 = \{(a, 1) \mid a \in A\}$ is a subgroup of $A \times B$ and that $A \times 1 \cong A$. (Note: A similar proof would show that $1 \times B$ is a subgroup of $A \times B$ isomorphic to B .)

Proof. We know that $A \times 1$ is non-empty because $1 \in A$, so $(1, 1) \in A \times 1$.

Now note that for every element $(a, 1) \in A \times 1$, we have that $a \in A$ and $1 \in B$. Hence, $A \times 1 \subset A \times B$.

Now let $(a_1, 1), (a_2, 1) \in A \times 1$. We have that $(a_2, 1)^{-1} = (a_2^{-1}, 1)$. We know $a_2^{-1} \in A$, so $(a_2^{-1}, 1) \in A \times 1$. Now consider,

$$(a_1, 1) \cdot (a_2^{-1}, 1) = (a_1 a_2^{-1}, 1)$$

Since A is a group and $a_1, a_2^{-1} \in A$, then $a_1 a_2^{-1} \in A$ and we have that $(a_1 a_2^{-1}, 1) \in A \times 1$.

As a result $A \times 1$ satisfies the subgroup criterion and hence $A \times 1 \leq A \times B$. □

4. Normalizers and Centralizers of subgroups.

Let $H \leq G$ (recall that \leq means “subgroup”).

(a) Show that $H \leq N_G(H)$.

Proof. Note that $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ □

(b) Give an example where A is not a subgroup of G and $A \not\leq N_G(A)$.

(c) Show $H \leq C_G(H)$ if and only if H is abelian.

(d) For any nonempty $A \subseteq G$, define $N_H(A) = \{h \in H \mid hAh^{-1} = A\}$. Show that $N_H(A) = H \cap N_G(A)$ and deduce $N_H(A) \leq H$.