

# Chapter 1

## Groups

### Definition 1.1

A group  $(G, *)$  is a set  $G$ , together with a binary operator  $*$  such that

Additive Group	Multiplicative Group
Let $G$ be a set, and $+$ be an operation, then $(G, +)$ is an additive group provided	Let $G$ be a set, and $\circ$ be an operation, then $(G, \circ)$ is a multiplicative group provided
1. $\forall a, b \in G, a + b \in G$	6. $\forall a, b \in G, a \circ b \in G$
2. $\forall a, b, c \in G, a + (b + c) = (a + b) + c$	7. $\forall a, b, c \in G, a \circ (b \circ c) = (a \circ b) \circ c$
3. $\forall a \in G, \exists 0 \in G$ (identity) s.t. $a + 0 = a = 0 + a$	8. $\forall a \in G, \exists 1 \in G$ (unity) s.t. $a \circ 1 = a = 1 \circ a$
4. $\forall a \in G, \exists -a \in G$ (additive inverse) s.t. $a + (-a) = 0 = (-a) + a$	9. $\forall a \in G, \exists a^{-1} \in G$ (unity) s.t. $a \circ a^{-1} = 1 = a^{-1} \circ a$
5. (Commutative) $\forall a, b \in G, a + b = b + a$	10. (Commutative) $\forall a, b \in G, a \circ b = b \circ a$

Joining additive and multiplicative groups together, we form a ring with **distributive laws**

$$11. \quad \forall a, b, c \in G, (a + b) \circ c = (a \circ c) + (b \circ c)$$

$$12. \quad \forall a, b, c \in G, c \circ (a + b) = (c \circ a) + (c \circ b)$$

- Abelian group: (1-5) or (6-10)
- Associative Ring: 1-6, with 11 and 12

- Semigroup: 1, 2 only
- Monoid: 1, 3 only
- Commutative ring: 1-5, 6, 10, 11, and 12
- Ring: 1-5, with 11 and 12
- Ring with unity: 1-6, with 8, 11, and 12
- Field: 1-12

**Lemma 1.1 Uniqueness of group identity**

In a group  $G$ , there is one and only one identity element  $e$ .

*Proof. For the sake of contradiction.* Suppose not, Suppose that  $e$  and  $e'$  are both identity elements of group  $G$ . Since  $e$  is an identity element of  $G$ , then  $e \in G$  and

$$ea = a = ae \quad \forall a \in G. \quad (\heartsuit)$$

Since  $e'$  is also an identity element of  $G$ . we said that  $e' \in G$  and

$$e'a = a = ae' \quad \forall a \in G. \quad (\clubsuit)$$

From  $(\heartsuit)$ , if we take  $a = e'$ , then  $e \cdot e' = e'$ .

From  $(\clubsuit)$ , if we take  $a = e$ , then  $e = e \cdot e'$ .

Combining the results we have  $e = e \cdot e' = e'$ , and so  $e = e'$ . There is only one identity element in  $G$ . We proved the uniqueness of identity.  $\square$

**Lemma 1.2 Cancellation rule**

In a group  $G$ ,  $ba = ca$  implies  $b = c$ ; and  $ab = ac$  implies  $b = c$ .

*Proof.* Consider  $G$  is a group, then

$$\forall a \in G, \exists a' \in G \quad s.t. \quad aa' = e = a'a.$$

To show the right cancellation works, we further consider  $ba = ca$ . Multiplying  $a'$  on both sides of the previous equation on right, we obtained

$$(ba)a' = (ca)a'$$

Then,  $b(aa') = c(aa')$  and so  $be = ce \Rightarrow \boxed{b = c}$ . The proof is now complete.  $\square$

**Theorem 1.1 Socks-shoes property**

$$(a \circ b)^{-1} = b^{-1} \circ a^{-1} \quad (1.1)$$

*Proof.* Since we know that  $G$  is a group, then  $ab \in G$  for all  $a, b \in G$  since  $G$  is closure. Next, we consider the following equation

$$\begin{aligned}
 (ab)(b^{-1}a^{-1}) &= a(bb^{-1})a^{-1} && G \text{ is associative} \\
 &= aea^{-1} \\
 &= aa^{-1} \\
 &= \boxed{e} && \text{cancellation rule returns identity}
 \end{aligned}$$

this equation states that

$$\boxed{(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1}} = e$$

now we cancel off  $ab$  from both sides of the equations, we now arrive at

$$(ab)^{-1} = b^{-1}a^{-1}$$

and we have done the proof.  $\square$

*Remark.* In abstract algebra, the position of inputs in binary operator is very important! The commutative property no necessary hold.  $a \circ b \neq b \circ a$ . E.g. matrix multiplication  $AB \neq BA$ .

**Example 1.0.1.** Consider  $(a, b)$  to be a fixed point on the 2-dimensional cartesian plane  $\mathbb{R}^2$ , we define a translation map  $T_{a,b} : \mathbb{R}^2 \rightarrow \mathbb{R}^2$  such that

$$T_{a,b}(x, y) = (x + a, y + b)$$

we again define  $G = \{T_{a,b} \mid a, b \in \mathbb{R}\}$ . Show that  $(G, \circ)$  is a group under function composition.

**Solution** 1. (Closure) We want to show:

$$\forall T_{a,b}, T_{c,d} \in G, \quad T_{a,b} \circ T_{c,d} \in G$$

We compute the composition

$$\begin{aligned}
 (T_{a,b} \circ T_{c,d})(x, y) &= T_{a,b}(T_{c,d}(x, y)) \\
 &= T_{a,b}(x + c, y + d) \\
 &= (x + a + c, y + b + d) \\
 &= (x + (a + c), y + (b + d)) && \text{assoiativity of ordinary addition} \\
 &= T_{a+c, b+d}(x, y)
 \end{aligned}$$

which closed under  $G$ .

2. ()

### Theorem 1.2

The following statements are equivalent.

1. Every subgroup of a cyclic group (multiplicative group) is cyclic.
2. If  $|\langle a \rangle| = n$ , then the order of any subgroup of  $\langle a \rangle$  is a divisor of  $n$ .
3. For each positive divisor  $k|n$ ,  $\langle a \rangle$  has exactly one subgroup of order  $k$ .  $\langle a^{n/k} \rangle$  if multiplicative group,  $\langle \frac{n}{k}a \rangle$  if additive group.

*Proof.* Let  $G$  be a cyclic group and  $H$  be a subgroup of  $G$ . We need to show that  $H$  is also cyclic. Example:  $H = \langle a^m \rangle$  s.t.  $m$  is the least positive integer.

By randomly pick integer  $b \in H$ ,  $b = a^k$ ,  $k \in \mathbb{Z}^+$ . By division algorithm,  $k = qm + r$ , where  $0 \leq r < m$ .

$$\begin{aligned} b = a^k &= a^{qm+r} = (a^m)^q a^r \Rightarrow a^r = (a^m)^{-q} b \in H \\ &\Rightarrow a^r \in H, \quad 0 \leq r < m \\ &\Rightarrow r = 0 \end{aligned}$$

□

## 1.1 Cyclic groups

Cyclic groups are groups in which every element is a power of some fixed element. In additive group, then every element is a multiple of some fixed element. For instance,

$$\underbrace{a + a + \cdots + a}_{n \text{ times}} = na, \quad n \text{ is integer}$$

### Definition 1.2 Generating subgroup

If  $G$  is a multiplicative group and  $g \in G$ , then the subgroup generated by element  $g$  is

$$\langle g \rangle = \{ \underbrace{a \cdot a \cdots a}_{n \text{ times}} \mid n \in \mathbb{Z} \} = \{ g^n \mid n \in \mathbb{Z} \} \quad (1.2)$$

If the group is abelian and is additive, then

$$\langle g \rangle = \{ \underbrace{a + a + \cdots + a}_{n \text{ times}} \mid n \in \mathbb{Z} \} = \{ ng \mid n \in \mathbb{Z} \} \quad (1.3)$$

*Remark.*  $\langle g \rangle$  is called a cyclic subgroup generated by  $g$  in group  $G$ . When  $G = \langle g \rangle$ , then  $G$  is called a cyclic group.

### Definition 1.3 Cyclic group

A group  $G$  is **cyclic** if  $G = \langle g \rangle$  for some  $g \in G$ .  $g$  is a **generator** of  $\langle g \rangle$ .

### Lemma 1.3

$\langle g \rangle$  is a subgroup of  $G$ .

*Proof.* We can use 2-step subgroup test to verify  $\langle g \rangle \leq G$ :

1. Since  $g \in \langle g \rangle \neq \emptyset$ .
2. For all  $g_1, g_2 \in \langle g \rangle$ , we have

$$g_1 = g^{n_1}, \quad g_2 = g^{n_2}$$

where  $n_1$  and  $n_2$  are integers. And since

$$g_1 g_2 = g^{n_1} g^{n_2} = g^{n_1+n_2}$$

and  $n_1+n_2 \in \mathbb{Z}$  implies that  $g_1 g_2 \in \langle g \rangle$ .

3. For all  $g_1 \in \langle g \rangle$ , we have  $g_1 = g^k$ , where  $k$  is integer. We compute the inverse

$$g_1^{-1} = (g^k)^{-1} = g^{-k}, \quad -k \in \mathbb{Z}$$

which tells us that  $g_1^{-1} \in \langle g \rangle$ .

Therefore, by 2-step subgroup test,  $\langle g \rangle$  is a subgroup of  $G$ .  $\square$

**Lemma 1.4**

If  $G$  is a cyclic group, then  $G$  is abelian.

*Proof.* Consider a cyclic group  $G$ . We want to show  $G$  is also an abelian group.

Since  $G$  is a group, we say

$$\forall g_1, g_2 \in G, \quad g_1 = g^{n_1}, \quad g_2 = g^{n_2}$$

where  $n_1$  and  $n_2$  are integers. In order to show that  $G$  is abelian, we need to show that the commutative law applied in group  $G$ .

now compute

$$\begin{aligned} g_1 g_2 &= a^{n_1} a^{n_2} \\ &= g^{n_1+n_2} \\ &= g^{n_2+n_1} && \text{commutative in normal addition} \\ &= g^{n_2} g^{n_1} = \boxed{g_2 g_1} \end{aligned}$$

thus  $G$  is an abelian group.  $\square$

**Definition 1.4**

The **center**,  $Z(G)$ , of a group  $G$  is a subset of elements in  $G$  that commute with every element of  $G$ , that is,

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}. \quad (1.4)$$

**Theorem 1.3**

The center of a group  $G$  is also a subgroup of  $G$ .

*Proof.* We use one-step subgroup test to verify:

1. Since we know that  $G$  is a group, certainly the identity  $e \in G$  and

$$ex = x = xe \quad \forall x \in G.$$

implies that  $e \in Z(G)$  and  $Z(G)$  is nonempty.

2. For any  $a_1, a_2$  in  $Z(G)$ , we need to show

$$a_1 a_2^{-1} \in Z(G).$$

Since  $Z(G)$  is the center, we have  $a_1 x = x a_1$  and  $a_2 x = x a_2$  for all  $x \in G$ . Proving  $a_1 a_2^{-1} \in Z(G)$  is equivalent to show

$$a_1 a_2^{-1} x = x a_1 a_2^{-1} \quad \forall x \in G$$

compute

$$\begin{aligned}
 a_1 a_2^{-1} x &= a_1 (a_2^{-1} x) && \text{Associativity of } Z(G) \\
 &= a_1 (x a_2^{-1}) && \text{Since } a_2^{-1} x = x a_2^{-1} \\
 &= (a_1 x) a_2^{-1} && \text{Associativity of } Z(G) \\
 &= (x a_1) a_2^{-1} && \text{Since } a_1 x = x a_1 \\
 &= \boxed{x a_1 a_2^{-1}}
 \end{aligned}$$

which is what we desired.

Therefore the center  $Z(G)$  is a subgroup of  $G$  by one-step subgroup test.  $\square$

### 1.1.1 Subgroup tests

#### Theorem 1.4 One step subgroup test

Suppose  $G$  is a multiplicative group and  $H \subseteq G$ . If

1.  $H \neq \emptyset$ ,
2.  $\forall a, b \in H, ab^{-1} \in H$

then  $H$  is a subgroup of  $G$ .

**Example 1.1.1.** Let

## 1.2 Sylow's theorem

#### Theorem 1.5

$C_5 \times C_2$  and  $C_{10}$  are two isomorphism classes.

*Proof.* From the *Third Sylow's theorem*, the number of Sylow 5-groups divides 2 and is  $1 \pmod{5}$ , so there is only one Sylow 5-group. And there is a normal subgroup  $K \trianglelefteq G$  such that  $|K| = 5$ .  $\square$

## 1.3 Automorphism

**Example 1.3.1.** Compute  $\text{Aut}(\mathbb{Z}_{10})$ .

**Solution** For any  $\alpha \in \text{Aut}(\mathbb{Z}_{10})$  and for any  $k \in \mathbb{Z}_{10}$ . We define  $k \mapsto k\alpha(1)$  such that

$$1 \mapsto \alpha_1 : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, \quad \alpha_1(x) = x$$

$$3 \mapsto \alpha_3 : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, \quad \alpha_3(x) = 3x$$

$$7 \mapsto \alpha_7 : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, \quad \alpha_7(x) = 7x$$

$$9 \mapsto \alpha_9 : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{10}, \quad \alpha_9(x) = 9x$$

In fact,  $\text{Aut}(\mathbb{Z}_{10})$  is isomorphic to  $U(10) = \{1, 3, 7, 9\}$ .  $\blacktriangleleft$

## 1.4 Cosets

**Example 1.4.1.** Consider  $G = \mathbb{Z}_9 = \{0, 1, 2, \dots, 8\}(\text{mod } 9)$ . We take a cyclic subgroup

$$H = \langle 3 \rangle = \{0, 3, 6\}$$

which came from  $(G, \oplus)$ . All **left cosets** of  $G$  with respect to  $H$  are  $\{H, 1 \oplus H, 2 \oplus H\}$  where

$$\begin{aligned} 0 \oplus H &= \{0 + 0, 0 + 3, 0 + 6\}(\text{mod } 9) = \{0, 3, 6\} = H \\ 1H &= 1 \oplus H = \{1 + 0, 1 + 3, 1 + 6\}(\text{mod } 9) = \{1, 4, 7\} \\ 2H &= 2 \oplus H = \{2 + 0, 2 + 3, 2 + 6\}(\text{mod } 9) = \{2, 5, 8\} \\ 3H &= 3 \oplus H = \{3 + 0, 3 + 3, 3 + 6\}(\text{mod } 9) = \{3, 6, 0\} = H \end{aligned}$$

As for the right cosets of  $G$  with respect to  $H$  are  $\{H, H \oplus 1, H \oplus 2\}$ . Pay attention that now the element of coset are being added to right-hand side instead of from left side.

$$\begin{aligned} 0 \oplus H &= \{0 + 0, 0 + 3, 0 + 6\}(\text{mod } 9) = \{0, 3, 6\} = H \\ H1 &= H \oplus 1 = \{0 + 1, 3 + 1, 6 + 1\}(\text{mod } 9) = \{1, 4, 7\} \\ H2 &= H \oplus 2 = \{0 + 2, 3 + 2, 6 + 2\}(\text{mod } 9) = \{2, 5, 8\} \\ H3 &= H \oplus 3 = \{0 + 3, 3 + 3, 6 + 3\}(\text{mod } 9) = \{3, 6, 0\} = H \end{aligned}$$

## 1.5 Normal subgroups, Quotient groups

### 1.5.1 Normal subgroups

#### Definition 1.5 Normal subgroups

A subgroup  $H$  of  $(G, \cdot)$  is called a normal subgroup if for all  $g \in G$  we have

$$gH = Hg. \tag{1.5}$$

We shall denote that  $H$  is a subgroup of  $G$  by  $H < G$ , and that  $H$  is a normal subgroup of  $G$  by  $H \triangleleft G$ .

If  $H$  is a normal subgroup of  $G$ , and the order of  $H$  is equal to the order of  $G$ , we called  $H$  the proper normal subgroup, write as  $H \trianglelefteq G$ .

You should be very careful here. The equality  $gH = Hg$  is a set equality. Not constants or numbers! It says that a right coset is equal to left a coset, it is not an equality elementwise.

**Example 1.5.1.** Let  $\mathbb{R}[x]$  denote the group of all polynomial with real coefficients under normal addition.

For any  $f$  in  $\mathbb{R}[x]$ , let  $f'$  denote the derivative of  $f$ . Then the mapping  $f \rightarrow f'$  is a homomorphism from  $\mathbb{R}[x]$  to itself. The kernel of the derivative mapping is the set of all constant polynomials  $f(x) = c$ .

Now suppose we have a group  $(G, \cdot)$ , and  $H$  is a normal subgroup of  $G$ , just said  $H \triangleleft G$ . The set  $G/H$  is defined by

$$G/H = \{gH \mid g \in G\}$$

#### Theorem 1.6 Orbit-Stabilizer theorem

For any group action  $\phi : G \rightarrow \text{Permutation}(S)$ , and for any  $s \in S$ ,

$$|\text{Orb}(s)| \cdot |\text{Stab}(s)| = |G|. \quad (1.6)$$

**Theorem 1.7**

The group of rotations of a cube is isomorphic to  $S_4$ .

## 1.6 Group homomorphisms

**Definition 1.6**

A group homomorphism is a map  $f : (G, \diamond_G) \rightarrow (H, \bullet_H)$  that respects binary operations:

$$f(a) \bullet_H f(b) = f(a \diamond_G b) \quad \forall a, b \in G \quad (1.7)$$

## 1.7 Tutorials

**Exercise 1.7.1** Prove whether the following group  $G$  together with operation  $*$  is a group.

1. Let  $*$  defined on  $G = \mathbb{R}$  by letting  $a * b = ab \quad \forall a, b \in \mathbb{R}$ .
2. Let  $*$  defined on  $G = 2\mathbb{Z}$  by letting  $a * b = a + b \quad \forall a, b \in 2\mathbb{Z}$ .
3. Let  $*$  defined on  $G = \mathbb{R}^\times$  by letting  $a * b = \sqrt{ab} \quad \forall a, b \in \mathbb{R}^\times$ .
4. Let  $*$  defined on  $G = \mathbb{Z}$  by letting  $a * b = \max(a, b) \quad \forall a, b \in \mathbb{Z}$ .

**Exercise 1.7.2** Determine whether the given set of matrices under the specified operation, matrix addition or multiplication, is a group.

1. All  $2 \times 2$  diagonal matrices under matrix addition.
2. All  $2 \times 2$  diagonal matrices under matrix multiplication.
3. All  $2 \times 2$  diagonal matrices with no zero diagonal entry under matrix multiplication.
4. All  $2 \times 2$  diagonal matrices with all diagonal entries either 1 or  $-1$  under matrix multiplication.
5. All  $2 \times 2$  upper-triangular matrices under matrix multiplication.
6. All  $2 \times 2$  upper-triangular matrices under matrix addition.
7. All  $2 \times 2$  upper-triangular matrices with determinant 1 under matrix multiplication.
8. All  $2 \times 2$  upper-triangular matrices with determinant either 1 or  $-1$  under matrix multiplication.



**Exercise 1.7.3** Prove whether

$$G = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid ad - bc \neq 0, a, b, c, d \in \mathbb{Z} \right\}$$

is a group under matrix multiplication.

**Exercise 1.7.4** Prove whether

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \mid ad \neq 0, a, b, d \in \mathbb{Z} \right\}$$

is a non-abelian group under matrix multiplication.

**Exercise 1.7.5** Prove whether

$$G = \left\{ \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} \mid a \neq 0, a, b \in \mathbb{Z} \right\}$$

is an abelian group under matrix multiplication.

**Exercise 1.7.6** Let  $(G, *)$  be a group and suppose that

$$a * b * c = e \quad \forall a, b, c \in G.$$

Show that  $b * c * a = e$ .

**Exercise 1.7.7** Show that if every element of the group  $G$  is its own inverse, then  $G$  is abelian.

**Exercise 1.7.8** Show that every group with identity  $e$  and  $x \cdot x = x$  for all  $x \in G$  is abelian.

**Exercise 1.7.9** Show that if  $G$  is a finite group with identity  $e$  and with even number of elements, then there is an  $a \neq e$  in  $G$  such that  $a * a = e$ .

**Exercise 1.7.10** Suppose  $G$  is a group such that

$$(ab)^2 = a^2 b^2 \quad \forall a, b \in G.$$

Show that  $G$  is abelian.

**Exercise 1.7.11** Find the order of the following cyclic groups.

1. The subgroup of  $U(6)$  generated by  $\cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$ .
2. The subgroup of  $U(5)$  generated by  $\cos\left(\frac{4\pi}{3}\right) + i\sin\left(\frac{4\pi}{3}\right)$ .
3. The subgroup of  $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$  generated by  $(1, 5)$ .

**Exercise 1.7.12** Let  $a$  and  $b$  be elements of a group  $G$ . Show that if  $ab$  has finite order  $n$ , then  $ba$  also has order  $n$ .

**Exercise 1.7.13** Show that a group with no proper nontrivial subgroup is cyclic.

**Exercise 1.7.14** Let  $G$  be a nonabelian group with center  $Z(G)$ . Show that there exists an abelian subgroup  $H$  of  $G$  such that  $Z(G) \subset H$  but  $Z(G) \neq H$ .

**Exercise 1.7.15** Find all subgroups of the following groups and draw the subgroups diagram for the subgroups. Hence, list all orders of the subgroups of the given groups.

1.  $\mathbf{Z}_{36}$
2.  $\mathbf{Z}_{60}$

**Exercise 1.7.16**

1. Find all the proper nontrivial subgroups of  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ .
2. Find all the subgroups of  $\mathbb{Z}_2 \times \mathbb{Z}_4$  of order 4.

**Exercise 1.7.17**

1. Are the groups  $\mathbb{Z}_2 \times \mathbb{Z}_{12}$  and  $\mathbb{Z}_4 \times \mathbb{Z}_6$  isomorphic?
2. Are the groups  $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$  and  $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40}$  isomorphic?

**Exercise 1.7.18** Find the conjugacy classes of dihedral group  $D_8$ .

**Exercise 1.7.19** Show that a group that has only finite number of subgroups must be a finite group.

**Exercise 1.7.20** Find all cosets of the subgroup  $4\mathbb{Z}$  of  $\mathbb{Z}$ .

**Exercise 1.7.21** Compute the quotient  $\mathbb{Z}_{12}/\langle 2 \rangle$ .

**Exercise 1.7.22** Show that if  $H$  is a subgroup of index 2 in a finite group  $G$ , then every left coset of  $H$  is also a right coset of  $H$ .

**Exercise 1.7.23** Let  $\phi : G \rightarrow G$  be a mapping defined by

$$\phi(x) = x^3 \quad \forall x \in G$$

where  $G = \mathbb{R} \setminus \{0\}$  is a group defined under usual multiplication. Show that  $\phi$  is a homomorphism, and hence find  $\ker(\phi)$ .

**Exercise 1.7.24** Let  $\phi : G \rightarrow G$  be a mapping defined by

$$\phi(x) = 5^x \quad \forall x \in G$$

where  $G = \mathbb{R} \setminus \{0\}$  is a group defined under usual multiplication. Show that  $\phi$  is a homomorphism, and hence find  $\ker(\phi)$ .

**Exercise 1.7.25** Let  $G$  be a group and  $g$  an element in  $G$ . Consider the mapping  $\phi : G \rightarrow G$  defined as  $\phi(x) = gxg^{-1}$ . Show that  $\phi$  is an isomorphism.

**Exercise 1.7.26** Find  $\ker(\phi)$  for map  $\phi : \mathbb{Z}_{10} \rightarrow \mathbb{Z}_{20}$  such that  $\phi(1) = 8$ .

**Exercise 1.7.27** Find  $\ker(\phi)$  for map  $\phi : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$  such that  $\phi(1, 0) = (2, -3)$  and  $\phi(0, 1) = (-1, 5)$ .

**Exercise 1.7.28** Let  $\phi : G \rightarrow H$  be a group homomorphism. Show that  $\phi(G)$  is abelian if and only if

$$xyx^{-1}y^{-1} \in \ker(\phi) \quad \forall x, y \in G.$$

**Exercise 1.7.29** Consider  $A$  the set of affine maps of  $\mathbb{R}$ , that is

$$A = \{f : x \mapsto ax + b, a \in \mathbb{R}^*, b \in \mathbb{R}\}$$

1. Show that  $A$  is a group with respect to the composition of map.

2. Let

$$N = \{g : x \mapsto x + b, b \in \mathbb{R}\}$$

Show that  $N \triangleleft A$ .

3. Show that the quotient group  $A/N$  is isomorphic to  $\mathbb{R}^*$ .

**Exercise 1.7.30** Let  $G = S_4$  and let

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$$

1. Show that  $H$  is a normal subgroup of  $G$ .

2. Let  $\overline{H} = \{\sigma \in S_4 \mid \sigma(4) = 4\}$ . Define  $\sigma : \overline{H} \rightarrow \text{Aut}(H)$  by  $\sigma(\tau) = \sigma\tau\sigma^{-1}$  for  $\sigma \in \overline{H}$ . Prove that

$$\overline{H} \ltimes_{\sigma} H \cong S_4.$$

**Exercise 1.7.31** Find (up to isomorphism) all abelian groups of order 45.

**Exercise 1.7.32** Show that any group of order  $p^2$  is abelian.

**Exercise 1.7.33** Let  $G$  be a group of order  $pq$ , where  $p$  and  $q$  are prime numbers. Show that every proper subgroup of  $G$  is cyclic.

**Exercise 1.7.34** If  $H, K \leq G$ , show that  $H \cap K \leq G$ .

**Exercise 1.7.35** If  $N \triangleleft G$  and  $H \leq G$ , show that  $NH \leq G$ .

**Exercise 1.7.36** If  $N_1, N_2 \triangleleft G$ , show that  $N_1 \cap N_2 \triangleleft G$ .

**Exercise 1.7.37** If  $N \triangleleft G$  and  $H \leq G$ , show that  $H \cap N \triangleleft G$ .