

# Group Theory

## Notes

Basu Dev Karki

# Content

<b>1</b>	<b>Subgroups</b>	<b>2</b>
1.1	Definitions and Examples . . . . .	2
1.2	Centralizers and Normalizers, Stabilizer and Kernels . . . . .	5
1.3	Cyclic and Cyclic Subgroups . . . . .	9
1.4	Subgroups Generated by Subsets of a Group . . . . .	14
<b>2</b>	<b>Quotients Groups and Homomorphism</b>	<b>18</b>
2.1	Definition and Examples . . . . .	18

# 1 Subgroups

First, we'll define some things which will come in handy later on.

## 1.1 Definitions and Examples

**Definition 1.1.** A subgroup  $H$  of  $G$  is subset of  $G$  such that every group axiom holds on  $H$  with the same group operation of  $G$ . If  $H$  is a subgroup of  $G$  we shall write  $H \leq G$ .

**Definition 1.2.** A *kernel* of a function  $\varphi : G \rightarrow H$  are groups, is the set

$$\ker(\varphi) = \{g \in G \mid \varphi(g) = e_H\}$$

where  $G$  and  $H$  are groups.

**Proposition 1.1.** A function  $\varphi : G \rightarrow H$  is injective if and only if  $\ker(\varphi) = \{0\}$ .

**Definition 1.3.** A group action is a function  $\mu : G \times A \rightarrow A$  such that

1.  $\mu(g_1, \mu(g_2, a)) = \mu(g_1 \cdot g_2, a)$
2.  $\mu(e, a) = a$

To make the notation simple enough, we abbreviate the notation of  $\mu(g, a)$  to  $g \cdot a$  or sometimes  $ga$ .

**Remark.** Instead of saying 'Group Action of  $G$  on  $A$ ', we saying group  $G$  acts on the set  $A$ .

**Definition 1.4.** Let group  $G$  act on set  $A$ . A *stabilizer of  $a$* , where  $a \in A$ , is a the set consisting of elements which fixes  $a$ . i.e

$$G_a = \{g \in G \mid g \cdot a = a\}$$

**Proposition 1.2.** The  $G_a$  is a subgroup of  $G$  for all  $a \in A$ .

**Proposition 1.3.** Let the group  $G$  act on a set  $A$ . The relation  $\sim$  defined on  $A$  by

$$a \sim b \iff a = hb \quad \text{for some } h \in G$$

is a equivalence relation.

**Definition 1.5.** For each  $a \in A$  the equivalence class under  $\sim$  is called *orbit of  $a$*  under action of  $G$ . Thus,

$$\mathcal{O}(a) = \{x \in A \mid x \sim a\} = \{ha \mid h \in G\}$$

**Definition 1.6.** Let  $G$  be an abelian group. Define

$$t = \{g \in G \mid |g| < \infty\}$$

and call it the torsion subgroup of  $G$ .

You can check that the set if a subgroup of  $G$ .

## Problems and Solutions

**Problem :** Find a non-abelian group  $G$  such that the set of all elements with finite order is not a subgroup of  $G$ .

*Solution :*  $G = GL_2(\mathbb{Q})$ . Take  $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  and  $b = \begin{pmatrix} 0 & 2 \\ 1/2 & 0 \end{pmatrix}$ .  
Here,  $|a| = |b| = 2$  but  $|ab| = \infty$ .

**Problem :** Let  $H$  and  $K$  be subgroups of  $G$ . Prove that  $H \cup K$  is a subgroup if and only if  $H \subseteq K$  or  $K \subseteq H$ .

*Solution :* The ( $\Leftarrow$ ) is pretty simple. For ( $\Rightarrow$ ), suppose neither of  $H \subseteq K$  or  $K \subseteq H$  is true. Then, there exists a element  $h, k$  s.t  $h \in H$  and  $h \notin K$  and  $k \in K$  and  $k \notin H$ . But since  $H \cup K$  is a subgroup,  $h \cdot k$  must be either in  $H$  or  $K$ . If  $h \cdot k \in H$  then  $h^{-1} \cdot (h \cdot k) \in H$  and if  $h \cdot k \in K$  then  $(h \cdot k) \cdot k^{-1} \in K$

**Problem :** Let  $F$  be any field. Define

$$SL_n(F) = \{A \in GL_n(F) \mid \det(A) = 1\}$$

(called the *special linear group*). Prove that  $SL_n(F) \leq GL_n(F)$ .

*Solution :* If we use some basic properties of determinants we should be able to prove that this is a subgroup of the general linear group. We know that,

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

From this basic fact, we should be able to verify every subgroup axiom.

**Problem :** Prove that the intersection of arbitrary amount of non-empty collection of subgroups of  $G$  is also a subgroup of  $G$ .

*Solution :* Let us suppose

$$K = \bigcap G_i$$

where  $G_i$  are the subgroups.

Let us take  $a \in K$ . Since,  $a \in K$  that implies that  $a \in G_i$ . Since, of them are subgroups  $a^{-1} \in G_i$  thus  $a^{-1} \in K$ . It's easy to see that  $e_G \in K$ . Associativity is also pretty easy to check. If  $a \in G$  and  $b \in G$  then  $ab \in G$  as  $a, b \in G_i$  which means  $ab \in G_i$ .

**Problem :** Let  $A$  be an abelian group and fix some  $n \in \mathbb{Z}$ . Prove that the following subsets are subgroup of  $A$ ,

1.  $\{a^n \mid a \in A\}$
2.  $\{a \in A \mid a^n = 1\}$

*Solution :* The problem can be easily solved if we know a facts about abelian group. Let  $a, b \in A$  then

1.  $(ab)^n = a^n b^n$
2.  $(a^{-1})^n = (a^n)^{-1}$  (This is true in general for all group  $A$ )

**Problem :** Let  $H$  be a subgroup of additive group of rational numbers with the property that  $1/x \in H$  for every non-zero element of  $x \in H$ . Prove that  $H = 0$  or  $H = \mathbb{Q}$ .

*Solution :* If  $H$  has no non-zero element then  $H = \{0\}$ . If  $H$  has a non-zero element  $x$  then  $x = \frac{a}{b}$  for some  $a, b \in \mathbb{Z}$ . Since,  $\frac{a}{b} \in H$  then  $a \in H$  because of the additive nature of  $H$ . Since,  $a \in H$  we have  $\frac{1}{a} \in H$ , thus  $1 \in H$  as  $a \cdot \frac{1}{a} = 1$ . Since,  $1 \in H$  we must have  $-1 \in H$  as well. Thus, every integer  $a$  is in  $H$ . Since,  $a \in H$  we have  $\frac{1}{a} \in H$  thus,  $\frac{b}{a} \in H$  for any  $b \in \mathbb{Z}$ . Thus, every rational number can be obtained by this method. Thus,  $\mathbb{Q} = H$ .

**Problem :** Show that  $\{x \in D_{2n} \mid x^2 = 1\}$  is not a subgroup of  $D_{2n}$  ( $n > 2$ ).

*Solution :* We know that  $(r^k s)^2 = 1$  for all  $0 \leq k \leq n$ . Thus,  $(r^k s)(r^j s) = r^k (s r^j) s = r^{k-j}$ . Thus  $r^k = r^j \implies k = j$ . But since  $n > 2$  we can take different  $k, j$ . Thus, the set is not closed and thus it cannot be a subgroup of  $D_{2n}$ .

**Remark.** Here, if you do not know about the Dihedral groups, then it might be little confusing but, essentially

$$D_{2n} = \{1, r, r^2, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}\}$$

This Dihedral group is the set of symmetries of a regular  $n$ -gon. You can check that

$$s r^k = r^{-k} s$$

## 1.2 Centralizers and Normalizers, Stabilizer and Kernels

We'll look at some important families of subgroups. Let  $A$  be any non-empty subset of  $G$ .

**Definition 1.7.** Define  $C_G(A) = \{g \in G \mid gag^{-1} = a \ \forall a \in A\}$ . This subset is called *centralizers* of  $A$  in  $G$ . The set is the collection of elements in  $G$  which commutes with every element of  $A$ .

**Proposition 1.4.**  $C_G(A) \leq G$

*Proof.* One can check that  $1 \in C_G(A)$ . Suppose  $x \in C_G(A)$ , then  $xax^{-1} = a \implies a = x^{-1}ax$ . Thus,  $x^{-1} \in C_G(A)$ . Let  $x, y \in C_G(A)$  then

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

Thus,  $xy \in C_G(A)$ . □

**Definition 1.8.** Define  $Z(G) = \{g \in G \mid gx = xg \ \forall x \in G\}$ . This is the set of elements in  $G$  such that it commutes with every other element of  $G$ . This is called the *center* of  $G$ .

**Remark.** You may notice that  $Z(G) = C_G(G)$ . Thus,  $Z(G) \leq G$ .

**Definition 1.9.** Define  $gAg^{-1} = \{gag^{-1} \in G \mid a \in A\}$ . Define the *normalizers* of  $A$  in  $G$  to be the set

$$N_G(A) = \{g \in G \mid gAg^{-1} = A\}$$

**Proposition 1.5.**  $N_G(A) \leq G$  and  $C_G(A) \leq N_G(A)$ .

*Proof.* Similar proof like **Proposition 1.4**. □

### Examples

1. Let  $G$  be abelian group. Then  $Z(G) = G$ , also  $N_G(A) = C_G(A) = G$ .
2. Let  $G = D_8$ . And let  $A = \{1, r, r^2, r^3\}$  be a subgroup of rotations in  $D_8$ . We show that  $C_{D_8}(A) = A$ . Since, powers of  $r$  commute with each other, we have  $A \leq C_{D_8}(A)$ . One can check  $s \notin C_{D_8}(A)$  as  $sr = r^{-1}s \neq rs$ . Now, if  $a \notin A$  and  $a \in D_8$  then  $a$  must be of the form  $sr^i$ . If  $a \in C_{D_8}(A)$  with  $a = sr^i$  then  $s = (sr^i)(r^{-i})$ , thus a contradiction.

### Stabilizer and Kernels of a Group Action

We have already seen what a stabilizer is, now let's look at what a kernel of a group action is.

**Definition 1.10.** A *kernel* of a group  $G$  acting on a set  $A$  is the set of elements in  $G$  such that it fixes every element in  $A$ . That is, if  $\phi : G \times A \rightarrow A$  is a group action then

$$\ker(\phi) = \{g \in G \mid g \cdot s = s \ \forall s \in A\}$$


---

**Proposition 1.6.** Kernel of a group action is a subgroup of the group  $G$ .

*Proof.* If  $g \in \ker(\phi)$  then  $g \cdot s = s \implies g^{-1} \cdot (g \cdot s) = g^{-1} \cdot s \implies s = g^{-1} \cdot s$ . Thus,  $g^{-1} \in \ker(\phi)$ . Similarly, you can verify other axioms.  $\square$

We'll see that the centralizers, normalizers and kernels are some special case of facts that stabilizer and kernels of actions are subgroups. Let  $S = P(G)$  be the collection of all the subsets of group  $G$ , and let  $G$  act on  $S$  by *conjugation* i.e

$$\phi : G \times S \rightarrow S \quad \text{where} \quad g \cdot A = gAg^{-1}$$

where  $gAg^{-1}$  is defined just like in **Definition 1.9**.

Under this action, the stabilizer of  $A$  is same as normalizer of  $A$  i.e  $N_G(A) = G_A$ . This is basically of the definition,  $N_G(A) = \{g \in G \mid gAg^{-1} = A\} = \{g \in G \mid g \cdot A = A\} = G_A$ . Thus,  $N_G(A) \leq G$ .

Next Let the group  $N_G(A)$  act on  $A \subseteq G$  by conjugation. One can check that the centralizer of  $A$  is the same as kernel of this action. Thus,  $C_G(A) = \ker(\phi) \leq N_G(A)$  and from the above argument  $C_G(A) \leq N_G(A) \leq G \implies C_G(A) \leq G$ . One can also check that  $G$  acting on  $G$  by conjugation has kernel same as the center of the group i.e  $Z(G)$  thus,  $Z(G) \leq G$

---

## Problems and Solutions

**Problem :** Prove that  $C_G(Z(G)) = G$  and  $N_G(Z(G)) = G$ .

*Solution :* We already know that  $C_G(Z(G))$  and  $N_G(Z(G))$  are the subgroups of  $G$ . Thus, if we prove every element of  $C_G(Z(G))$  and  $N_G(Z(G))$  is also an element of  $G$  then we're done. Let  $a \in Z(G)$ , then  $ga = ag$  for any  $g \in G$ . Thus,  $g \in C_G(Z(G))$ . Since,  $gZ(G)g^{-1} = \{gag^{-1} \mid a \in Z(G)\} = \{a \mid a \in Z(G)\} = Z(G)$ . Thus, for any  $g \in G$  we have  $gZ(G)g^{-1} = Z(G)$  which means that  $N_G(Z(G))$  collects all the  $g \in G$ . Thus,  $N_G(Z(G)) = G$ .

**Problem :** If  $A$  and  $B$  are the subsets of  $G$  such that  $A \subseteq B$  then  $C_G(B) \leq C_G(A)$ .

*Solution :* Every element of  $C_G(B)$  is in  $C_G(A)$  as  $xb = bx$  for all  $b \in B$  so  $xa = ax$  for all  $a \in A$  thus,  $x \in C_G(A)$ . Thus, we are done.

**Problem :** Let  $H$  be a subgroup of  $G$ .

1. Show that  $H \leq N_G(H)$ .
2. Show that  $H \leq C_G(H) \iff H$  is abelian.

*Solution :* For the first part,  $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ . If we let  $g \in H$  be an arbitrary element then  $\{ghg^{-1} \mid h \in H\} = H$ . This, can be proved by proving  $\varphi_g : H \rightarrow H$  is a bijection for  $g \in H$ . Since,  $g$  is arbitrary  $H \leq N_G(H)$ .

For the second part, if  $H$  is abelian then  $ga = ag$  for every  $a, g \in H$  thus  $H \leq C_G(H)$ . If  $H \leq C_G(H)$  then  $ga = ag$  for all  $a \in H$  and since  $H$  is a subgroup of  $C_G(H)$  every element of  $H$  is in  $C_G(H)$  that means  $ga = ag$  for every  $a, g \in H$ . Thus  $H$  is abelian.

**Problem :** Let  $n \in \mathbb{Z}$  and  $n \geq 3$ . Prove the following

1.  $Z(D_{2n}) = \{1\}$  if  $n$  is odd
2.  $Z(D_{2n}) = \{1, r^k\}$  if  $n = 2k$

*Solution :* We know that only elements that commute with powers of  $r$  are powers of  $r$ . Thus,  $r^i$  be the element that commutes with every element of  $D_{2n}$ . Then,  $r^i(sr^i) = (sr^i)r^i \implies r^i(r^{-i}s) = sr^{2i} \implies s = sr^{2i} \implies r^{2i} = 1 \implies n \mid i$  if  $n$  is odd. But  $i < n$  so  $i = 0$ . If  $n = 2k$  then  $n \mid 2i \implies 2i = nk$  but  $2i < 2n \implies 2 > k \implies k = 1$ . Thus  $i = n/2$ .

**Problem :** Let  $G = S_n$  and fix an  $i \in \{1, 2, 3, \dots, n\}$  and let  $G_i = \{\sigma \in G \mid \sigma(i) = i\}$ . Prove that  $G_i$  is a subgroup of  $G$  and find  $|G_i|$ .

*Solution :* The subgroup part of this is pretty easy. To find,  $|G_i|$  we fix the map  $i \rightarrow i$  and let the other maps vary. The number of ways to do this is  $(n-1)!$  and this is the size of the group.



**Problem :** For any subgroup  $H$  of  $G$  and for any non-empty subset of  $A$  in  $G$  define  $N_H(A) = \{h \in H \mid hAh^{-1} = A\}$ . Show that  $N_H(A) = N_G(A) \cap H$  and deduce that  $N_H(A)$  is a subgroup of  $H$ .

*Solution :*  $N_H(A)$  collects every  $h \in H$  for which  $hAh^{-1} = A$ .  $N_G(A) \cap H$  also collects  $h \in H$  for which  $hAh^{-1} = A$  thus  $N_G(A) \cap H = N_H(A)$ . To deduce  $N_H(A)$  is a subgroup of  $H$ , you can easily check the axioms.

**Problem :** Let  $H$  be a subgroup of order 2 in  $G$ . Show that  $N_G(H) = C_G(H)$ . Deduce that if  $N_G(H) = G$  then  $H \leq Z(G)$ .

*Solution :* Since,  $H$  has order 2  $H$  must be  $\{e, h\}$  where  $h \neq e$  and  $h^2 = e$ . Now, if  $gHg^{-1} = H$  then  $\{ghg^{-1} \mid g \in G\} = \{e, ghg^{-1}\} = \{e, h\} \implies gh = hg$ . Thus,  $N_G(H)$  collects  $g \in G$  which commutes with  $h$  which is exactly  $C_G(H)$ . For the second part, since  $N_G(H) = G$  that means  $h$  commutes with every  $g \in G$ . Thus,  $\{e, h\} \subseteq Z(G)$  and  $H \leq Z(G)$ .

**Problem :** Prove that  $Z(G) \leq N_G(A)$  for any subset  $A$  of  $G$ .

*Solution :* Since  $Z(G)$  collects every  $g \in G$  such that it commutes with every other element of  $G$ , it must commute with every element of  $A$ . Thus,  $gAg^{-1} = \{gag^{-1} \mid g \in Z(G)\} = \{a \mid g \in Z(G)\} = A$  which means every  $g \in Z(G)$  is also an element of  $N_G(A)$ .

### 1.3 Cyclic and Cyclic Subgroups

**Definition 1.11.** A group  $G$  is called *cyclic* if it can be generated by a single element i.e there is some  $x \in G$  such that  $H = \{x^n \mid n \in \mathbb{Z}\}$ . We write it as  $G = \langle x \rangle$  and say  $G$  is generated by  $x$ .

**Proposition 1.7.** If  $H = \langle x \rangle$  then  $|H| = |x|$ .

*Proof.* Suppose  $|x| = n < \infty$  then  $1, x, \dots, x^{n-1}$  are all distinct. Thus  $|H|$  is at least  $n$ . Now, using the division algorithm we can show that these are all of them.

Suppose now  $|x| = \infty$  then that means there is no finite  $n \in \mathbb{Z}$  s.t  $x^n = 1$ . If  $x^b = x^c$  then  $x^{b-c} = 1$  contradicting the fact that there is no  $n$  s.t  $x^n = 1$ . Thus, all of the powers of  $x$  are different and thus  $|H| = \infty$ .  $\square$

**Proposition 1.8.** Let  $G$  be a group and let  $x \in G$ . If  $x^m = 1$  for some  $m \in \mathbb{Z}$  then  $|x|$  divides  $m$ .

**Proposition 1.9.** Any two cyclic group of same order are isomorphic. More specifically,

1. If  $n \in \mathbb{Z}^+$  and  $\langle x \rangle$  and  $\langle y \rangle$  are both cyclic groups of order  $n$ , then the map

$$\begin{aligned} \varphi : \langle x \rangle &\rightarrow \langle y \rangle \\ x^k &\rightarrow y^k \end{aligned}$$

is well defined and is an isomorphism.

2. If  $\langle x \rangle$  is an infinite cyclic group then

$$\begin{aligned} \varphi : \mathbb{Z} &\rightarrow \langle x \rangle \\ k &\rightarrow x^k \end{aligned}$$

is well defined and is an isomorphism.

**Proposition 1.10.** Let  $G$  be a group, let  $x \in G$  and let  $a \in \mathbb{Z} \setminus \{0\}$  then

1. If  $|x| = \infty$  then  $|x^a| = \infty$
2. If  $|x| = n < \infty$  then  $|x^a| = \frac{n}{(n,a)}$

*Proof.* 1. is pretty simple. Suppose  $|x^a| = k$  then  $x^{ak} = 1$  now  $n \mid ak$ . Write  $(n, a) = d$  and  $n = du$  and  $a = dv$ . Then,  $du \mid dvk \implies u \mid k$ . But

$$\begin{aligned} x^a = x^{dv} &\implies (x^{du})^v = (x^n)^v = 1 \\ &\implies (x^a)^u = 1 \\ &\implies k \mid u \end{aligned}$$

. Thus,  $k = u \implies n = dk \implies k = \frac{n}{d} = \frac{n}{(n,a)}$ .  $\square$

**Proposition 1.11.** Let  $H = \langle x \rangle$ .

1. Assume  $|x| = \infty$ . Then  $H = \langle x^a \rangle \iff a = \pm 1$ .

2. Assume  $|x| = n < \infty$ . Then  $H = \langle x^a \rangle \iff (a, n) = 1$ . The number of generators of  $H$  is  $\varphi(n)$ .

*Proof.* For 1. we know  $x \in \langle x^a \rangle$  as  $\langle x^a \rangle = \langle x \rangle$  thus

$$x = x^{ak} \implies ak = 1 \implies a = \pm 1$$

For 2. we know  $H = \langle x^a \rangle \implies |H| = |x^a| \iff |x| = |x^a|$ ,

$$\iff \frac{n}{(n, a)} = n$$

$$\iff (n, a) = 1$$

Since, the number of positive integers less than  $n$  and co-prime to  $n$  are exactly  $\varphi(n)$ , thus the number of generators are exactly equal to  $\varphi(n)$ .  $\square$

**Theorem 1.1.** Let  $H = \langle x \rangle$  be a cyclic group.

1. Every subgroup of  $H$  is cyclic. More precisely, if  $K \leq H$ , then either  $K = \{1\}$  or  $K = \langle x^d \rangle$ , where  $d$  is the smallest positive integer such that  $x^d \in K$ .
2. If  $|H| = \infty$ , then for any distinct nonnegative integers  $a$  and  $b$ ,  $\langle x^a \rangle \neq \langle x^b \rangle$ .
3. If  $|H| = n < \infty$ , then for each positive integer  $a$  dividing  $n$  there is a unique subgroup of  $H$  of order  $a$ . This subgroup is the cyclic group  $\langle x^d \rangle$ , where  $d = \frac{n}{a}$ . Furthermore, for every integer  $m$ ,  $\langle x^m \rangle = \langle x^{(n, m)} \rangle$ , so that the subgroups of  $H$  correspond bijectively with the positive divisors of  $n$ .

*Proof.* 1. and 2. are pretty easy. For 3. the cyclic group  $\langle x^{n/a} \rangle$  has order  $a$ . To prove uniqueness, suppose  $K$  is any subgroup of  $H$  with order  $a$ , then  $\langle x^b \rangle = K$  where  $b$  is the smallest positive integer  $b$  s.t  $x^b \in K$  (this is from 1.). Thus,

$$|\langle x^{n/a} \rangle| = |\langle x^b \rangle| \implies \frac{n}{d} = a = \frac{n}{(n, b)}$$

$$\implies d = (n, b) \implies d \mid b$$

Hence,  $\langle x^b \rangle \leq \langle x^d \rangle$  and since they both have same order  $\langle x^b \rangle = \langle x^d \rangle$ .

For the assertion on 3., one can prove that  $\langle x^m \rangle \leq \langle x^{(n, m)} \rangle$  as  $(n, m) \mid n$ , and since they have same order  $\langle x^m \rangle = \langle x^{(n, m)} \rangle$ . This means that the number of subgroups has a bijection with the divisors of  $n$ .  $\square$

## Problems and Solutions

**Problem :** Find all subgroup of  $\mathbf{Z}_{45} = \langle x \rangle$ , giving a generator of each. Describe the containment between these subgroups.

*Solution :* There are exactly 6 different subgroups of  $\mathbf{Z}_{45}$ . Since there is a one to one correspondence between divisors of 45 and subgroups of  $\mathbf{Z}_{45}$  we can list all of them,

$$\{1\}, \langle r \rangle, \langle r^3 \rangle, \langle r^5 \rangle, \langle r^9 \rangle, \langle r^{15} \rangle$$

**Problem :** If  $x$  is an element of a finite group  $G$  and  $|x| = |G|$ . Prove that  $G = \langle x \rangle$ .

*Solution :* Let  $|x| = n$ . We know that  $\{1, x, \dots, x^{n-1}\}$  is a subgroup of  $G$ . Since, it is a subgroup and has the same order as  $G$  thus  $G = \{1, x, \dots, x^{n-1}\} = \langle x \rangle$ .

**Problem :** Let  $\mathbf{Z}_{48} = \langle x \rangle$  and use isomorphism  $\mathbb{Z}/48\mathbb{Z} \cong \mathbf{Z}_{48}$  with  $[1] \mapsto x$  to find all the subgroups of  $\mathbf{Z}_{48}$ .

*Solution :* If  $\langle [x] \rangle$  is a cyclic subgroup of  $\mathbb{Z}/48\mathbb{Z}$  then  $\langle \varphi([x]) \rangle$  is a subgroup of  $\mathbf{Z}_{48}$  where  $\varphi$  is the isomorphic map.

**Problem :** Let  $\mathbf{Z}_{48} = \langle x \rangle$ . For which integer  $a$  does the map  $\varphi_a$  defined by  $\varphi_a : [1] \mapsto x^a$  extends to an isomorphism from  $\mathbb{Z}/48\mathbb{Z}$  to  $\mathbf{Z}_{48}$ .

*Solution :* We already know it is an homomorphism as

$$\varphi([u] + [v]) = (x^a)^{u+v} = (x^a)^u (x^a)^v = \varphi([u])\varphi([v])$$

But to be an isomorphism  $x^{na}$  needs to cover  $\mathbf{Z}_{48}$  for all  $n \in \mathbb{Z}$ . Thus,

$$\begin{aligned} \mathbf{Z}_{48} = \langle x \rangle &= \langle x^a \rangle \\ \implies (48, a) &= 1 \end{aligned}$$

So, for all the  $a$  which are co-prime to 48 the map,  $\varphi_a$  is an isomorphism.

**Problem :** Let  $\mathbf{Z}_{36} = \langle x \rangle$ . For which integer  $a$  does the map  $\psi_a : [1] \mapsto x^a$  extend to an well defined homomorphism from  $\mathbb{Z}/48\mathbb{Z}$  onto  $\mathbf{Z}_{36}$ . Can  $\psi_a$  ever be surjective?

*Solution :* One can check that the map is a homomorphism. Now, we need to show that

$$[u] = [v] \implies \psi_a([u]) = \psi_a([v])$$

If  $[u] = [v]$  then  $u - v = 48m$

$$\begin{aligned} 1 = \psi_a([0]) &= \psi_a([u - v]) = x^{a(u-v)} = x^{48am} \\ \implies 36 &\mid 48am \\ \implies 3 &\mid am \end{aligned}$$

Since  $3 \mid am$  must hold for all integer  $m$ , if  $3 \nmid a$  then  $3 \mid m$  for all integer  $m$  which is clearly absurd thus  $3 \mid a$ . Thus,  $x^{48 \cdot 3k \cdot m} = 1$  as  $36 \mid 144km$ . Thus,

$$x^{a(u-v)} = 1 \implies x^{au} = x^{av} \implies \psi_a([u]) = \psi_a([v])$$

**Problem :** Find a presentation for  $\mathbf{Z}_n$  with one generator.

*Solution :*  $\mathbf{Z}_n = \langle r \mid r^n = 1 \rangle$ .

**Problem :** Show that if  $H$  is any group with  $h^n = 1$  then there exists a unique homomorphism from  $\mathbf{Z}_n = \langle x \rangle$  to  $H$  such that  $x \mapsto h$ .

*Solution :* Define  $\psi : \mathbf{Z}_n \rightarrow H$  by  $\psi(x^k) = h^k$ . This is a homomorphism and is unique because the output is completely determined by  $h$ .

**Problem :** Show that if  $H$  is any group and  $h$  is an element of  $H$ , then there is a unique homomorphism from  $\mathbb{Z}$  to  $H$  such that  $1 \mapsto h$ .

*Solution :* Define  $\psi : \mathbb{Z} \rightarrow H$  by  $\psi(k) = h^k$ . This is a homomorphism and is unique as the output is completely determined by  $h$ .

**Problem :** Let  $p$  be a prime and  $n$  be a positive integer. Show that if  $x$  is an element of the group  $G$  such that  $x^{p^n} = 1$  then  $|x| = p^m$  for some  $m \leq n$ .

*Solution :* We know that if  $x^n = 1$  then  $|x|$  must divide  $n$ . Thus,  $|x|$  must divide  $p^n$  but the only divisors of  $p^n$  are powers of  $p$ . Thus,  $|x| = p^m$  for some  $m \leq n$ .

**Problem :** Show that  $(\mathbb{Z}/2^n\mathbb{Z})^\times$  is not cyclic.

*Solution :* Consider  $\{1, -1\}$  and  $1, 1 + 2^{n-1}$ . They both are subgroups of order 2. But a cyclic group has exactly 1 subgroup of order  $d$ , where  $d$  is the divisor of order of the cyclic group  $G$ . But we found two distinct subgroups of the group with same order.

**Problem :** Let  $G$  be a finite group and let  $x \in G$ .

1. Prove that if  $g \in N_G(\langle x \rangle)$  then  $gxg^{-1} = x^a$  for some  $a \in \mathbb{Z}$ .
2. Prove conversely that if  $gxg^{-1} = x^a$  for some  $a \in \mathbb{Z}$  then  $g \in N_G(\langle x \rangle)$ . [Show first that  $gx^k g^{-1} = (gxg^{-1})^k = x^{ak}$  for any integer  $k$ , so that  $g\langle x \rangle g^{-1} \leq \langle x \rangle$ . If  $x$  has order  $n$ , show the elements  $gx^i g^{-1}$ ,  $i = 0, 1, \dots, n-1$ , are distinct, so that  $|g\langle x \rangle g^{-1}| = |\langle x \rangle| = n$  and conclude that  $g\langle x \rangle g^{-1} = \langle x \rangle$ .]

**Problem :** Let  $G$  be a cyclic group of order  $n$  and let  $k$  be an integer relatively prime to  $n$ . Prove that the map  $x \mapsto x^k$  is surjective. Use Lagrange's Theorem (Exercise 19, Section 1.7) to prove the same is true for any finite group of order  $n$ . (For such  $k$  each element has a  $k$ th root in  $G$ . It follows from Cauchy's Theorem in Section 3.2 that if  $k$  is not relatively prime to the order of  $G$  then the map  $x \mapsto x^k$  is not surjective.)

**Problem :** Let  $\mathbf{Z}_n$  be a cyclic group of order  $n$  and for each integer  $a$  let

$$\sigma_a : \mathbf{Z}_n \rightarrow \mathbf{Z}_n \quad \text{by} \quad \sigma_a(x) = x^a \quad \text{for all } x \in \mathbf{Z}_n.$$

1. Prove that  $\sigma_a$  is an automorphism of  $\mathbf{Z}_n$  if and only if  $a$  and  $n$  are relatively prime.
2. Prove that  $\sigma_a = \sigma_b$  if and only if  $a \equiv b \pmod{n}$ .

3. Prove that every automorphism of  $Z_n$  is equal to  $\sigma_a$  for some integer  $a$ .
  4. Prove that  $\sigma_a \circ \sigma_b = \sigma_{ab}$ . Deduce that the map  $a \mapsto \sigma_a$  is an isomorphism of  $(\mathbb{Z}/n\mathbb{Z})^\times$  onto the automorphism group of  $Z_n$  (so  $\text{Aut}(Z_n)$  is an abelian group of order  $\varphi(n)$ ).
-

## 1.4 Subgroups Generated by Subsets of a Group

**Proposition 1.12.** If  $\mathcal{A}$  is any non empty collection of subsets of  $G$  then the intersection of all members of  $\mathcal{A}$  is also a subgroup of  $G$ .

*Proof.* Trivial. □

**Definition 1.12.** If  $A$  is any subset of group  $G$  define

$$\langle A \rangle = \bigcap_{\substack{A \subseteq H \\ H \leq G}} H$$

This is called subgroup generated by  $A$ .

**Definition 1.13.** Let  $A = \{a_1, \dots, a_n\}$  then define

$$\bar{A} = \{a_1^{\epsilon_1} a_2^{\epsilon_2} \cdots a_n^{\epsilon_n} \mid n \in \mathbb{Z}_{\geq 0}, a_i \in A, \epsilon_i = \pm 1\}$$

where  $\bar{A} = \{1\}$  if  $A = \emptyset$ .

**Remark.** Here,  $a_i$ 's need not to be distinct.

**Proposition 1.13.**  $\bar{A} = \langle A \rangle$

*Proof.* First we prove that  $\bar{A}$  is a subgroup. Note that  $\bar{A} \neq \emptyset$ . If  $a, b \in \bar{A}$  then write  $a = a_1^{\epsilon_1} \cdots a_n^{\epsilon_n}$  and  $b = b_1^{\delta_1} \cdots b_m^{\delta_m}$  then one can check that  $ab^{-1} \in \bar{A}$ . Thus,  $\bar{A}$  is a subgroup of  $G$ .

Now, since  $A \subseteq \bar{A}$  as  $a = a^1$  for every  $a \in A$ , we can say that  $\langle A \rangle \subseteq \bar{A}$ . It is because  $\langle A \rangle$  is the intersection of all the subgroups containing  $A$ . Now, since  $\langle A \rangle$  contains  $A$  and is a group, it must contain every element of form  $a_1^{\epsilon_1} \cdots a_n^{\epsilon_n}$  thus  $\bar{A} \subseteq \langle A \rangle$ . This completes the proposition. □

## Problems and Solutions

1. Prove that if  $H$  is a subgroup then  $\langle H \rangle = H$ .

*Solution :* From the definition,

$$\langle H \rangle = \bigcap_{\substack{H \subseteq K \\ K \leq G}} K$$

Since,  $H \subseteq H$  and  $H \leq G$  thus  $\langle H \rangle \subseteq H$ . But also  $H \subseteq \langle H \rangle$ .

2. Prove if  $A$  is a subset of  $B$  then  $\langle A \rangle \leq \langle B \rangle$ . Give an example of  $A \subseteq B$  with  $A \neq B$  but  $\langle A \rangle = \langle B \rangle$ .

*Solution :* From the definition we have,

$$\langle B \rangle = \bigcap_{\substack{B \subseteq K \\ K \leq G}} K$$

Since,  $A \subseteq B$  we have  $\langle A \rangle \leq \langle B \rangle$ . For the example, take  $G = D_{16}$  and  $A = \{r\}$  and  $B = \{r, r^3\}$ .

3. Prove if  $H$  is an abelian subgroup of  $G$  then  $\langle H, Z(G) \rangle$  is abelian. Give an explicit example of a abelian subgroup  $H$  such that  $\langle H, C_G(H) \rangle$  is not abelian.

*Solution :* We know that,  $\bar{A} = \langle A \rangle$  thus

$$\langle H, Z(G) \rangle = \{a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} \mid e_i = \pm 1, n \in \mathbb{Z}_{\geq 0}, a_i \in H \cup Z(G)\}$$

So, if you take two elements from  $\langle H, Z(G) \rangle$ , they will commute thus  $\langle H, Z(G) \rangle$  is an abelian group. For the example, choose  $H = \{1, r^2\}$  and  $G = D_8$ .

3. Prove that  $H$  is a subgroup then  $H$  is generated by  $H - \{1\}$ .

*Solution :* Since, we know that  $\bar{A} = \langle A \rangle$  thus

$$\langle H - \{1\} \rangle = \{a_1^{\epsilon_1} \cdots a_n^{\epsilon_n} \mid a_i \in H - \{1\}, n \in \mathbb{Z}_{\geq 0}, \epsilon_i = \pm 1\}$$

Thus, for  $a \in H$  and  $a \neq 1$ ,  $a \in \langle H - \{1\} \rangle$  and also  $1 = a^1 a^{-1} \in \langle H - \{1\} \rangle$ . Also,  $a \in \langle H - \{1\} \rangle$  is just some combination of elements in  $H$  thus  $a \in H$ . Thus, we have

$$\langle H - \{1\} \rangle = H$$

4. Prove that the multiplicative group of positive rational numbers is generated by the set  $\left\{ \frac{1}{p} \mid p \text{ is a prime} \right\}$ .

*Solution :* Since,

$$\left\langle \left\{ \frac{1}{p} \mid p \text{ is a prime} \right\} \right\rangle = \left\{ \frac{p_1^{a_1} \cdots p_n^{a_n}}{q_1^{b_1} \cdots q_m^{b_m}} \mid p_i, q_i \in \mathbf{Primes} \right\} = \mathbb{Q}_{>0}$$



5. A group  $H$  is called *finitely generated* if there is a finite set  $A$  such that  $H = \langle A \rangle$ .
- (a) Prove that every finite group is finitely generated.
  - (b) Prove that  $\mathbb{Z}$  is finitely generated.
  - (c) Prove that every finitely generated subgroup of the additive group  $\mathbb{Q}$  is cyclic. [If  $H$  is a finitely generated subgroup of  $\mathbb{Q}$ , show that  $H \leq \langle \frac{1}{k} \rangle$ , where  $k$  is the product of all the denominators which appear in a set of generators for  $H$ .]
  - (d) Prove that  $\mathbb{Q}$  is not finitely generated.
6. Exhibit a proper subgroup of  $\mathbb{Q}$  which is not cyclic.
7. A subgroup  $M$  of a group  $G$  is called a *maximal subgroup* if  $M \neq G$  and the only subgroups of  $G$  which contain  $M$  are  $M$  and  $G$ .
- (a) Prove that if  $H$  is a proper subgroup of the finite group  $G$  then there is a maximal subgroup of  $G$  containing  $H$ .
  - (b) Show that the subgroup of all rotations in a dihedral group is a maximal subgroup.
  - (c) Show that if  $G = \langle x \rangle$  is a cyclic group of order  $n \geq 1$  then a subgroup  $H$  is maximal if and only if  $H = \langle x^p \rangle$  for some prime  $p$  dividing  $n$ .
8. This is an exercise involving Zorn's Lemma (see Appendix I) to prove that every nontrivial finitely generated group possesses maximal subgroups. Let  $G$  be a finitely generated group, say  $G = \{g_1, g_2, \dots, g_n\}$ , and let  $\mathcal{S}$  be the set of all proper subgroups of  $G$ . Then  $\mathcal{S}$  is partially ordered by inclusion. Let  $\mathcal{C}$  be a chain in  $\mathcal{S}$ .
- (a) Prove that the union,  $H$ , of all the subgroups in  $\mathcal{C}$  is a subgroup of  $G$ .
  - (b) Prove that  $H$  is a proper subgroup. [If not, each  $g_i$  must lie in  $H$  and so must lie in some element of the chain  $\mathcal{C}$ . Use the definition of a chain to arrive at a contradiction.]
  - (c) Use Zorn's Lemma to show that  $\mathcal{S}$  has a maximal element (which is, by definition, a maximal subgroup).
9. Let  $p$  be a prime and let
- $$Z = \{z \in \mathbb{C} \mid z^{p^m} = 1 \text{ for some } m \in \mathbb{Z}^+\}$$
- (so  $Z$  is the multiplicative group of all  $p$ -power roots of unity in  $\mathbb{C}$ ). For each  $k \in \mathbb{Z}^+$  let
- $$H_k = \{z \in Z \mid z^{p^k} = 1\}$$
- (the group of  $p^k$ th roots of unity). Prove the following:
- (a)  $H_k \leq H_m$  if and only if  $k \leq m$ .
  - (b)  $H_k$  is cyclic for all  $k$  (assume that for any  $n \in \mathbb{Z}^+$ ,  $\{e^{2\pi it/n} \mid t = 0, 1, \dots, n-1\}$  is the set of all  $n$ th roots of 1 in  $\mathbb{C}$ ).
  - (c) Every proper subgroup of  $Z$  equals  $H_k$  for some  $k \in \mathbb{Z}^+$  (in particular, every proper subgroup of  $Z$  is finite and cyclic).
  - (d)  $Z$  is not finitely generated.
-

**10.** A nontrivial abelian group  $A$  (written multiplicatively) is called *divisible* if for each element  $a \in A$  and each nonzero integer  $k$  there is an element  $x \in A$  such that  $x^k = a$ , i.e., each element has a  $k$ th root in  $A$  (in additive notation, each element is the  $k$ th multiple of some element of  $A$ ).

- (a) Prove that the additive group of rational numbers,  $\mathbb{Q}$ , is divisible.
- (b) Prove that no finite abelian group is divisible.

**11.** Prove that if  $A$  and  $B$  are nontrivial abelian groups, then  $A \times B$  is divisible if and only if both  $A$  and  $B$  are divisible groups.

## 2 Quotients Groups and Homomorphism

### 2.1 Definition and Examples

**Definition 2.1.** Let  $\varphi : G \rightarrow H$  be a homomorphism. A *fiber* over  $a$ , where  $a \in \text{im}(\varphi)$ , is the set of elements in  $G$  that gets mapped to  $a$  under  $\varphi$  i.e

$$X_a = \{g \in G \mid \varphi(g) = a\}$$

It is also denoted by  $\varphi^{-1}(a)$ .

**Definition 2.2.** We define the product of *fibers* as following

$$X_a \cdot X_b = \{g_1 g_2 \mid g_1 \in X_a, g_2 \in X_b\}$$

**Remark.** By definition of the product of fibers, we can see that

$$X_a \cdot X_b = X_{ab}$$

**Proposition 2.1.** The set of *fibers* over the elements of  $\text{im}(\varphi)$  forms a group.

*Proof.* The identity element of the set is going to be  $X_{1_H}$ . The inverse of  $X_a$  is going to be  $X_{a^{-1}}$ . And one can check that the associativity the closure property holds.  $\square$

**Definition 2.3.** If  $\varphi$  is a homomorphism  $\varphi : G \rightarrow H$ , the *kernel* of  $\varphi$  is the set

$$\{g \in G \mid \varphi(g) = 1_H\}$$

and will be denoted by  $\ker \varphi$ .

**Remark.** The kernel of  $\varphi$  is the same as the fiber over  $1_H$  i.e

$$\ker \varphi = X_{1_H}$$

**Definition 2.4.** Let  $\varphi : G \rightarrow H$  be a homomorphism with kernel  $K$ . The *quotient group* or the *factor group*,  $G/K$  (read as  $G \bmod K$ ), is the group whose elements are the *fibers* of  $\varphi$ .

**Proposition 2.2.** Let  $\varphi : G \rightarrow H$  be a homomorphism of groups with kernel  $K$ . Let  $X \in G/K$  be the fiber above  $a$ . i.e  $X = \varphi^{-1}(a)$

1. For any  $u \in X$ ,  $X = \{uk \mid k \in K\} = uK$
2. For any  $u \in X$ ,  $X = \{ku \mid k \in K\} = Ku$

*Proof.* We'll prove 2. and leave 1. for the future me. Suppose  $k \in K$  then

$$\begin{aligned} \varphi(ku) &= \varphi(k)\varphi(u) \\ &= 1 \cdot \varphi(u) \\ &= a \end{aligned}$$

Thus,  $ku \in X \implies Ku \subseteq X$ . Now, to show  $X \subseteq Ku$ , take any  $g \in X$  then define  $k := gu^{-1}$  thus

$$\begin{aligned} \varphi(k) &= \varphi(gu^{-1}) = aa^{-1} = 1 \\ &\implies k \in K \end{aligned}$$

Thus,  $g = ku \in Ku \implies X \subseteq Ku$ .  $\square$

**Remark.** Any coset (check below for the definition) is also an *fiber* for some element. It is because

$$uK = \varphi^{-1}(\varphi(u)) = uK$$

**Definition 2.5.** For a  $N \leq G$  and any  $g \in G$  let

$$gN = \{gn \mid n \in N\} \quad \text{and} \quad Ng = \{ng \mid n \in N\}$$

be the *left coset* and *right coset* of  $N$  in  $G$ . Any element of a coset is called a *representative* of the coset.

**Remark.** To verify a map is a well defined map, one can't just use the condition imposed on the map. For example, the proof of the theorem below, I have said the operation is indeed well-defined but didn't prove it. You can't go about doing the following.

Let  $uK = u'K$  and  $vK = v'K$  thus

$$\begin{aligned} (uv)K &= (uK)(vK) \\ &= (u'K)(v'K) \\ &= (u'v')K \end{aligned}$$

Here, you're assuming that  $a = b \implies f(a) = f(b)$  which is true if  $f$  were to be a function. But to be a function, it needs to be well defined. Therefore you're assuming it's well defined to begin with.

**Theorem 2.1.** Let  $G$  be a group and let  $K$  be the kernel of some homomorphism from  $G$  to another group. Then the set whose elements are left cosets of  $K$  in  $G$  with operation defined by

$$(uK) \circ (vK) = (uv)K$$

forms a group,  $G/K$ .

*Proof.* One can check that the set whose elements are left cosets of  $K$  in  $G$  with operation defined above, does indeed form a group. Note that the operation is also well defined. Now, if  $X$  and  $Y$  are fibers then  $Z = XY$  is also a fiber. Now, we can write each fiber as

$$X = uK, \quad Y = vK, \quad XY = jK$$

But we set  $j = uv$  as  $uv \in XY$ . Thus, every element of  $G/K$  is in set  $\{uK \mid u \in G\}$ . But we also that every coset is also a fiber thus, every element of  $\{uK \mid u \in G\}$  is in  $G/K$ .  $\square$