Group Theory

Nirjhar Nath
nirjhar@cmi.ac.in

Contents

1 Introduction to Groups

1.1 Definition and Examples

Definition 1. A *binary operation* $*$ on a set S is a function $* : S \times S \to S$. For any $a, b \in S$, we write $a * b$ for $*(a, b)$. We say S is *closed* under $*$ if $a * b \in S \; \forall \; a, b \in S$.

Definition 2. A *group* is a set G with a binary operation $*$ on G, satisfying the following properties:

1. $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3) \; \forall \; g_1, g_2, g_3 \in G$, i.e., $*$ is associative.
2. $\exists \; e \in G$, called the *identity* of G, such that $\forall \; g \in G$, we have $g * e = e * g = g$.
3. For each $g \in G$, $\exists$ an element $g^{-1} \in G$, called the *inverse* of g, such that $g * g^{-1} = g^{-1} * g = e$.

We say $(G, *)$ is a group. Less formally, we might also say that G is a group under $*$ if $(G, *)$ is a group (or simply G is a group when the operation $*$ is clear from the context). We see some examples below:

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are groups under $+$ with $e = 0$ and $a^{-1} = -a \; \forall \; a$.
2. $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q}^+, \mathbb{R}^+$ are groups under $\times$ with $e = 1$ and $a^{-1} = \frac{1}{a} \; \forall \; a$. However, $\mathbb{Z} - \{0\}$ is not a group under $\times$ because the element 2, for instance, does not have an inverse in $\mathbb{Z} - \{0\}$.
3. Define $S_3 :=$ set of all bijections from $\{1, 2, 3\}$ to $\{1, 2, 3\} = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, where

$$f_1 := \begin{cases} 1 \longrightarrow 1 \\ 2 \longrightarrow 2 \\ 3 \longrightarrow 3 \end{cases} \quad f_2 := \begin{cases} 1 \longrightarrow 2 \\ 2 \longrightarrow 1 \\ 3 \longrightarrow 3 \end{cases} \quad f_3 := \begin{cases} 1 \longrightarrow 3 \\ 2 \longrightarrow 2 \\ 3 \longrightarrow 1 \end{cases}$$

$$f_4 := \begin{cases} 1 \longrightarrow 1 \\ 2 \longrightarrow 3 \\ 3 \longrightarrow 2 \end{cases} \quad f_5 := \begin{cases} 1 \longrightarrow 2 \\ 2 \longrightarrow 3 \\ 3 \longrightarrow 1 \end{cases} \quad f_6 := \begin{cases} 1 \longrightarrow 3 \\ 2 \longrightarrow 1 \\ 3 \longrightarrow 2 \end{cases}$$

   Then S_3 is a group under composition $\circ$, i.e., $(S_3, \circ)$ is a group. Defining S_n similarly, we have $(S_n, \circ)$, in general, is a group, called the *symmetry group on n letters.*

4. Fix $n \in \mathbb{Z}^+$. Define $\theta_n := \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. Then

$$\theta_n^n = \left(\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \right)^n = \cos(2\pi) + i \sin(2\pi) = 1$$

   We say θ_n is a *primitive n^{th} root of unity* (n^{th} root of unity because $\theta_n^n = 1$ and primitive because $\theta_n^m \neq 1$ if $0 < m < n$). Now define $G_n := \{1, \theta_n, \theta_n^2, \ldots, \theta_n^{n-1}\}$. Note that $(G_n, \times)$ is a group, called the *group of n^{th} roots of unity*, where the operation $\times$ is the multiplication of complex numbers.

5. $\mathcal{M}_{m \times n}(\mathbb{R}) :=$ set of $m \times n$ real matrices, is a group under addition of matrices, with identity as zero matrix and inverse as the negative of a matrix. However, $\mathcal{M}_{m \times n}(\mathbb{R})$ is not a group under multiplication of matrices, because $m \times n$ matrices cannot be multiplied unless $m = n$. But $\mathcal{M}_n(\mathbb{R}) :=$ set of $n \times n$ real matrices, is also not a group under multiplication because inverses do not exist in general. However, $GL_n(\mathbb{R}) :=$ set of invertible $n \times n$ real matrices, is a group under multiplication of matrices.

Definition 3. A group $(G, *)$ is called *abelian* or *commutative* if $g_1 * g_2 = g_2 * g_1 \ \forall \ g_1, g_2 \in G$.

For example, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are abelian groups under addition and $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}, \mathbb{Q} - \{0\}, \mathbb{R} - \{0\}$ are abelian groups under multiplication, whereas S_n is not abelian for $n \geq 3$ (S_1, S_2 are abelian).

Definition 4. A group G is called *finite* if the number of elements in G is finite.

For example, S_n is finite $\forall \ n \geq 1$ and it has $n!$ elements.

Definition 5. If G is a finite group, then the *order* of G, denoted by $|G|$, is defined to be the number of elements of G.

Definition 6. Let $G = \{g_1, g_2, \ldots, g_n\}$ be a finite group with $g_1 = e$. The *multiplication table* or *group table* of G is the $n \times n$ matrix whose $(i, j)^{\text{th}}$ entry is $g_i * g_j \in G$.

For example, the group table of S_3 is the matrix

$$\begin{pmatrix} f_1 & f_2 & f_3 & f_4 & f_5 & f_6 \\ f_2 & f_1 & f_5 & f_6 & f_3 & f_4 \\ f_3 & f_6 & f_1 & f_5 & f_4 & f_2 \\ f_4 & f_5 & f_6 & f_1 & f_2 & f_3 \\ f_5 & f_4 & f_2 & f_3 & f_6 & f_1 \\ f_6 & f_3 & f_4 & f_2 & f_1 & f_5 \end{pmatrix}$$

1.2 Properties of groups

It is tiresome to keep writing the $*$ for the product in G, so from now on we shall write the product $a * b$ as $a \cdot b$ or simply $ab \ \forall a, b \in G$.

Proposition 1 (Cancellation property). If G is a group and $a, b, c \in G$ such that $ab = ac$, then $b = c$.

Proof. We have,

$$\begin{aligned} & ab = ac \\ \implies & a^{-1}(ab) = a^{-1}(ac) \\ \implies & (a^{-1}a)b = (a^{-1}a)c \qquad \text{(using associativity)} \\ \implies & eb = ec \\ \implies & b = c \end{aligned}$$

A similar argument shows that $ba = ca \implies b = c$. □

Proposition 2. Let $g_1, g_2 \in G$. Suppose $g_1 g_2 = e$, then $g_2 g_1 = e$.

Proof. We have,

$$\begin{aligned} & g_1 g_2 = e \\ \implies & g_2(g_1 g_2) = g_2 e \\ \implies & (g_2 g_1) g_2 = e g_2 \\ \implies & g_2 g_1 = e \qquad \text{(using cancellation property)} \end{aligned}$$

Thus, if $g_1 g_2 = e$, then $g_2 = (g_1)^{-1}$ and $g_1 = (g_2)^{-1}$. □

Proposition 3. If G is a group, then

1. G has a unique identity.
2. Every $g \in G$ has a unique inverse $g^{-1} \in G$.
3. If $g \in G$, then $(g^{-1})^{-1} = g$.
4. For $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$.

Proof. 1. Suppose G has two identities e and e'. Then since e and e' are both identities, so $ee = e = ee'$ and hence by cancellation property, we have $e = e'$.

2. Suppose g has two inverses g_1 and g_2, then $gg_1 = e = gg_2$ and hence by cancellation property, we have $g_1 = g_2$.
3. Since $g^{-1} \in G$, so $g^{-1}(g^{-1})^{-1} = e = g^{-1}g$, so by cancellation property, we have $(g^{-1})^{-1} = g$.
4. We have,

$$\begin{aligned}(gh)(h^{-1}g^{-1}) &= ((gh)h^{-1})g^{-1} && \text{(using associativity)}\\ &= (g(hh^{-1}))g^{-1} && \text{(again using associativity)}\\ &= (ge)g^{-1} = gg^{-1} = e\end{aligned}$$

□

□

1.3 Some exercises

1. Check whether the following are groups:

(i) $(\mathbb{Z}, *)$, with $*$ defined as $a * b = a - b \; \forall \; a, b \in \mathbb{Z}$.

(ii) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ under $*$, defined as $a * b = a + b + ab$.

(iii) $G = \left\{\frac{a}{b} \in \mathbb{Q} : (a, b) = 1 \text{ and } 5 \mid b\right\}$ under addition.

(iv) $G' = \left\{\frac{a}{b} \in \mathbb{Q} : (a, b) = 1 \text{ and } 5 \nmid b\right\}$ under addition.

Solution.

(i) Clearly, $*$ is a binary operation on $\mathbb{Z}$. But $5, 3, 2 \in \mathbb{Z}$ and

$$(5 * 3) * 2 = (5 - 3) - 2 = 0 \neq 4 = 5 - (3 - 2) = 5 * (3 * 2)$$

Therefore, $*$ is not associative, and hence $(\mathbb{Z}, *)$ is not a group. It can also be checked that $\mathbb{Z}$ has no identity under $*$, because if there were one (say e), then $a - e = e = e - a$, which is only possible when $e = a = 0$.

(ii) Clearly, for any $a, b \in \mathbb{Z}$, $a * b = a + b + ab \in \mathbb{Z}$, i.e., $*$ is a binary operation on $\mathbb{Z}$. We also have $a * 0 = a = 0 * a$, i.e., 0 is an identity of $(\mathbb{Z}, *)$. Also, $*$ is associative because

$$\begin{aligned}(a * b) * c = (a + b + ac) * c &= (a + b + ab) + c + (a + b + ab)c\\ &= a + b + c + ab + bc + ca + abc\\ &= a + (b + c + bc) + a(b + c + bc)\\ &= a * (b + c + bc) = a * (b * c)\end{aligned}$$

We see that

$$a * b = 0 = b * a \implies a + b + ab = 0 \implies b = \frac{-a}{1+a} \notin \mathbb{Z} \;\forall\; a \in \mathbb{Z}$$

Therefore, $*$ does not admit inverses and hence $(\mathbb{Z}, *)$ is not a group. For $\mathbb{Q}$ and $\mathbb{R}$, similar properties hold, but inverse does not exist for $a = -1$ and thus, $(\mathbb{Q}, *)$ is not a group. However, $(\mathbb{Q} - \{-1\}, *)$ and $(\mathbb{R} - \{-1\}, *)$ are groups.

(iii) Clearly, $\frac{2}{5}, \frac{3}{5} \in G$, but $\frac{2}{5} + \frac{3}{5} = 1 \notin G$. Hence, $(G, +)$ is not a group.

(iv) Let $\frac{a}{b}, \frac{c}{d} \in G'$. Then $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \in G$, because $5 \nmid b$ and $5 \nmid d$, so $5 \nmid bd$ and hence after reducing $\frac{ad+bc}{bd}$ in the simplest form (say p/q), $5 \nmid q$. Therefore, addition is a binary operation on G'. Also, any $\frac{a}{b} \in G'$ is such that $\frac{a}{b} + 0 = 0 + \frac{a}{b} = 0$ with $0 = \frac{0}{1} \in G'$. Also, for any $\frac{a}{b}$, $\exists\ \frac{-a}{b} \in G'$ such that $\frac{a}{b} + \left(\frac{-a}{b}\right) = \frac{-a}{b} + \frac{a}{b} = 0$. Therefore, $(G', +)$ is a group. □

2. G is a finite group. Show that for every $a \in G$, there exists a positive integer n such that $a^n = e$. (Note that a^n means $a * a * \cdots * a$ (n times), where $*$ is the underlying operation on the group.)

Solution. Choose $a \in G$ and consider the elements $e = a^0, a^1, a^2, a^3, a^4, \ldots$ of the group G. Since G is finite, so we must have positive integers n and m ($n \neq m$) such that $a^n = a^m$. Assume without loss of generality (WLOG) that $n > m$. Then

$$\begin{aligned} & a^n = a^m \\ \implies & a^n a^{-m} = a^m a^{-m} \\ \implies & a^{n-m} = e \qquad \text{(using associativity)} \end{aligned}$$

where $n - m = n'$ (say) is a positive integer so that $a^{n'} = 1$. Note that $a^{-m} := (a^{-1})^m$. □

3. G is a finite group. Show that there exists a positive integer n such that $a^n = e$ for all $a \in G$. (This is different from the previous problem in the sense that the previous problem asks to prove that there exists n for a given $a \in G$, i.e., the choice of n might vary depending on the choice of a, but here it asks to prove that there exists one n that works for any $a \in G$.)

Solution. By the previous problem, for any $a \in G$, there exists a positive integer n_{a_i} (n depending on a) such that $a^{n_a} = e$. Define $n = \prod_{a_i \in G} n_{a_i}$, where there are only a finite number of n_{a_i}'s (say r) because G is a finite group. We claim that this n works, i.e., $a^n = e$ for all $a \in G$. This is because

$$a^n = a^{\prod n_{a_i}} = a^{n_{a_1} n_{a_2} \cdots n_{a_r}} = (a^{n_{a_1}})^{n_{a_2} \cdots n_{a_r}} = e^{n_{a_2} \cdots n_{a_r}} = e$$

□

4. G is a finite group. Suppose $a \in G$ and m, n are positive integers such that $a^n = e$

and n divides m, then $a^m = e$.

Solution. Since n divides m, so $m = nk$ for some positive integer k. Then

$$a^m = a^{nk} = a^{nk} = e^k = e$$

□

5. Show that any group G of order ≤ 5 is abelian.

Solution. We consider the following cases: (we denote the identity by e)
Case 1: $|G| = 1$, then let $G = \{e\}$, which is abelian.
Case 2: $|G| = 2$, then let $G = \{e, a\}$ (with $e \neq a$), which is abelian because $ea = ae$, by definition.
Case 3: $|G| = 3$, then let $G = \{e, a, b\}$ (with e, a, b mutually distinct). Then $ea = ae$ and $eb = be$, by definition, i.e., e commutes mutually with a and b. To prove that a and b commute, we see that ab should also be an element of G. Thus, $ab = e$ or $ab = a$ or $ab = b$. By cancellation property, $ab = a = ae \implies b = e$ and $ab = b = eb \implies a = e$, but e, a, b are mutually distinct. Hence, $ab = e$ and so by Proposition 2, we have $ba = e = ab$. Thus, a and b commute and hence $G = \{e, a, b\}$ is abelian.
Case 4: $|G| = 4$. If G is not abelian, then $\exists\ a, b \in G$ such that $ab \neq ba$. Then $e, a, b \in G$. Also, $e \neq a$ and $e \neq b$, because if $e = a$, then $ab = eb = be = ba$ and similarly if $e = b$, then $ab = ba$. Furthermore, $a \neq b$, because if $a = b$, then $ab = a^2 = ba$. We claim that the other element is ab, and it is mutually distinct from e, a, b. It is clear from the argument in Case 3 that ab is mutually distinct from e, a, b. So we conclude that $G = \{e, a, b, ab\}$. But then, by the same argument, ba is mutually distinct from e, a, b and hence $ba = ab$, a contradiction. Therefore, G is abelian.
Case 5: $|G| = 5$. If G is not abelian, then $\exists\ a, b \in G$ such that $ab \neq ba$. Then by the previous argument, we must have $G = \{e, a, b, ab, ba\}$. We claim that $aba = b$ and $bab = a$. If $aba = e$, then $(ab)a = e \implies ab = a^{-1}$ and $a(ba) = e \implies ba = a^{-1}$, i.e., $ab = ba$, a contradiction. If $aba = a = ea$, then by cancellation property, we have $ab = e$ (but ab and e are distinct). Also if $aba = ab = abe$, then by cancellation property, we have $a = e$ (but a and e are distinct). Similarly, $aba = ba$ gives $a = e$, which is not possible. Therefore, $aba = b$ and similarly, $bab = a$. Also, we claim that $a^2 = b^2$. This is true because $aba = b \implies abab = b^2$ and $bab = a \implies abab = a^2$, i.e., $a^2 = b^2$. Now, we should have $a^2 \in G$, but $a^2 = a \implies a = e$, $a^2 = b \implies b^2 = b \implies b = e$, $a^2 = ab \implies a = b$ and $a^2 = ba \implies a = b$. Therefore, $a^2 = e \stackrel{?}{=} b^2$. But $aba = b \implies aaba = ab \implies a^2ba = ab \implies eba = ab \implies ba = ab$, a contradiction. Therefore, G is abelian.

1.4 Subgroups

Definition 7. A nonempty subset, H, of a group G is called a subgroup of G if

1. H is closed under the binary operation of G, i.e., $a, b \in H \implies ab \in H$.
2. The identity element $e \in H$.
3. If $a \in H$, then it's inverse $a^{-1} \in H$.

For example, $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ under addition, $\mathbb{Q}$ is a subgroup of $\mathbb{R}$ or $\mathbb{C}$ under addition, $\mathbb{Q} - \{0\}$ is a subgroup of $\mathbb{R} - \{0\}$ or $\mathbb{Q} - \{0\}$ under multiplication, $\mathbb{Z} - \{0\}$ is not a subgroup of $\mathbb{Q} - \{0\}$ under multiplication, since $\mathbb{Z} - \{0\}$ does not admit inverses. Is $H = \{2x : x \in \mathbb{Z}\}$ a subgroup of $(\mathbb{Z}, +)$? Clearly, H is closed under $+$, since for any $2a, 2b \in H$, $2a + 2b = 2(a + b) \in H$. Also, the identity $0 = 2 \times 0 \in H$ and the inverse of any element $2a \in H$ is $-2a \in H$. Thus, H is a subgroup of $(\mathbb{Z}, +)$. However, $H' = \{2x + 1 : x \in \mathbb{Z}\}$ is not a subgroup of $(\mathbb{Z}, +)$, because it is neither closed nor the identity 0 is odd. Also, $\{3x : x \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$. More generally, $n\mathbb{Z} := \{nx : x \in \mathbb{Z}\}$ is a subgroup of $(\mathbb{Z}, +)$ $\forall$ $n \in \mathbb{Z}$. Also, we have the following theorem:

Theorem 1. *Every subgroup of $\mathbb{Z}$ is of the form $n\mathbb{Z}$ for some non-negative integer n.*

Proof. Let H be a subgroup of $\mathbb{Z}$. If $H = \{0\}$, then $H = 0\mathbb{Z} = \{0x : x \in \mathbb{Z}\} = \{0\}$. Suppose that $H \neq \{0\}$. So H contains an integer $a \neq 0$. In fact, H contains an integer $a > 0$. This is because if $a > 0$, we are done and if $a < 0$, then $-a > 0$, where $-a \in H$ (because H is a subgroup). Let n be the smallest positive integer contained in H. We claim that $H = n\mathbb{Z}$. So, let $m \in H$ and assume $m > 0$. By the choice of n, $m \geq n$. Then,

$$\begin{aligned} m &= nq + r, \qquad\qquad q \in \mathbb{Z}, 0 \leq r < n \\ \implies m - nq &= r \end{aligned}$$

Note that $n \in H$, so $-n \in H$ and hence

$$-nq = q(-n) = \underbrace{(-n) + (-n) + \cdots + (-n)}_{q \text{ times}} \in H.$$

Therefore, $m + (-nq) = m - nq = r \in H$. It is not possible that $0 < r < n$, since n was chosen to be the smallest positive integer contained in H. Therefore, only $r = 0$ is possible and so $m = nq \implies m \in n\mathbb{Z}$, i.e., every positive integer in H is a multiple of n. Also, if $m \in H$ and $m < 0$, we consider $-m > 0$ and $-m \in H$. Then $-m = nq$ for some $q \in Z$, i.e., $m = n(-q)$. Thus, every element of H is a multiple of n. Hence, $H \subseteq n\mathbb{Z}$. But clearly, $n\mathbb{Z} \subseteq H$ because H is a subgroup and $n \in H$. Therefore, $H = n\mathbb{Z}$. □

Remark: Every group G has two *trivial* subgroups $\{e\}$ and G.

1.5 Types of groups

Definition 8. Let G be a group and let $a \in G$. The *subgroup generated by a* is the subgroup $\langle a \rangle := \{a^n : n \in \mathbb{Z}\}$.

Note: If a subgroup H of G contains a, then $a^n \in H$ for every $n \in \mathbb{Z}$. So, $\langle a \rangle \subseteq H$. Therefore, $\langle a \rangle$ is the smallest subgroup of G containing a.

Definition 9. A group G is called *cyclic* if $\exists$ an element $a \in G$ such that $\langle a \rangle = G$. We say that *G is generated by a* or *a is a generator of G*.

For example, $(\mathbb{Z}, +)$ is cyclic since $\langle 1 \rangle = \mathbb{Z}$. Also, $\langle -1 \rangle = \mathbb{Z}$. We say that 1 and -1 both are generators of $\mathbb{Z}$. But 2 is not a generator of $\mathbb{Z}$, since $\langle 2 \rangle = 2\mathbb{Z} \neq \mathbb{Z}$. In fact, no integer other than 1 and -1 is a generator of $\mathbb{Z}$.

Definition 10. The *order of a*, denoted by $\text{ord}(a)$, is the order of $\langle a \rangle$ if $\langle a \rangle$ is finite. Otherwise we say that the *order of a* is infinite.

For example, $\text{ord}(e) = 1$ for any group G, since $\langle e \rangle = \{e\}$. Also, for $G = \mathbb{Z}$, $\text{ord}(a) = \infty$ if $a \neq 0$. Recall $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$. From the group table of S_3, we have

$$\langle f_1 \rangle = \{f_1\}, \langle f_2 \rangle = \{f_1, f_2\}, \langle f_3 \rangle = \{f_1, f_3\}, \langle f_4 \rangle = \{f_1, f_4\}, \langle f_5 \rangle = \langle f_6 \rangle = \{f_1, f_5, f_6\},$$

and hence,

$$\text{ord}(f_1) = 1, \text{ord}(f_2) = \text{ord}(f_3) = \text{ord}(f_4) = 2 \text{ and } \text{ord}(f_5) = \text{ord}(f_6) = 3.$$

The following theorem is obvious.

Theorem 2. *Let G be a finite group of order n. Then G is cyclic if and only if, G contains an element of order n.*

Theorem 3. *Suppose G contains no subgroups different from $\{e\}$ and G. Then G is cyclic.*

Proof. If $G = \{e\}$, then it is cyclic. Assume that $G \neq \{e\}$. Let $a \in G$, $a \neq e$. Then $\langle a \rangle \neq \{e\}$. By hypothesis, G contains no subgroups different from $\{e\}$ and G, and thus $\langle a \rangle = G$. So, G is cyclic. □

Definition 11. The *center* of a group G, denoted by $Z(G)$, is defined as

$$Z(G) := \{g \in G : ag = ga \text{ for every } a \in G\}$$

Proposition 4. If G is a group, then

1. $Z(G)$ is a subgroup of G.
2. If G is abelian, then $Z(G) = G$.

Proof.
1. Let $g_1, g_2 \in Z(G)$. Now, for any $a \in G$, we have

   $$(g_1 g_2)a = g_1(g_2 a) = g_1(a g_2) = (g_1 a) g_2 = (a g_1) g_2 = a(g_1 g_2)$$

   Thus, $g_1 g_2 \in Z(G)$, i.e., $Z(G)$ is closed under the binary operation of G. Also, $ea = ae = a \; \forall \; a \in G$, i.e., $e \in Z(G)$. Now, for $g \in Z(G)$ and any $a \in G$, we also have

   $$g^{-1}a = (a^{-1}g)^{-1} = (ga^{-1})^{-1} = ag^{-1}$$

   Therefore, $g^{-1} \in Z(G)$. Hence, $Z(G)$ is a subgroup of G.
2. Clearly, $Z(G) \subseteq G$. Now since G is abelian, so for any $x \in G$, $xa = ax \; \forall \; a \in G$, i.e., $x \in Z(G)$. Therefore, $G \subseteq Z(G)$ and hence, $Z(G) = G$ if G is abelian.

□

Definition 12. The *centralizer* of $a \in G$, denoted by $C(a)$, is defined as

$$C(a) := \{g \in G : ag = ga\}$$

Proposition 5. If G is a group and $a \in G$, then

1. $C(a)$ is a subgroup of G.
2. $Z(G) \subseteq C(a) \; \forall \; a \in G$.
3. If G is abelian, then $C(a) = G = Z(G) \; \forall \; a \in G$.

Proof.
1. The proof of this is similar to that of Proposition 4, with a fixed here.
2. Let $x \in Z(G)$, then $xy = yx \; \forall \; y \in G$. Therefore, for any $y = a \in G$, $xa = ax$, i.e., $Z(G) \subseteq C(a) \; \forall \; a \in G$.
3. Clearly, $C(a) \subseteq G$. Now since G is abelian, so for any $x \in G$, $xa = ax \; \forall \; a \in G$, i.e., $x \in Z(G) \subseteq C(a)$. Therefore, $G \subseteq C(a)$ and hence, $C(a) = G = Z(G) \; \forall \; a \in G$.

□

1.6 Group homomorphisms and examples

Definition 13. A *homomorphism of groups* is a function $\varphi : G \to G'$ such that

$$\varphi(ab) = \varphi(a)\varphi(b)\ \forall\ a, b \in G$$

Given below are some examples.

1. Consider $\varphi : \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi(a) = na$. Then $\varphi(a+b) = n(a+b)$ and $\varphi(a) + \varphi(b) = na + nb = n(a+b) = \varphi(a+b)\ \forall a, b \in \varphi$ and thus, φ is a group homomorphism.
2. Now consider $\varphi : \mathbb{Z} \to \{1, -1\}$ (Note that $\{1, -1\}$ is group under multiplication. Also note that $\{1, -1\}$ is a subgroup of $\mathbb{Q} - \{0\}$.) defined by

$$\varphi(a) = \begin{cases} 1, & \text{if } a \text{ is even} \\ -1, & \text{if } a \text{ is odd} \end{cases}$$

   We want to check if $\varphi(a+b) = \varphi(a)\varphi(b)$ or not. If a and b have the same parity, then $a+b$ is even and hence $\varphi(a+b) = 1 = \varphi(a)\varphi(b)$. If a and b have different parity, then $a+b$ is odd and hence $\varphi(a+b) = -1 = 1 \cdot (-1) = (-1) \cdot 1 = \varphi(a)\varphi(b)$. Therefore, φ is a group homomorphism.
3. We consider another example with the function $\varphi : \mathbb{Z} \to \{1, -1\}$ defined by

$$\varphi(a) = \begin{cases} -1, & \text{if } a \text{ is even} \\ 1, & \text{if } a \text{ is odd} \end{cases}$$

   For $3, 4 \in \mathbb{Z}$, $\varphi(3+4) = \varphi(7) = 1$ whereas, $\varphi(3)\varphi(4) = 1 \cdot (-1) = -1$. Therefore, φ is not a group homomorphism.
4. Consider $\varphi : GL_n(\mathbb{R}) \to \mathbb{R} - \{0\}$ defined as $\varphi(A) =$ determinant of A. Therefore, φ is a group homomorphism by the well known property of determinants that $\det(AB) = \det(A)\det(B)$.
5. Now consider an arbitrary group G and fix an element $a \in G$, and consider the function $\varphi : \mathbb{Z} \to G$ defined by $\varphi(n) = a^n$. Then

$$\varphi(m+n) = a^{m+n} \stackrel{?}{=} a^m \cdot a^n = \varphi(m)\varphi(n)$$

   and hence φ is a group homomorphism.
6. Consider $\varphi : G \to G$, where G is an abelian group, defined by $\varphi(a) = a^2$. We want to check if φ is a group homomorphism. We have,

$$\varphi(ab) = (ab)^2 = (ab)(ab) = a(ba)b = a(ab)b = (aa)(bb) = a^2b^2 = \varphi(a)\varphi(b)$$

   and hence φ is a group homomorphism.
   Note: In general, $(ab)^2 \neq a^2b^2$. Thus, φ is not a group homomorphism in general, when G is not abelian. Recall $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, which is not abelian, and let $\varphi : S_3 \to S_3$ defined by $\varphi(f_i) = f_i^2$. From the group table of S_3, we have

$$\varphi(f_2f_3) = \varphi(f_5) = f_5^2 = f_6$$

   whereas

$$\varphi(f_2)\varphi(f_3) = f_2^2f_3^2 = f_1f_1 = f_1$$

   and hence φ is not a group homomorphism.

1.7 Properties of group homomorphisms

Proposition 6. Let $\varphi : G \to G'$ be a group homomorphism. Then

1. $\varphi(e_G) = e_{G'}$.
2. If $a \in G$, then $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

Proof.

1. Since $e_G = e_G e_G$, so $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$. Thus, by cancellation property in G', we get $\varphi(e_G) = e_{G'}$.
2. Let $a \in G$, then $aa^{-1} = e_G$ and so

$$\begin{aligned} &\varphi(aa^{-1}) = \varphi(e_G) = e_{G'} \\ \implies &\varphi(a)\varphi(a^{-1}) = e_{G'} \\ \implies &\varphi(a^{-1}) = (\varphi(a))^{-1} \end{aligned}$$

□

Recall the function $\varphi : \mathbb{Z} \to \{1, -1\}$ defined by

$$\varphi(a) = \begin{cases} -1, & \text{if } a \text{ is even} \\ 1, & \text{if } a \text{ is odd} \end{cases}$$

Here, $e_{\mathbb{Z}} = 0$ is even, so $\varphi(e_{\mathbb{Z}}) = -1$ and $e_{\{1,-1\}} = 1$ is odd, so $\varphi(e_{\{1,-1\}}) = 1 \neq \varphi(e_{\mathbb{Z}})$ and hence φ is not a group homomorphism.
Let $\varphi : G \to G'$ is a group homomorphism. Then we have the following definitions.

Definition 14. The kernel of φ, $\mathrm{Ker}(\varphi)$, is defined as

$$\mathrm{Ker}(\varphi) = \{a \in G : \varphi(a) = e_{G'}\} \subseteq G$$

Definition 15. The image of φ, $\mathrm{im}(\varphi)$, is defined as

$$\mathrm{im}(\varphi) = \{\varphi(a) : a \in G\} \subseteq G'$$

Proposition 7. For any group homomorphism $\varphi : G \to G'$,

1. $\mathrm{Ker}(\varphi)$ is a subgroup of G.
2. $\mathrm{im}(\varphi)$ is a subgroup of G'.

Proof.

1. For any $a, b \in \mathrm{Ker}(\varphi)$, we have $\varphi(a) = \varphi(b) = e_{G'}$. Since φ is a group homomorphism, so $\varphi(ab) = \varphi(a)\varphi(b) = e_{G'}e_{G'} = e_{G'}$ and hence, $ab \in \mathrm{Ker}(\varphi)$. Therefore, φ is closed under the binary operation of G. Also by Proposition 6, $\varphi(e_G) = e'_G$ and hence $e_G \in \mathrm{Ker}(\varphi)$. Now, $a \in \mathrm{Ker}(\varphi) \implies \varphi(a) = e_{G'}$ and again by Proposition 6, $\varphi(a^{-1}) = (\varphi(a))^{-1} = (e_{G'})^{-1} = e_{G'}$, i.e., $a^{-1} \in \mathrm{Ker}(\varphi)$ for all $a \in \mathrm{Ker}(\varphi)$. Therefore, $\mathrm{Ker}(\varphi)$ is a subgroup of G.
2. Consider $\varphi(a), \varphi(b) \in \mathrm{im}(\varphi)$ with $a, b \in G$. Then by the definition of group homomorphism, $\varphi(a)\varphi(b) = \varphi(ab) \in \mathrm{im}(\varphi)$. Also, $e'_G = \varphi(e_G) \in \mathrm{im}(\varphi)$. We also have $\varphi(a^{-1}) = (\varphi(a))^{-1} \in \mathrm{im}(\varphi)$ for all $\varphi(a) \in \mathrm{im}(\varphi)$. Hence, $\mathrm{im}(\varphi)$ is a subgroup of G.

□

We see some examples given below:

1. Consider the group homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}$ defined by $\varphi(a) = na$. Then $\text{Ker}(\varphi) = \{a \in \mathbb{Z} : na = 0\} = \{0\}$ and $\text{im}(\varphi) = \{na : a \in \mathbb{Z}\} = n\mathbb{Z}$ are both subgroups of $\mathbb{Z}$.
2. Consider the determinant group homomorphism $\varphi : GL_n(\mathbb{R}) \to \mathbb{R} - \{0\}$ defined as $\varphi(A) = \det(A)$. Then, $\text{Ker}(\varphi) = \{A \in GL_n(\mathbb{R}) : \det(A) = 1\}$, which is called the *special linear group* $SL_n(\mathbb{R})$, and $\text{im}(\varphi) = \{\det(A) : A \in GL_n(\mathbb{R})\} \stackrel{?}{=} \mathbb{R} - \{0\}$.
3. Consider an arbitrary group G and fix an element $a \in G$, and consider the function $\varphi : \mathbb{Z} \to G$ defined by $\varphi(n) = a^n$. Then, $\text{Ker}(\varphi) = \{n \in \mathbb{Z} : a^n = e_G\}$ and $\text{im}(\varphi) = \{\varphi(n) : n \in \mathbb{Z}\} = \{a^n : n \in \mathbb{Z}\} = \langle a \rangle$.
   Remark: Since $\text{Ker}(\varphi)$ is a subgroup of $\mathbb{Z}$, so by Theorem 1, $\text{Ker}(\varphi) = b\mathbb{Z}$ for some non-negative integer b. Note that b is related to $\text{ord}(a)$, where

   (i) If $a^n = e_G$ for some positive integer n, then $\text{ord}(a)$ is the smallest positive integer m such that $a^m = e_G$

   (ii) If $a^n \neq e_G$ for any positive integer n, then $\text{ord}(a) = \infty$.

   If $b = 0$, then $\text{Ker}(\varphi) = \{0\} \implies \text{ord}(a) = \infty$. If $b > 0$, then $\text{ord}(a) = b$.

1.8 Group isomorphisms

Let $\varphi : G \to G'$ be a group homomorphism.

Definition 16. φ is 1-1 (or *injective*) if $\varphi(a) = \varphi(b) \implies a = b$, or equivalently $a \neq b \implies \varphi(a) \neq \varphi(b)$.

Definition 17. φ is onto (or *surjective*) if $\text{im}(\varphi) = G'$.

Definition 18. φ is bijective if it is both injective and surjective.

Proposition 8. φ is injective if and only if $\text{Ker}(\varphi) = \{e_G\}$.

Proof. Suppose φ is injective. Let $a \in \text{Ker}(\varphi)$. Then

$$\varphi(a) = e_{G'} = \varphi(e_G) \implies a = e_G$$

and hence $\text{Ker}(\varphi) = \{e_G\}$. For the other direction, suppose $\text{Ker}(\varphi) = \{e_G\}$. Then for any $a, b \in G$,

$$\varphi(a) = \varphi(b) \implies \varphi(a)(\varphi(b))^{-1} = e_{G'} \implies \varphi(a)\varphi(b^{-1}) = e_{G'} \implies \varphi(ab^{-1}) = e_{G'}$$

Therefore, $ab^{-1} \in \text{Ker}(\varphi) = \{e_G\}$. So $ab^{-1} = e_G$ and hence $a = b$, i.e., φ is injective. □

Definition 19. An *isomorphism* of groups is a group homomorphism $\varphi : G \to G'$ such that φ is 1-1 and onto (i.e., φ is bijective).

Proposition 9. If $\varphi : G \to G'$ is a group isomorphism, then $\varphi^{-1} : G' \to G$ is also a group isomorphism.

Proof. Since φ is a bijection, so we have an inverse mapping $\varphi^{-1} : G' \to G$. Also, for all $g \in G, g' \in G'$, $\varphi(g) = g' \iff \varphi^{-1}(g') = g$. Now suppose $g_1, g_2 \in G$ and $g_1' = \varphi(g_1), g_2' = \varphi(g_2) \in G'$ and hence

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = g_1' g_2'$$

So,

$$\varphi^{-1}(g_1'g_2') = g_1g_2 = \varphi^{-1}(g_1')\varphi^{-1}(g_2')$$

Therefore. φ^{-1} is a bijection and a group homomorphism, hence an isomorphism. $\square$

Consider the group of fourth roots of unity $G_1 = \{1, i, -1, -i\}$, where $i = \sqrt{-1}$, and the group $G_2 = \{e, a, a^2, a^3\}$. (We say groups G_1 and G_2 are isomorphic if there is a group isomorphism $\varphi : G_1 \to G_2$.) Define $\varphi : G_1 \to G_2$ such that $\varphi(1) = e$, $\varphi(i) = a$, $\varphi(-1) = a$ and $\varphi(-i) = a^3$. This is a bijection by the definition of φ. One can check that $\varphi(ab) = \varphi(a)\varphi(b)\ \forall\ a, b \in G_1$ and hence G_1 and G_2 are isomorphic.

Theorem 4. *If groups G and G' are isomorphic, then*

1. *G is abelian if and only if G' is abelian.*
2. *G is cyclic if and only if G' is cyclic.*

Proof. Let $\varphi : G \to G'$ is an isomorphism.

1. Suppose G is abelian. Consider any $g_1', g_2' \in G'$. Let $g_1' = \varphi(g_1)$ and $g_2' = \varphi(g_2)$ for some $g_1, g_2 \in G$. Then,

$$g_1'g_2' = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) = \varphi(g_2g_1) = \varphi(g_2)\varphi(g_1) = g_2'g_1'$$

and hence G' is abelian.

Now suppose G' is abelian. By Proposition 9, we have $\varphi^{-1} : G' \to G$ is an isomorphism. Consider any $g_1, g_2 \in G$. Let $g_1 = \varphi^{-1}(g_1')$ and $g_2 = \varphi^{-1}(g_2')$ for some $g_1', g_2' \in G'$. Then,

$$g_1g_2 = \varphi^{-1}(g_1')\varphi^{-1}(g_2') = \varphi^{-1}(g_1'g_2') = \varphi^{-1}(g_2'g_1') = \varphi^{-1}(g_2')\varphi^{-1}(g_1') = g_2g_1$$

and hence G is abelian.

2. Suppose G is cyclic. Consider any $g' \in G'$, then $g' = \varphi(g)$ for some $g \in G$. Since G is cyclic, so $g = a^n$ for some $n \in \mathbb{Z}$. Using the definition of homomorphism, we have

$$g' = \varphi(g) = \varphi(a^n) = (\varphi(a))^n$$

So, $g' \in \langle\varphi(a)\rangle$ and hence, $G' \subseteq \langle\varphi(a)\rangle$. By definition, $\langle\varphi(a)\rangle \subseteq G'$. Therefore, $\langle\varphi(a)\rangle = G'$, i.e., G' is cyclic. A similar argument proves the other direction.

$\square$

2 Normal subgroups

Definition 20. Let G be a group. A subgroup H of G is *normal* if $ghg^{-1} \in H$ for every $g \in G$ and $h \in H$.

Theorem 5. *If G is abelian, then every subgroup of G is normal.*

Proof. For every $g \in G, h \in H$, $ghg^{-1} = gg^{-1}h = h \in H$. $\square$

Recall $S_3 = \{f_1, f_2, f_3, f_4, f_5, f_6\}$. Then the group $H = \{f_1, f_2\}$ is not normal in S_3. This is because $f_3^2 = f_1 \implies f_3 = f_3^{-1}$ and hence

$$f_3f_2f_3^{-1} = f_3f_2f_3 = f_4 \notin H$$

2.1 Important examples of normal subgroups

Proposition 10. For any group homomorphism $\varphi : G \to G'$, $\mathrm{Ker}(\varphi)$ is a normal subgroup of G.

Proof. We have already seen in Proposition 7 that $\mathrm{Ker}(\varphi)$ is a subgroup of G. To prove that it is normal in G, take any $g \in G$ and $h \in \mathrm{Ker}(G)$. Then,

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)e_{G'}(\varphi(g))^{-1} = \varphi(g)(\varphi(g))^{-1} = e_{G'}$$

and hence $ghg^{-1} \in \mathrm{Ker}(G)$, i.e., $\mathrm{Ker}(\varphi)$ is a normal subgroup of G. □

Proposition 11. The center, $Z(G)$ is a normal subgroup of G.

Proof. We have already seen in Proposition 4 that $Z(G)$ is a subgroup of G. To prove that it is normal in G, take any $g \in G$ and $h \in Z(G)$. We need to prove that $ghg^{-1} \in Z(G)$. We have,

$$ghg^{-1} = gg^{-1}h = h \in Z(G)$$

and hence $Z(G)$ is a normal subgroup of G. □

2.2 Some exercises

1. Describe all group homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$.

Solution. Suppose that $\varphi : \mathbb{Z} \to \mathbb{Z}$ is a group homomorphism. Then, we should have $\varphi(0) = 0$. Suppose that $\varphi(1) = a \in \mathbb{Z}$. Then $\varphi(1+1) = \varphi(1) + \varphi(1) = 2a$. In general, for all $n \in \mathbb{N}$, we have

$$\varphi(n) = \varphi(1) + \varphi(1) + \cdots + \varphi(1) \ (n \text{ times}) = na$$

By a property of group homomorphism, we have $\varphi(-n) = -\varphi(n) = -na$ for all $n \in \mathbb{N}$. Therefore, for all $n \in \mathbb{Z}$, we have

$$\varphi(n) = na = n\varphi(1)$$

This means that φ is determined by $\varphi(1)$, i.e., the group homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}$ are determined by the image of 1, which can be any integer. □

2. Which of these homomorphisms $\varphi_a : \mathbb{Z} \to \mathbb{Z}$ are isomorphisms? (Here, $\varphi_a : \mathbb{Z} \to \mathbb{Z}$ is such that $\varphi_a(1) = a \in \mathbb{Z}$.)

Solution. For $|a| \geq 2$, $\varphi_a(n) = an$ for all $n \in \mathbb{Z}$. Hence, φ_a is injective, but not surjective because 1 is not in the image of $\varphi(a)$. Also, φ_0 (defined by $\varphi_0(n) = 0$ for all $n \in \mathbb{Z}$) is not an injection and hence not an isomorphism. However, φ_1 (defined by $\varphi_1(n) = n$) and φ_{-1} (defined by $\varphi_{-1}(n) = -n$) are isomorphisms. □
Summary: Every group homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ is one of the homomorphisms $\{\varphi_a,\, a \in \mathbb{Z}\}$. φ_a is an isomorphism $\iff a = 1$ or $a = -1$. φ_a is injective $\iff a \neq 0$ (note that this satisfies Proposition 8). φ_a is surjective $\iff a = 1$ or $a = -1$.

3. Let G be a group and let $a \in G$. Suppose that $\mathrm{ord}(a) = r$. If $a^n = e$ for some positive integer n, then show that r divides n.

Solution. By definition, since r is the smallest positive integer such that $a^r = e$, the identity element, so we have $n > r$. Therefore, $n = qr + s$ for $s < r$. So,

$$e = a^n = a^{qr+s} = a^{qr} \cdot a^s = (a^r)^q \cdot a^s = e \cdot a^s = a^s$$

which is a contradiction for $s > 0$ since r is the smallest positive integer such that $a^r = e$. Therefore, $s = 0$ and hence $n = qr$, i.e., $r \mid n$. □

Alternative: Consider the homomorphism $\varphi : \mathbb{Z} \to G$ given by $\varphi(m) = a^m$ (see Section 1.6). Then note that $\mathrm{Ker}(\varphi) = r\mathbb{Z}$. Since $a^n = e$, so $n \in \mathrm{Ker}(\varphi) = r\mathbb{Z}$. This implies that n is a multiple of r, i.e., r divides n. □

4. Suppose $\varphi : G \to G'$ is a group homomorphism and $a \in G$. Let $\mathrm{ord}(a) = m$. Then prove that $\mathrm{ord}(\varphi(a))$ divides m.

Solution: Since $\mathrm{ord}(a) = m$, so $a^m = e_G$. This gives $(\varphi(a))^m = \varphi(a^m) = \varphi(e_G) = e_{G'}$. Therefore, by the previous problem, we have, $\mathrm{ord}(a)$ divides m. □

Note: In particular, if $\varphi : G \to G'$ is a group homomorphism and $a \in G$ has order p, where p is a prime, then φ has order 1 or p.

2.3 Equivalence relations and equivalence classes

Let S be a set. An equivalence relation on S is a relation, denoted by $\sim$, satisfying:
(i) $a \sim a$ for any $a \in S$
(ii) $a \sim b \implies b \sim a$ for any $a, b \in S$
(iii) $a \sim b, b \sim c \implies a \sim c$ for any $a, b, c \in S$.

For example,
(1) The relation $\sim$ defined by $a \sim b$ if $4 \mid a - b$ is an equivalence relation on $\mathbb{Z}$.
(2) Let G be a group and H be a subgroup of G. Let $a, b \in G$. We define $a \sim b$ if $a^{-1}b \in H$. Clearly, $a \sim a$ because $a^{-1}a = e \in G$. Also,

$$a \sim b \implies a^{-1}b \in H \implies (a^{-1}b)^{-1} \in H \implies b^{-1}a \in H \implies b \sim a$$

Now,

$$a \sim b, b \sim c \implies a^{-1}b \in H, b^{-1}c \in H \implies (a^{-1}b)(b^{-1}c) \in H \implies a^{-1}c \in H \implies a \sim c$$

Therefore, $\sim$ is an equivalence relation on G.

An equivalence relation on a set S partitions the set into equivalence classes. For $a \in S$, the *equivalence class* of a is defined as

$$[a] = \{b \in S : a \sim b\}$$

In the previous examples,
(1) The equivalence class of 5 is

$$[5] = \{b \in \mathbb{Z} : 5 \sim b\} = \{b \in \mathbb{Z} : 4 \mid 5 - b\} = 4\mathbb{Z} + 1$$

(2) The equivalence class of $a \in G$ is

$$\begin{aligned}[a] = \{b \in G : a \sim b\} = \{b \in G : a^{-1}b \in H\} &= \{b \in G : b = ah \text{ for some } h \in H\} \\ &= \{ah : h \in H\} =: aH\end{aligned}$$

(We similarly define $Ha := \{ha : h \in H\}$.)

2.4 Cosets and Lagrange's Theorem

Definition 21. If H is a subgroup of G, the *left cosets* of H are subsets aH, $a \in G$ and the *right cosets* of H are subsets Ha, $a \in G$.

If H is a subgroup of a group G and for $a, b \in G$, we define an equivalence relation $a \sim b$ if $a^{-1}b \in H$, then the equivalence classes are simply the left cosets of H. This means that G is the disjoint union of left cosets.
Note: aH and Ha are just sets and have no further structure.

Proposition 12. Let H be a subgroup of a finite group G and let $a \in G$. Then the number of elements of aH is equal to $|H|$.

Proof. Consider the mapping $f : H \to aH$ given by $h \overset{f}{\longmapsto} ah$. Then f is injective because for $h_1, h_2 \in H$, we have,

$$f(h_1) = f(h_2) \implies ah_1 = ah_2 \implies h_1 = h_2$$

Also, f is clearly surjective because for every $ah \in aH$, there exists $h \in H$ such that $f(h) = ah$. Therefore, f is bijective and hence the number of elements of aH is equal to $|H|$. (We shall write $|aH| = |H|$, where $|aH|$ denotes the cardinality of the set aH, whereas $|H|$ denotes the cardinality of the group H.) □

Theorem 6 (Lagrange's theorem). *If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.*

Proof. Let n be the number of left cosets of H, say $a_1H = H$ $(a_1 = e)$, $a_2H, a_3H, \dots, a_nH$. Then

$$G = \bigsqcup_{1 \le i \le n} a_iH$$

By Proposition 12,

$$|eH| = |a_2H| = |a_3H| = \cdots = |a_nH| = |H|,$$

and hence

$$|G| = \sum_{1 \le i \le n} |a_iH| = \sum_{1 \le i \le n} |H| = n|H|$$

which gives $|H|$ divides $|G|$. □

Definition 22. The number of left cosets of H in G is called the *index of H in G*; it is denoted by $[G : H]$.

Then as in the proof of the Lagrange's theorem, we have the following counting formula:

$$|G| = [G : H]|H|$$

Corollary 6.1. If G is a finite group and $a \in G$, then $\text{ord}(a)$ divides $|G|$.

Proof. Consider the cyclic subgroup $\langle a \rangle$ of G, generated by a. Clearly, $a^{\text{ord}(a)} = e$, so $\langle a \rangle$ at most $\text{ord}(a)$ elements. Also, $\langle a \rangle$ cannot be fewer than $\text{ord}(a)$ elements because if $a^i = a^j$ for some integers $0 \le i < j < \text{ord}(a)$, then $a^{j-i} = e$ for $0 < j - i < \text{ord}(a)$, which contradicts the meaning of $\text{ord}(a)$. Therefore, $\langle a \rangle$ has exactly $\text{ord}(a)$ elements and since $\langle a \rangle$ is a subgroup of G, by Lagrange's Theorem, $\text{ord}(a)$ divides G. □

Corollary 6.2. If G is a finite group and $a \in G$, then $a^{|G|} = e$.

Proof. By Corollary 6.1, $\text{ord}(a)$ divides $|G|$, so $|G| = m \cdot \text{ord}(a)$ for some $m \in \mathbb{Z}$. Therefore,

$$a^{|G|} = a^{m \cdot \text{ord}(a)} = \left(a^{\text{ord}(a)}\right)^m = e^m = e.$$

□

Corollary 6.3. If G is a finite group whose order is a prime p, then G is cyclic.

Proof. Let $a \in G \setminus \{e\}$. Then by Lagrange's theorem, we have $\text{ord}(a)$ divides $|G| = p$, so $\text{ord}(a) = 1$ or p. Since $a \neq a$, so $\text{ord}(a) \neq 1$. Therefore, $\text{ord}(a) = |G|$ and hence $\langle a \rangle = G$, i.e., G is cyclic. □

For $m \geq 1$, $\phi(m)$ denotes the number of positive integers not exceeding m that are relatively prime to m.

Corollary 6.4. (Euler) If $n \in \mathbb{Z}^+$ and a is relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Proof. The set of positive integers not exceeding n that are relatively prime to n is denoted by $(\mathbb{Z}/n\mathbb{Z})^\times$ and is called the group of units modulo n. We shall prove that this set forms a group under multiplication mod n.

Let $a, b \in (\mathbb{Z}/n\mathbb{Z})^\times$, then $\gcd(a, n) = \gcd(b, n) = 1$, which implies $\gcd(ab, n) = 1$. Therefore, $ab \in (\mathbb{Z}/n\mathbb{Z})^\times$ and hence the set is closed under multiplication. Associativity in $(\mathbb{Z}/n\mathbb{Z})^\times$ under multiplication follows from that in integers. Since 1 is relatively prime to n, so $1 \in (\mathbb{Z}/n\mathbb{Z})^\times$ and also for any $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, $1a = a1 = a$. Thus, 1 is the identity element. Also for any $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, since $\gcd(a, n) = 1$, there exists $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Taking mod n, we get $ax \equiv 1 \pmod{n}$ and hence x is the inverse of a. Thus, every element in $(\mathbb{Z}/n\mathbb{Z})^\times$ has an inverse. Thus, $(\mathbb{Z}/n\mathbb{Z})^\times$ is a group and also $\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$, by the definition of $(\mathbb{Z}/n\mathbb{Z})^\times$.

Applying Corollary 6.3, we have

$$a^{\phi(n)} = a^{\left|(\mathbb{Z}/n\mathbb{Z})^\times\right|} \equiv 1 \pmod{n}.$$

□

The following corollary then directly follows:

Corollary 6.5 (Fermat)**.** If p is a prime and a is any integer, then $a^p \equiv a \pmod{p}$.

2.5 A counting principle

Let us generalize the notions of left and right cosets. Let H, K be subgroups of a group G, we write

$$HK = \{hk \mid h \in H, k \in K\}.$$