Chapter - 1 : Fundamentals of Group Theory

Definition .1 (Group) *A non-empty set G, along with a binary operation denoted by $*$, is defined to constitute a group if the following conditions are met:*

1. *For all $a, b \in G$, it holds that $a * b \in G$ (Closure).*
2. *For all $a, b, c \in G$, the equation $a * (b * c) = (a * b) * c$ is satisfied (Associative Law).*
3. *There exists an element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$ (Existence of an Identity).*
4. *For each $a \in G$, there exists an element $b = a^{-1} \in G$ such that $b * a = a * b = e$ (Existence of an Inverse).*

Definition .2 (Abelian Group) *A group G is classified as an abelian (or commutative) group if, for all $a, b \in G$, the equation $a * b = b * a$ holds true (Commutative Law).*

Example 1.0.1 1. *$(\mathbb{Z}, +)$, the set of integers with addition as the binary operation, forms a group.*
2. *$(\mathbb{R}, +)$, the set of real numbers with addition as the binary operation, constitutes a group.*
3. *$(\mathbb{R} - \{0\}, *)$, the set of non-zero real numbers under multiplication as the binary operation, also constitutes a group.*

Note 1 *All of the above groups are abelian groups.*

Definition .3 (Finite (Infinite) Group) *A group G is termed a finite (infinite) group if the set G is finite (infinite).*

Example 1.0.2 (Finite Group) 1. *Consider $G = \{-1, 1\}$ equipped with the multiplication of real numbers; then G forms a group (abelian), and it is also a finite group.*
2. *Let $G = S_3$, a set consisting of all injective maps on the set $\{1, 2, 3\}$ onto itself, using map composition as the binary operation. G is a finite group.*

Example 1.0.3 (Infinite Group) *$(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{R} - \{0\}, *)$ are all infinite groups.*

Definition .4 (Order of a Group) *For a finite group G, the order of the group, denoted as $|G|$, is defined as the number of elements in G.*

Note 2 *If G has an infinite number of elements, then G possesses infinite order.*

Example 1.0.4 1. *The group $G = \{1, -1\}$ has an order 2.*
2. *The group $G = S_3$ has an order 6.*
3. *The group $(\mathbb{Z}, +)$ has an infinite order.*

Proposition .1 *If G is a group under the operation $*$, then*

1. *the identity e of G is unique.*
2. *for any $a \in G$, the inverse a^{-1} is uniquely determined.*
3. *$(a^{-1})^{-1} = a$ for all $a \in G$.*
4. *$(a * b)^{-1} = b^{-1} * a^{-1}$.*

Hint(s):

1. *Let e_1 and e_2 be two identities. Then,*

$$e_1 * e_2 = e_2 * e_1 = e_2 \text{ and}$$
$$e_2 * e_1 = e_1 * e_2 = e_1 \Rightarrow e_1 = e_2.$$

2. *If b and c in G are inverses of $a \in G$, then $a * b = b * a = e$, $a * c = c * a = e$*
$\Rightarrow a * b = a * c \Rightarrow b * (a * b) = b * (a * c)$

$\Rightarrow (b*a)*b = (b*a)*c \Rightarrow e*b = e*c$
$\Rightarrow b = c.$

3. *Exercise.*

4. *Exercise.* ■

Exercise 1 *For any elements a,b,c belonging to the group G, if the equation $a*b = a*c$ holds true, then it implies that $b = c$. This is referred to as the left cancellation law. Similarly, applying cancellation from the right leads to the right cancellation law.*

1. *Is $(\mathbb{Z},-)$ a group? Hint:* $1-(2-3) \neq (1-2)-3$.

2. *Investigate whether the structures $(\mathbb{Z},*)$, $(\mathbb{Q},*)$, $(\mathbb{R},*)$, and $(\mathbb{C},*)$ are groups or not.*

3. *Consider*

$$U(n) = \{x \in \mathbb{N} : 1 \leq x \leq n \text{ and } (x,n) = 1\}$$
$$= \text{the set of positive numbers less than n and relatively prime to } n.$$

Verify whether $(U(n),\times_n)$ forms a group, where $\times_n$ represents multiplication modulo n, i.e., $a \times_n b = a \cdot b (mod\ n)$.

4. *Similarly, investigate whether $(\mathbb{Z}_n,+_n)$ is a group. Here, $\mathbb{Z}_n = \{\bar{0},\bar{1},\bar{2},\ldots,\bar{n-1}\}$, and $\bar{0} = \{x \in \mathbb{Z} \mid x\%n = 0,$ i.e., $x = nk$ for some $k\}$,*
$\bar{1} = \{x \in \mathbb{Z} \mid x\%n = 1$, i.e., $x = 1 + nk$ for some $k\}$, and so on.
The operation $+_n$ is defined as $a +_n b = a + b(\mod n)$ $(a \equiv b (mod\ n) \Leftrightarrow n|a-b \Leftrightarrow a - b = nk$ for some $k)$.

5. *Find $U(8)$, determine the identity element, and find the inverse of all elements in $U(8)$. Perform the same tasks for $(\mathbb{Z}_8,+_8)$.*

6. *Let $G = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : ad - bc \neq 0, a,b,c,d \in \mathbb{Z}\right\}$. Determine if G is a group:*

   (a) under addition of matrices

   (b) under multiplication of matrices

   Repeat the process, after replacing the condition $ad - bc \neq 0$ with $ad - bc = 1$.

7. *Is $\mathbb{Z}_{10}$ a group under multiplication modulo 10? If not, identify the reason and generalize it to $\mathbb{Z}_n$ (the general case).*

1.1. Quaternion group

Definition .5 (Quaternion Group) *The quaternion group Q_8 is defined as $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, where $i^2 = j^2 = k^2 = -1$, and the following relations hold:*

$$i \cdot j = k, \quad j \cdot i = -k$$
$$j \cdot k = i, \quad k \cdot j = -i$$
$$k \cdot i = j, \quad i \cdot k = -j$$

Note 3 $(-1)\cdot(-1) = 1$ *and* $(-1)\cdot a = a \cdot (-1) = -a$ *for all* $a \in Q_8$.

Exercise 2 *Provide a composition table for Q_8.*

1.1.1. Subgroups

Definition .6 (Subgroup) *Let G be a group. The subset H of G is a subgroup of G if H is non-empty, and for all $x,y \in H$:*

1. *$xy \in H$, and*

2. *$x^{-1} \in H$*

In other words, H forms a group under the same operation as G.

Note 4 *We denote $H \leq G$ to represent that H is a subgroup of G.*

Example 1.1.1 *1. $\mathbb{Z} \leq \mathbb{Q}$ and $\mathbb{Q} \leq \mathbb{R}$ under addition.*

2. *For any group G, the groups $H = G$ and $H = \{e\}$ are trivial subgroups of G.*
3. *Let $G = D_{2n}$ and $H = \{1, r, r^2, \ldots, r^{n-1}\}$, where H represents the set of rotations in G.*
4. *In the quaternion group $G = Q_8$, the subgroups $H_1 = \{\pm 1, \pm i\}$, $H_2 = \{\pm 1, \pm j\}$, $H_3 = \{\pm 1, \pm k\}$, and $H_4 = \{\pm 1\}$ are examples of subgroups of Q_8.*

Proposition .2 (Finite Subgroup Test) *If H is a non-empty finite subset of G, then H is a subgroup of G if it is closed under the operation of G.*

Hint(s): *The closure property of H and the fact that H is finite imply that for any $a \in H$, there exists an integer m such that $a^m = e$, and thus $a^{-1} = a^{m-1}$ (since $a^i = a^j$ implies $a^{i-1} = e$). Hence, the proof follows.* ■

Example 1.1.2 *1. For any group G and $a \in G$, the set $< a >= \{a^i : i \in \mathbb{Z}\}$ is a subgroup of G.*

2. *In the group $U(10)$, the subgroup $< 3 >$ is equal to $U(10)$.*
3. *In the group $\mathbb{Z}_{10}$, the subgroup $< 2 >= \{0, 2, 4, 6, 8\}$.*
4. *In the group $\mathbb{Z}$, the subgroup $< -1 >= \mathbb{Z}$.*
5. *In the dihedral group D_n, the subgroup $< r >$ represent the set of rotations.*

Exercise 3 *Prove that the set of even integers is a subgroup of the group of all integers under addition.*

Note 5 *The operation of H and G must be the same.*

Example 1.1.3 *1. The subset $\mathbb{Q} - \{0\}$ under multiplication is not a subgroup of $\mathbb{R}$ under addition.*

2. *The set $\mathbb{Z}^+$ is not a subgroup of $\mathbb{Z}$ under addition.*
3. *The group D_6 is not a subgroup of D_8 (as D_6 is not even a subset of D_8).*

Exercise 4 *If H is a subgroup of G and K is a subgroup of H, then K is also a subgroup of G.*

Exercise 5 *If H and K are subgroups of G, then $H \cap K$ is also a subgroup of G.*

Exercise 6 *Is the union of subgroups a subgroup?*

Definition .7 (Cartesian (Direct) Product) *Let A and B be two groups. Their direct product is defined as*

$$A * B = \{(a, b) : a \in A, b \in B\}$$

with some suitable binary operation on $A * B$.

For instance, if $(A, *)$ and $(B, \circ)$ are two groups, and for $(a, b), (c, d) \in A * B$, we have $(a, b)(c, d) = (a * c, b \circ d)$, then $A * B$ is also a group.

Exercise 7 *1. Determine whether the following subsets of $A * B$ are subgroups of $A * B$.*

(a) $\{(a, 1) : a \in A\}$

(b) $\{(1, b) : b \in B\}$

(c) $\{(a, a) : a \in A\}$, *where $A = B$.*

2. *Prove that $H = \{x \in D_n,\ x^2 = 1\}$ is not a subgroup of D_n (for $n \geq 3$).*

1.2. Centralizers and Normalizers

Definition .8 (Centralizer) *Let $\phi \neq A \subseteq G$. We define*

$$C_G(A) = \{g \in G : ga = ag \ \forall\ a \in A\}$$

This subset of G is called the centralizer of A in G, meaning it contains elements in G that can commute with all elements of A.

Exercise 8 *Let $\phi \neq A \subseteq G$. Prove that $C_G(A)$ is a subgroup of G.*

Hint(s): *To show that $x, y \in C_G(A) \Rightarrow xy^{-1} \in C_G(A)$ and that $C_G(A)$ is a non-empty set, observe that $ax = xa \Rightarrow a = xax^{-1}$ and $ay = ya \Rightarrow a = yay^{-1}$. It's clear that $e \in G \Rightarrow e \in C_G(A)$. Then, $(xy)a(xy)^{-1} = (xy)a(y^{-1}x^{-1}) = xax^{-1} = a$. In particular, if $A = \{a\}$ for some $a \in G$, then we write $C_G(A) = \{x \in G : ax = xa\}$. It's evident that $a^n \in C_G(a)\ \forall\ n \in \mathbb{Z}$.*

Example 1.2.1 (Centralizer) *1. Determine $C_{Q_8}(i)$ for $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$.*

2. Calculate $C_{S_3}((123))$ and $C_{S_3}((12))$.

Definition .9 (Center) *The set*

$$Z(G) = \{g \in G : xg = gx\ \forall\ x \in G\}$$

is known as the Center of G.

Note 6 *$Z(G) = C_G(G)$, therefore $Z(G)$ is also a subgroup of G.*

Proposition .3 *If G is abelian, then $Z(G) = G$.*

Let's define a set $gAg^{-1} = \{gag^{-1} : a \in A\}$.

Definition .10 (Normalizer) *The normalizer of A in G is defined as the set*

$$N_G(A) = \{g \in G : gA = Ag \text{ (or) } gAg^{-1} = A\}$$

Remark 1 *1. If $g \in C_G(A) \Rightarrow g \in N_G(A)$. Thus, $C_G(A) \subseteq N_G(A)$.*

2. $N_G(A)$ is also a subgroup of G.

Proposition .4 *For an abelian group G, $N_G(A) = C_G(A) = G$ holds for any subset $A \subset G$.*

Exercise 9 *1. Find $C_{D_8}(A)$, where $A = \{1, r, r^2, r^3\}$.*

2. If $A \subseteq B$, then $C_G(B) \subseteq C_G(A)$.

Definition .11 (Stabilizer) *The set*

$$G_s = \{g \in G : g.s = s\}$$

is known as the stabilizer of s in G.

Proposition .5 *The stabilizer of s is a subgroup of G.*

Proof: *It is evident that if $x, y \in G_s$, then $x.s = s$ and $y.s = s$. Also,*

1. *$(xy)s = x(ys) = x(s) = s$*
2. *$y^{-1}(s) = y^{-1}(ys) = (y^{-1}y)s = 1.s = s$*

Therefore, $xy \in G_s$ and $y^{-1} \in G_s$. Consequently, G_s is a subgroup of G. ■

1.3. Cyclic Groups

Consider a group G and an element $x \in G$. One way to define a subgroup of G is by collecting all the possible powers of x, i.e.,

$$H = \{x^n : n \in \mathbb{Z}\}$$

where $x \in G$ is fixed.

Definition .12 (Cyclic Group) *A group G is referred to as a cyclic group if it is generated by a single element, i.e., $\exists\ x \in G$ such that $\forall\ y \in G$, $y = x^n$ for some $n \in \mathbb{Z}$.*

The element x is called a generator of G. We write $G =< x >$. A cyclic group may have more than one generator. For instance, if $H =< x >$, then $H =< x^{-1} >$ since $(x^{-1})^n = (x^n)^{-1} = x^{-n}$.

Example 1.3.1 *Consider a set G of 7^{th} roots of unity with the binary operation of multiplication, i.e., $G = \{1, \omega, \omega^2, \cdots, \omega^6 \ : \ \omega^7 = 1\}$. In this case, G forms a group. Moreover, G is a cyclic group generated by ω, thus $G =< \omega >$. Here, ω is a generator of G but not the only one. ω^2 can also generate the entire group G. Similarly, $\omega^3, \omega^4, \omega^5, \omega^6$ are also generators of G.*

Exercise 10 *Let $G = \{1, x, x^2, \cdots, x^8 \ : \ x^9 = 1\}$. Find the following:*

1. *Generators of G.*
2. *Order of all elements of G.*

Exercise 11 *If G is a cyclic group, then G is an abelian group.*

Note 7 *The converse may not hold true. For example, consider the K_4 group.*

Proposition .6 *If $|G| = |x| = n$, then $|x^a| = \frac{n}{(n,a)}$.*

Hint(s): *Let $y = x^a$ and $(n,a) = d \Rightarrow d|n, d|a \Rightarrow n = db$ and $a = dc$ where $(b,c) = 1$. Consider $y^b = (x^a)^b = x^{ab} = x^{dcb} = (x^n)^c = 1$. Hence, $|y||b$. Let $|y| = k$. Also, $x^{ak} = y^k = 1 \Rightarrow n|ak \Rightarrow db|dck \Rightarrow b|ck \Rightarrow b|k$ $((b,c) = 1) \Rightarrow b||y|$. Therefore, $|y| = b \Rightarrow |x^a| = \frac{n}{d} = \frac{n}{(n,a)}$.* ■

Note 8 *If $x \in G$ is a generator of G (finite cyclic group), it can generate all elements of G, implying $O(x) \geq O(G)$; but $O(x) \leq O(G) \Rightarrow O(x) = O(G)$.*

Proposition .7 *If $G =< x >$, then x^a is also a generator, and $|G| = n$ if and only if $(a,n) = 1$.*

Hint(s): *x^a is a generator of G if and only if $O(x^a) = O(x) = n \Leftrightarrow \frac{n}{(a,n)} = n \Leftrightarrow (a,n) = 1$. Thus, the number of generators of a cyclic group of order n is $\phi(n)$, where ϕ is Euler's ϕ-function.*

Exercise 12

1. *Every subgroup of a cyclic group is cyclic.*
2. *Find all the generators of $\mathbb{Z}_{12}$.*
3. *Find a subgroup of D_8 that is not cyclic. Find all the cyclic subgroups of D_8.*
4. *Check whether $U(10)$ is a cyclic group.*

1.4. Symmetric Groups

Definition .13 (Symmetric Group) *Given a finite set $S = \{1, 2, \cdots, n\}$, let S_n be the set of all bijections from S to itself, i.e., the set of all permutations of S. Under function composition $\circ$, which is a binary operation on S_n, associative, permutation 1 is the identity of S, and inverses exist for all $\sigma \in S_n$. This group is called the symmetric group on the set S.*

Note 9

1. *The set S can also be infinite.*
2. *S_n, for finite n, is also called the finite symmetric group of degree n.*

Since there are $n!$ permutations of $S = \{1, 2, \cdots, n\}$, then $|S_n| = n!$ since permutation is an injective map. Thus, there are n choices for 1, $n-1$ choices for 2 once 1 is fixed, and so on. In total, $n!$ such maps are possible.

To efficiently notate elements of S_n, a cyclic decomposition known as cycles is used.

Definition .14 (Cycle) *The cycle $(a_1\ a_2 \cdots a_m)$ is the permutation that sends $a_i \to a_{i+1}$ for $1 \leq i \leq m-1$, and $a_m \to a_1$.*

Example 1.4.1 $(1\ 2\ 3)$ *represents $1 \to 2$, $2 \to 3$, and $3 \to 1$.*

In general, the numbers from 1 to n will be rearranged and grouped into k cycles of the form (all a_i's distinct)

$(a_1\ a_2 \cdots a_{m_1})(a_{m_1+1} \cdots a_{m_2}) \cdots (a_{m_{k-1}} \cdots a_{m_k})$ *for an element* $\sigma \in S_n$. *The action of* σ *will be as follows:*

$$\sigma(x) = \begin{cases} \text{the integer appearing immediately to the right of } x \text{ if } x \text{ is not followed immediately by a right parenthesis} \\ \text{the integer at the start of the cycle ending with } x \text{ if } x \text{ is followed immediately by a right parenthesis} \end{cases}$$

The product of all the cycles is called the cycle decomposition of σ.

Example 1.4.2 (Cycle-decomposition) *In* S_{13}, *consider* σ=(1 12 8 10 4)(2 13)(3)(5 11 7)(6 9).

Note 10 *1. The length of a cycle is the number of integers that appear in it.*

2. A cycle of length t is called a t-cycle.

3. Two cycles are called disjoint if they have no numbers in common (they can commute).

In σ *above, there are 5 disjoint cycles: a 5-cycle, a 2-cycle, a 1-cycle, a 3-cycle, and another 2-cycle. For our convenience, we will not write a 1-cycle in-cycle decomposition. That is, if any integer is missing in the cycle decomposition, it is understood that* σ *fixes that integer. The identity permutation has the cycle decomposition* $(1)(2)\cdots(n)$ *and is denoted by* 1.

1.5. Cosets and Lagrange's Theorem

Definition .15 (Left coset) *Let G be a group, and let H be a subset of G. For any* $a \in G$, *define*

$$aH = \{ah : h \in H\}$$

When H is a subgroup of G, the set aH is called a left coset of H in G.

Similarly, $Ha = \{ha : h \in H\}$ *is called a right coset of H in G.*

Note 11 *In general, Ha (or) aH is not a subgroup of G.*

Example 1.5.1 *Let* $G = S_3$, *and* $H = \{(1), (1\ 3)\}$. *Then the left cosets of H in G are*

$$\begin{aligned} e * H &= H \\ (1\ 2) * H &= \{(1\ 2), (1\ 3\ 2)\} \\ (1\ 3) * H &= H \\ (2\ 3) * H &= \{(2\ 3), (1\ 2\ 3)\} \\ (1\ 2\ 3) * H &= \{(1\ 2\ 3), (2\ 3)\} \\ (1\ 3\ 2) * H &= \{(1\ 3\ 2), (1\ 2)\} \end{aligned}$$

Therefore, $(1\ 3\ 2) * H = (1\ 2) * H$, $(2\ 3) * H = (1\ 2\ 3) * H$, $e * H = (2\ 3) * H$.

In total, there are three left cosets of H in G.

Exercise 13 *1. Let* $G = D_4$, *and* $H = \{e, r^2\}$. *Find all the right cosets of H in G.*

2. Let $H = \{0, 3, 6\}$ *in* $\mathbb{Z}_9$ *under the operation of addition modulo 9. Find all the left cosets of H in* $\mathbb{Z}_9$.

Proposition .8 (Properties of Cosets) *Let H be a subgroup of G, and let* $a, b \in G$, *then*

1. $a \in aH$.
2. $aH = H$ *if and only if* $a \in H$.
3. $aH = bH$ *(or)* $aH \cap bH = \varnothing$.
4. $aH = bH$ *if and only if* $a^{-1}b \in H$.
5. $|aH| = |bH|$.
6. $aH = Ha$ *if and only if* $H = aHa^{-1}$.

7. *aH is a subgroup of G if and only if $a \in H$ i.e., $aH = H$.*

Hint(s):

1. *Since H is a subgroup, then $e \in H \Rightarrow ae = a \in aH$.*
2. *Suppose $aH = H \Rightarrow a = ae \in aH = H$. Conversely, suppose $a \in H \Rightarrow \forall h \in H$, $ah \in H$ (closure property) $\Rightarrow aH \subseteq H$. Also, let $h \in H \Rightarrow a^{-1}h \in H$ (as $a \in H \Rightarrow a^{-1} \in H$). Therefore, $h = eh = aa^{-1}h = a(a^{-1}h) \in aH \Rightarrow H \subseteq aH$. Hence, $aH = H$.*
3. *Suppose $aH \cap bH \neq \varnothing$. Let $x \in aH \cap bH$, then $\exists\ h_1, h_2 \in H$ such that $x = ah_1$ and $x = bh_2$. Thus, $a = xh_1^{-1}$ and so $a = (bh_2)h_1^{-1}$. Therefore, $aH = (bh_2h_1^{-1})H = b(h_2h_1^{-1})H = bH$ as $h_2h_1^{-1} \in H$.*
4. *By Property 2.*
5. *Since $|aH| = |H|$ as $\{ah_1, ah_2, \cdots, ah_m\}$ has distinct elements in H. Also $|bH| = |H|$. Therefore, $|aH| = |bH|$.* ■

1.6. Cosets and Lagrange's Theorem

Theorem .1 (Lagrange's Theorem) *If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $\frac{|G|}{|H|}$.*

Hint(s): *Let $a_1H, a_2H, \cdots, a_rH$ denote the distinct left cosets of H in G. Now, for all $a \in G$, we have $aH = a_iH$ for some $1 \leq i \leq r$. Also, since $a \in aH \Rightarrow \forall\ x \in G \Rightarrow x \in a_1H \cup a_2H \cup \cdots \cup a_rH \Rightarrow G \subseteq a_1H \cup a_2H \cup \cdots \cup a_rH$ but $a_1H \cup a_2H \cup \cdots \cup a_rH \subseteq G$ as $a_iH \subseteq G\ \forall\ a_i \in G$. Therefore, $G = a_1H \cup a_2H \cup \cdots \cup a_rH$.*

We know that, $|aH| = |bH|\ \forall\ a, b \in G$ and $aH \cap bH = \varnothing$ if $aH \neq bH \Rightarrow |G| = |a_1H| + |a_2H| + \cdots + |a_rH| = r|H| \Rightarrow r = \frac{|G|}{|H|}$.

Corollary .2 *$|a|\,||G|\ \forall\ a \in G$.*

Hint(s): *When $H = \langle a \rangle$, then $|H| = |a|$.*

Corollary .3 *Every group of prime order is cyclic.*

Corollary .4 *$a^{|G|} = e\ \forall\ a \in G$.*

Hint(s): *Since $|G| = |a|.k \Rightarrow a^{|G|} = a^{k|a|} = e^k = e$.*

Note 12 *In general, the converse of Lagrange's theorem is not true. If $n\,||G|$, then G may not have a subgroup of order n ($n \in \mathbb{Z}$).*

Example 1.6.1 *Let $G = A_4$, where A_4 is the alternating group of order 12. Now $6 \mid 12 = |G|$. If possible, assume that H is a subgroup of A_4 of order 6. A_4 has eight elements of order 3, which are*

$$A_4 = \left\{ \begin{array}{l} 1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1\,2\,3), (1\,2\,4) \\ (1\,3\,4), (2\,3\,4), (1\,3\,2), (1\,4\,2), (1\,4\,3), (2\,4\,3) \end{array} \right\}$$

elements of order 8 are all 3-cycles. The order of H is 6, implying that all 3-cycles do not belong to H. There exists $\sigma \in A_4$ such that σ is a 3-cycle and $\sigma \notin H$ ($\sigma \notin H \Leftrightarrow \sigma^2 \notin H$ and $\sigma^3 = 1$). The cosets of H in A_4 are H, σH, $\sigma^2 H$. But the total number of cosets of H in A_4 is 2, i.e., $\frac{|A_4|}{|H|} = 2$. Equality of any two cosets out of these three implies that $\sigma H = H \Leftrightarrow \sigma \in H$, which is a contradiction to our assumption.

1.7. Homomorphisms and Quotient Groups

Definition .16 (Homomorphism) *Let $(G, *)$ and $(H, \circ)$ be groups. A map $\phi : G \to H$ such that*

$$\phi(x * y) = \phi(x) \circ \phi(y)\ \forall\ x, y \in G$$

is called a homomorphism.

Definition .17 (Isomorphism) *The map $\phi : G \to H$ is called an isomorphism, and G, H are called to be isomorphic if*

1. *ϕ is a homomorphism*

2. ϕ *is a bijection.*

We write $G \cong H$ *if* G *and* H *are isomorphic.*

Definition .18 (Epimorphism) *A homomorphism which is also surjective is called an epimorphism.*

Definition .19 (Endomorphism) *A homomorphism of a group* G *onto itself is called an endomorphism.*

Definition .20 (Monomorphism) *A homomorphism which is also injective is called a monomorphism.*

Definition .21 (Automorphism) *An isomorphism of a group* G *onto itself is called an automorphism.*

Theorem .5 *Let* G *and* G' *be any two groups with identities* e *and* e' *respectively, then*

1. $f(e) = e'$
2. $f(x^{-1}) = (f(x))^{-1} \ \forall \ x \in G$

Hint(s):

1. *Since* $e * e = e \Rightarrow f(e * e) = f(e) \Rightarrow f(e) * f(e) = f(e) \Rightarrow f(e) = e'$.
2. *We know that* $x * x^{-1} = x^{-1} * x = e \Rightarrow f(x) * f(x^{-1}) = f(x^{-1}) * f(x) = e \Rightarrow f(x^{-1}) = (f(x))^{-1}$.

Definition .22 (Kernel) *Let* f *be a homomorphism of a group* G *into a group* G'*, then the kernel of* f *is the set*

$$\ker(f) = \{x \in G \ : \ f(x) = e'\}$$

where e' *is the identity in* G'.

Definition .23 *A subgroup* N *of* G *is said to be a normal subgroup of* G *if and only if for all* $g \in G$ *and* $n \in N$, $gng^{-1} \in N$, *and we denote it by* $N \trianglelefteq G$.

If $gNg^{-1} = \{gng^{-1} \ : \ n \in N\}$, *then* N *is normal if and only if* $gNg^{-1} \subset N \Rightarrow g^{-1}(gNg^{-1})g \subset gNg^{-1} \Rightarrow N \subset gNg^{-1} \Rightarrow N = gNg^{-1} \Rightarrow Ng = gN$. *Moreover,* G *has a normal subgroup* N *if and only if every left coset of* N *is a right coset of* N *in* G. *Conversely, if the left coset is also right, but both have* g *in common. Hence, they are* $Hg = gH$ *only.*

Definition .24 (Coset) *The collection of all (right/left) cosets of* N *in* G*, where* N *is a normal subgroup of* G*, then*

$$G/N = \{Na \ : \ a \in G\}$$

is a group under multiplication of cosets defined as

$$(Na)(Nb) = N(aN)b = N(Na)b = N(ab)$$

1. $\forall \ Na, Nb \in G/N \Rightarrow (Na)(Nb) = N(ab) \in G/N$, *since* $a, b \in G \Rightarrow ab \in G$.
2. *The associative law can be verified easily.*
3. $N = Ne \in G/N$ *and* $\forall \ X = Na \in G/N$ *for* $a \in G$, $XN = (Na)(Ne) = N(ae) = Na = X$. *Similarly,* $NX = X \Rightarrow Ne$ *is the identity element of* G/N.
4. $X = Na \in G/N$. *Consider* $Na^{-1} \in G/N$ *so that* $(Na)(Na^{-1}) = N(aa^{-1}) = Ne \Rightarrow Na^{-1} = (Na)^{-1} \in G/N$.

Hence G/N *is a group.*

Note 13 *The above theory can be understood without assuming* N *to be a normal subgroup of* G. *However, when* N *is a normal subgroup of* G, G/N *is called the quotient group (or factor group) of* G *by* N.

Clearly, $|G/N| = \frac{|G|}{|N|}$ *(by Lagrange's Theorem).*

Exercise 14

1. *Any subgroup* H *of index 2 in* G *is a normal subgroup of* G.
   - ***Hint(s):*** *Consider* H, Hx, $xH \Rightarrow Hx = xH$.
2. *The intersection of two normal subgroups of* G *is normal.*

3. *Let $H \subseteq G$ and $N \trianglelefteq G$, then $H \cap N \subseteq G$.*

4. *If H is the only subgroup in the finite group G, then H is normal.*

Theorem .6 *Any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$, and any infinite cyclic group is isomorphic to $\mathbb{Z}$.*

Hint(s): *If a is a generator of the cyclic group, then define*

$$f : G \to \mathbb{Z} \text{ (or) } \mathbb{Z}_n$$
$$a^k \to k$$

The map is an isomorphism and hence proves the result. ■

Corollary .7 *Any two cyclic groups of the same order are isomorphic.*

Note 14 *We know that $\phi(x) = x^3$ is a one-to-one and onto map, but not a homomorphism as $\phi(x+y) = (x+y)^3 \neq x^3 + y^3$, so ϕ is not an isomorphism.*

Example 1.7.1 *We know that $U(10) \cong \mathbb{Z}_4$ and $U(5) \cong \mathbb{Z}_4$. Since $U(10)$ and $U(5)$ are cyclic groups of order 4, we have $U(10) \cong U(5)$. However, $U(10) \ncong U(5)$, as $U(12) = \{1,5,7,11\}$, which is not a cyclic group. Moreover, if $\phi : U(10) \to U(12)$ is an isomorphism, then $\phi(9) = \phi(3).\phi(3) = (\phi(3))^2$ but $x^2 = 1,\ \forall\ x \in U(12) \Rightarrow \phi(9) = 2$. Also, $\phi(1) = 1 \Rightarrow \phi(9) = \phi(1)$, but $9 \neq 1$. This shows that ϕ is not a one-to-one map, which leads to a contradiction.*

Theorem .8 (Cayley's Theorem) *Every group is isomorphic to a group of permutations, i.e., for every group G, there exists a group $\bar{G}$ of permutations and an isomorphism $f : G \to \bar{G}$.*

Hint(s): *We claim that $f : G \to \bar{G}$ can be defined as follows: choose $a \in G$ and define $f_a : G \to G$ by $f_a(x) = ax\ \forall\ x \in G$, where f_a is a permutation on G. Now define $f(a) = f_a\ \forall\ a \in G$.*

Exercise 15 *Verify whether f, defined above, is indeed an isomorphism.*

Example 1.7.2 (Cayley's Theorem) *Let $G = U(12) = \{1,5,7,11\}$. Define the permutations $f_1 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 1 & 5 & 7 & 11 \end{pmatrix}$, $f_5 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 5 & 1 & 11 & 7 \end{pmatrix}$, $f_7 = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 7 & 11 & 1 & 5 \end{pmatrix}$, and $f_{11} = \begin{pmatrix} 1 & 5 & 7 & 11 \\ 11 & 7 & 5 & 1 \end{pmatrix}$. Now, let's define a map $f : U(12) \to \{f_1, f_5, f_7, f_{11}\}$ such that $1 \mapsto f_1$, $5 \mapsto f_5$, $7 \mapsto f_7$, and $11 \mapsto f_{11}$. This map is an isomorphism.*

Definition .25 (Natural Homomorphism) *Consider the map $\phi : G \to \frac{G}{N}$, where $N \trianglelefteq G$, defined as $\phi(a) = Na$ for all $a \in G$. For any $a, b \in G$, we can see that $\phi(ab) = N(ab) = (Na)(Nb) = \phi(a)\phi(b)$. Furthermore, for any $X \in G/N$, where $X = Na$ for some $a \in G$, there exists an $a \in G$ such that $\phi(a) = Na = X$. Thus, ϕ is a homomorphism from G onto G/N, and it's called the natural homomorphism.*

Proposition .9 *If $\phi : G \to G'$ is a homomorphism, then the kernel is defined as $\ker\phi := \{x \in G\ :\ \phi(x) = e'\}$, where e' is the identity of G'. The kernel K is a normal subgroup of G.*

Hint(s): *Let $x, y \in K$ where $K = \ker\phi$. This implies $\phi(x) = e' = \phi(y)$. Consider $\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)(\phi(y))^{-1} = e'.(e')^{-1} = e' \Rightarrow xy^{-1} \in K$. Now, for $g \in G$ and $k \in K$, it follows that $\phi(k) = e'$. Consider $\phi(gkg^{-1}) = \phi(g)\phi(k)(\phi(k))^{-1} = \phi(g)e'(\phi(g))^{-1} = \phi(g)(\phi(g))^{-1} = e' \Rightarrow gkg^{-1} \in K \Rightarrow K$ is normal.* ■

Proposition .10 *A homomorphism ϕ of G onto G' with kernel K is an isomorphism if and only if $K = \{e\}$.*

Hint(s): *Suppose ϕ is a homomorphism and $K = \{e\}$. Consider $\phi(a) = \phi(b)$ for some $a, b \in G$. Then, $\phi(a)(\phi(b))^{-1} = e' \Rightarrow \phi(a)\phi(b^{-1}) = e' \Rightarrow \phi(a.b^{-1}) = e' \Rightarrow ab^{-1} \in K = \{e\} \Rightarrow ab^{-1} = e \Rightarrow a = b$. Thus, ϕ is one-to-one, which implies that ϕ is an isomorphism.*

Theorem .9 *Let ϕ be a homomorphism of G onto G' with kernel K. Then, $G/K \cong G'$.*

Proof: *Exercise.*

Theorem .10 *Let ϕ be a homomorphism of G onto G' with kernel K. Suppose $N \trianglelefteq G$ and $N = \{x \in G\ :\ \phi(x) \in N\}$. Then, $G/N \cong G'/N$ or equivalently $G/N \cong \frac{G/K}{N/K}$.*

Proof: *Define a map* $f : G \to \frac{G'}{N}$ *such that* $a \mapsto \bar{N}\phi(a)$. *The homomorphism property of* f *can be shown as* $f(ab) = \bar{N}\phi(ab) = \bar{N}\phi(a)\phi(b) = \bar{N}\phi(a)\bar{N}\phi(b) = f(a).f(b)$. *Additionally, for any* $\bar{N}a' \in \frac{G'}{N}$ *where* $a' \in G'$, *we can find* $a \in G$ *such that* $\phi(a) = a'$, *resulting in* $f(a) = \bar{N}\phi(a) = \bar{N}a'$. *By the fundamental theorem,* $G \to \frac{G'}{N}$ *is a homomorphism and onto map, so* $\frac{G}{\ker f} \cong \frac{G'}{N}$ *where* $\ker f = \{a \in G : f(a) = \bar{N}\} = N$. *Hence the result.* ■

Hint(s): *Since* $\ker\phi = K$ *is a normal subgroup of G, prove that* $\frac{N}{K}$ *is a subgroup of* $\frac{G}{K}$ *(given* $K \subseteq N$, *then show it). Using the natural homomorphism* $f : G \to \frac{G}{K}$ *and* $f^{-1}(\frac{N}{K}) = N$, *apply the previous result to deduce* $\frac{G}{N} \cong \frac{\frac{G}{K}}{\frac{N}{K}}$.

Proposition .11 (Product of Two Subgroups) *Let H and K be two subgroups of a group G. The product of H and K is defined as*

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

is a subgroup of G if and only if $HK = KH$.

Proof: *Suppose HK is a subgroup of G. Consider* $(kh)^{-1} = h^{-1}k^{-1} \in HK$ *for* $h \in H,\ k \in K$. $\Rightarrow (kh)^{-1} \in KH \Rightarrow kh \in HK \Rightarrow KH \subseteq HK$. *Similarly,* $HK \subseteq KH \Rightarrow KH = HK$.

Conversely, let $HK = KH$. *Clearly, HK is non-empty as* $e \in HK$. *Let* $x, y \in HK$, *then* $x = h_1k_1$ *and* $y = h_2k_2 \Rightarrow xy^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1}$. *Also,* $(k_1k_2^{-1})h_2^{-1} \in KH(= HK) \Rightarrow (k_1k_2^{-1})h_2 = h_3k_3 \in HK \Rightarrow xy^{-1} = h_1(h_3k_3) = (h_1h_3)k_3 \in HK \Rightarrow HK$ *is a subgroup of G.* ■

Corollary .11 1. *If H and K are two subgroups of G, and either H or K is normal in G, then HK is a subgroup of G.*

2. *If G is abelian, then HK is a subgroup for* $H, K \subseteq G$.

Theorem .12 *If H and K are finite subgroups of a group G, then*

$$O(HK) = \frac{O(H) \cdot O(K)}{O(H \cap K)}$$

Proof: *Let* $D = H \cap K$. *If* $K = \sum_{i=1}^{k} DK_i$ *is the decomposition of K into disjoint right cosets of D in K (where D need not be normal), then* $t = \frac{O(K)}{O(D)}$. *Furthermore,* $HK = H(\sum_{i=1}^{t} DK_i) = \sum_{i=1}^{t} HDK_i = \sum_{i=1}^{t} HK_i$. *Verify that* Hk_i, $i = 1, 2, \ldots, t$ *are pairwise disjoint and distinct. Since* HK_i*'s are all disjoint right cosets of H in HK,*

$$\begin{aligned} O(HK) &= t \cdot O(H) \\ &= O(H) \cdot \frac{O(K)}{O(D)} = \frac{O(H) \cdot O(K)}{O(H \cap K)} \end{aligned}$$

Theorem .13 (Second Isomorphism Theorem) *Let H be a normal subgroup of a group G, and K be any subgroup of G. Then,*

$$\frac{K}{H \cap K} \simeq \frac{HK}{K}$$

Proof: *Firstly,* $\frac{HK}{K}$ *is well defined. Let us define the homomorphism:*

$$\begin{aligned} f : K &\to \frac{HK}{K} \\ k &\mapsto Hk \end{aligned}$$

Thus, f is a homomorphism. By the Fundamental Theorem, we have

$$\frac{K}{\ker f} \simeq \frac{HK}{H}$$

where

$$\ker f = \{x \in K \,:\, f(x) = H\} = \{x \in K \,:\, Hx = H\} = \{x \in K \,:\, x \in H\} = H \cap K$$

Hence the result. ■

Exercise 16 *Let G be a group such that $\frac{G}{Z(G)}$ is cyclic. Show that G is abelian.*

Hint(s): *For $a, b \in G \Rightarrow aZ \in < gZ >$ where $Z = Z(G)$. Thus, $aZ = (gZ)^k = g^kZ$ and $bZ = g^lZ$, and so*

$$ab = n_1 g^k n_2 g^l = n_1 n_2 g^{k+l}$$
$$ba = n_2 g^l n_1 g^k = n_1 n_2 g^{k+l}$$

1.8. Conjugacy and Class Equation

Definition .26 *Let G be a group, and $a, b \in G$. An element $a \in G$ is said to be a conjugate of b in G if there exists $c \in G$ such that $a = c^{-1}bc$.*

Note 15 *If a is a conjugate of b, then b is also a conjugate of a, as $b = (c^{-1})^{-1}ac^{-1}$ for $c^{-1} \in G$.*

We denote $a \sim b$ if a is a conjugate of b. The relation $\sim$ is an equivalence relation, i.e.,

1. $a \sim a$
2. $a \sim b \Rightarrow b \sim a$
3. $a \sim b,\ b \sim c \Rightarrow a \sim c$

Every equivalence relation on a set can divide it into equivalence classes, forming a partition of the set. Let $[a]$ or $C_l(a)$ denote the conjugate class of a, i.e.,

$$C_l(a) = \{b \mid b \sim a\}$$
$$= \{x^{-1}ax \mid x \in G\}$$

Note 16 *For a group G, $C_l(a) = \{a\}$ if and only if $a \in Z(G)$.*

If G is a finite group, and $C_l(a_1), C_l(a_2), \ldots, C_l(a_n)$ are all the conjugate classes of G, let M be a set consisting of representatives of $C_l(a_i)$ for all i, i.e., $M = \{a_1, a_2, \ldots, a_n\}$. Let C_a denote the number of elements in $C_l(a)$, then $|G| = \sum_{a \in M} C_a$.

Recall $N(a) = \{x \in G \mid xa = ax\}$, which is the normalizer of a or the centralizer of a. We know that $N(a) = G \Leftrightarrow a \in Z(G)$ (the center of G), and $N(a)$ is a subgroup of G. It's important to note that $N(a)$ does not necessarily need to be a normal subgroup. We define a map :

$$\phi : \frac{G}{N(a)} \to C_l(a) \text{ by}$$
$$xN(a) \mapsto x^{-1}ax$$

Thus, ϕ is well-defined, for $xN(a) = yN(a) \Rightarrow xy^{-1} \in N(a) \Rightarrow xy^{-1}a = axy^{-1} \Rightarrow x^{-1}ax = y^{-1}ay \Rightarrow \phi(xN(a)) = \phi(yN(a))$. It can be checked that ϕ is one-to-one and onto. Hence, there is a one-to-one correspondence between $\frac{G}{N(a)}$ and $C_l(a)$. This implies $\frac{O(G)}{O(N(a))} = C_a$. Therefore, we have

$$|G| = \sum_{a \in M} \frac{O(G)}{O(N(a))}$$

If $a \in Z(G) \Leftrightarrow N(a) = G \Leftrightarrow C_a = 1$, then

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$$

*The above equation is known as the **class equation** of a group G.* ■

Example 1.8.1 *Verifying the class equation for $G = S_3$. By referring to the composition table of S_3, we have:*

$$C_l((1\,2)) = \{(1\,2),(1\,3),(2\,3)\} \text{ and } N((1\,2)) = \{1,(1\,2)\}$$
$$C_l((1\,2\,3)) = \{(1\,2\,3),(1\,3\,2)\} \text{ and } N((1\,2\,3)) = \{1,(1\,2\,3),(1\,3\,2)\}$$
$$C_l(1) = \{1\} \Rightarrow \text{so } |Z(G)| = 1$$

Since $|G| = 6$, we can compute: $\frac{O(G)}{O(N(1\,2))} = \frac{6}{2} = 3$ and $\frac{O(G)}{O(N(1\,2\,3))} = \frac{6}{3} = 2$.

The class equation can be verified:

$$|G| = |Z(G)| + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$$
$$6 = 1 + \frac{O(G)}{O(N(1\,2))} + \frac{O(G)}{O(N(1\,2\,3))}$$
$$6 = 1 + 3 + 2$$

Exercise 17 *Verify the class equation for D_4, where D_4 is the dihedral group of order 8.*

Exercise 18 *For any permutations σ and τ belonging to the symmetric group S_n, the cycle types of $\sigma^{-1}\tau\sigma$ and τ are identical.*

Hint(s): *Let $\sigma, \tau \in S_n$, where $\tau = (a_1 a_2 \ldots a_k)$ represents a k-cycle. Then prove it:*

$$\sigma\tau\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\ldots\sigma(a_k)).$$

Exercise 19 *Assume $\sigma, \tau \in S_n$ with $\tau = (a_1 a_2 \ldots a_{m_1})(b_1 b_2 \ldots b_{m_2})\ldots$ representing a finite product of disjoint cycles. Then,*

$$\sigma\tau\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\ldots\sigma(a_{m_1}))(\sigma(b_1)\sigma(b_2)\ldots\sigma(b_{m_2}))\ldots$$

1.8.1. Application(s) of Class Equation

Theorem .14 *If $O(G) = p^n$ for some prime p and positive integer n, then $Z(G) \neq \{e\}$.*

Proof: *Since $O(G) = O(Z(G)) + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$, i.e., $p^n = O(Z(G)) + \sum_{a \notin Z(G)} \frac{O(G)}{O(N(a))}$. Suppose, for the sake of contradiction, that $Z(G) = \{e\}$, meaning $O(Z(G)) = 1$. Therefore, for any $(e \neq)a \in G$, we have $N(a) \neq G$ and $N(a) \subseteq G$. This implies that $O(N(a)) \neq p^n$. Consequently, $\frac{O(G)}{O(N(a))} = p^t$, $t \geq 1$ $(t = n - k)$. Since $\frac{O(G)}{O(N(a))}$ is divisible by p, $O(Z(G))$ should also be divisible by p, which contradicts the assumption that $p \nmid O(Z(G)) = 1$. Therefore, we conclude that $Z(G) \neq \{e\}$.* ■

Corollary .15 *Let $O(G) = p^2$. Then G is abelian.*

Proof: *Since $Z(G) \neq \{e\}$, we have $O(Z(G)) = p$ or p^2.*

1. *If $O(Z(G)) = p^2$, then $Z(G) = G$, and therefore, G is abelian.*
2. *If $O(Z(G)) \neq p^2$, then $O(Z(G)) = p \neq O(G)$. There exists $a \in G$ such that $a \notin Z(G)$, and so $N(a) \neq G$. Moreover, for $b \in Z(G)$, $b \in N(a) \Rightarrow Z(G) \subseteq N(a)$. However, $a \in N(a)$ but $a \notin Z(G)$, implying $O(Z(G)) < O(N(a))$, and thus $O(N(a)) = p^2 = O(G)$. This contradicts the fact that $N(a) \neq G$.* ■

1.9. Generating Set

If we generalize the concept of a generator of a cyclic group, we obtain the concept of a generating set.

Definition .27 *Let S be a subset of a group G. A subgroup H of G is said to be generated by S if*

1. *$S \subseteq H$*
2. *If K is any subgroup of G such that $S \subseteq K$, then $H \subseteq K$ i.e., H is the smallest subgroup containing S.*

We denote this subgroup H as $< S >$.

Proposition .12 *A subgroup H containing the set S of group G is said to be generated by S if it is the intersection of all subgroups of G containing S.*

Proof: *If $K = \cap H_i$ where $S \subseteq H_i$, and H_i's are subgroups of G, then $K \subseteq H =< S >$. Furthermore, K contains S since $S \subseteq H_i$, and since K is a subgroup, we have $H \subseteq K \Rightarrow H = K$.*

The family of H_i is definitely not empty as $G = H_i$, since $G \subseteq G$ and $S \subseteq G$. For a subset S of G, G itself can be a subgroup generated by S, in which case S is called a set of generators for G. In particular, if $G = \langle a \rangle$ is a cyclic group, then $S = \{a\}$ is a set of generators for G. If $S \neq \varnothing$ is a subset of G, then

$$H = \langle S \rangle = \{a_1 a_2 \cdots a_n \ : \ a_i \in S \text{ or } a_i^{-1} \in S\}$$

Exercise 20 *Prove that H is a subgroup of a G containing S.*

Example 1.9.1 *1. Let A be the set of all transpositions in the symmetric group S_n. Then, A generates S_n.*

2. *Consider $S_3 = \{1, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}$. Let $a = (1\ 2)$ and $b = (1\ 2\ 3)$. It follows that $S_3 = \langle A \rangle$, where $A = \{a, b\}$. Since $ba = (1\ 3)$, $ab = (2\ 3)$, and $b^2 = (1\ 3\ 2)$.*

3. *Let $G = \{\pm 1, \pm i, \pm j, \pm k\}$. Then, $G = \langle \{i, j\} \rangle$.*

Definition .28 *Consider $H = \langle a^{-1}b^{-1}ab \ : \ a, b \in G \rangle$, where G is a group. H is called the commutator subgroup of G.*

Exercise 21 *1. Prove that H is a normal subgroup of G.*

2. *For any normal subgroup N of G, G/N is abelian if and only if $H \subseteq N$.*

Hint(s):

1. *To prove that H is a normal subgroup of G, consider $H = \langle a^{-1}b^{-1}ab \ : \ a, b \in G \rangle$. If $x \in H$, then $x = g_1 g_2 \cdots g_r$ where each g_i is a commutator in G for all i. Thus, $x, y \in H \Rightarrow xy \in H$. Also, $(a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba$ is again a commutator. This shows that $x \in H$ implies $x^{-1} \in H$. For $x \in H$ and $a \in G$, consider $a^{-1}xa = a^{-1}(g_1 g_2 \cdots g_r)a$. Each $a^{-1}g_i a$ is a commutator, and this shows that $a^{-1}xa \in H$. Hence, H is a normal subgroup of G.*

2. *Furthermore, if G/N is abelian (i.e., $(aN)(bN) = (bN)(aN)$ for all $a, b \in G$), then $H \subseteq N$. Conversely, if $H \subseteq N$, then $a^{-1}b^{-1}ab \in N$ for all $a, b \in G$. This implies that G/N is abelian.*

Proposition .13 *A group G is abelian if and only if $H = \{e\}$, where H is the commutator subgroup of G.*

For convenience, we write the commutator subgroup of G as G'.

Exercise 22 *1. Prove that for $G = S_3$, we have $G' = A_3$.*

2. *Let $H, K \subseteq G$. If $H \subseteq K$, then $H' \subseteq K'$.*

3. *If N is a normal subgroup of a group G and $N \cap G' = \{e\}$, then $N \subseteq Z(G)$.*