

CHAPTER TWO

SPECIAL SUBGROUPS AND FACTOR GROUPS

1. INTRODUCTION

Subgroups play a significant role in the theory of groups. They are like building blocks from which groups of larger size can be constructed. The process can also be reversed. That is, if a group under investigation is difficult to comprehend because of its nature or large size, we have techniques to reduce it to a group of smaller size. We can then identify this reduced group with an already known group and achieve our objective. A group can be reduced by factorizing it through its subgroups. But this subgroup has to be a special one. Another important relationship between a group and its subgroup is that the order of a group is multiple of the order of its subgroup.

This chapter is devoted to the study of special types of subgroups, called normal subgroups and their relationship with their respective groups. Some special normal subgroups and the respective factor groups (or quotient groups) are also described.

2. COSETS AND LAGRANGE'S THEOREM

In chapter one we considered two subgroups H and K of a group G and defined their product as $HK = \{hk : h \in H, k \in K\}$. If we take H to be a singleton set $\{h\}$ and write hK instead of $\{h\}K$, then the set hK is called left coset of K in G . Here, K is a subgroup of G and hK is a set. In a similar fashion, a right coset of a subgroup in a group can be defined. That is, the right coset of a subgroup H in a group G is Hk where $k \in K \leq G$. Notice that a coset is a right or left coset such that the element x is on the right or left of a subgroup H of a group G . In the case where the group G is a group under addition, a left coset of a subgroup H in G is written as $g + H = \{g + h : h \in H\}$.

Let us consider a few examples to illustrate these concepts.

Example 2.2.1

Consider a subgroup $H = \{1, x^2\}$ of a group $C_4 = \langle x : x^4 = 1 \rangle$. Then $1H = \{1, x^2\}$, $xH = \{x, x^3\}$, $x^2H = \{x^3, x\}$ are the left cosets of H in C_4 . Since $1H = x^2H$ and $xH = x^3H$, there are in fact two left cosets of H in C_4 , namely H and xH .

Example 2.2.2

The left cosets of $H = \{1\}$ in $V_4 = \langle x, y : x^2 = y^2 = (xy)^2 = 1 \rangle$ are $1H$, xH , yH , xyH . Thus, the singleton sets $\{1\}$, $\{x\}$, $\{y\}$ and $\{xy\}$ are the left cosets of H in V_4 .

Example 2.2.3

Let us determine the left cosets of the subgroup $C_2 = \langle x : x^2 = 1 \rangle$ of $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$. Amongst $1C_2$, xC_2 , yC_2 , y^2C_2 , xyC_2 and xy^2C_2 the following three left cosets: C_2 , yC_2 , y^2C_2 are the distinct left cosets of C_2 in S_3 .

We recall that a family of subsets of a set X is a partition of X if they are non-empty, disjoint and their union is X . Next we want to show that the left cosets of a subgroup H of a group G form a partition of G by H . In other words, we intend to show that the union of all the left cosets of H in G is G itself and any pair of distinct cosets has empty intersection. We achieve this in the following theorem.

Theorem 2.2.4

If G is a group and $H \leq G$, then the left cosets of H in G form a partition of G by H .

Proof

Each gH is non-empty because $1 \in H$ and $g = g.1$. Let us show that $G = \bigcup_{g \in G} gH$. Since $gH \subseteq G$, therefore $\bigcup_{g \in G} g \subseteq gH$. Conversely, let $g \in G$ then $g = g.1$ implies that $g \in gH$, as $H \leq G$. This means that $\bigcup_{g \in G} \{g\} \subseteq \bigcup_{g \in G} gH$. But $\bigcup_{g \in G} \{g\} = G$. The two inclusions therefore imply that $G = \bigcup_{g \in G} gH$.

Let us now proceed to show that any pair of left cosets is either disjoint or they are equal. Consider two left cosets g_1H and g_2H with $g_1, g_2 \in G$ and $g_1H \cap g_2H \neq \emptyset$. Let $x \in g_1H \cap g_2H$. Then $x = g_1h_1 = g_2h_2$ for some $h_1, h_2 \in H$. This implies that $g_1 = g_2h_2h_1^{-1}$ because $H \leq G$ and $h_1 \in H$. Take now an arbitrary element $y \in g_1H$. Then $y = g_1h_3$, for some $h_3 \in H$. But $g_1 = g_2h_2h_1^{-1}$; so $y = (g_2h_2h_1^{-1})h_3 = g_2(h_2h_1^{-1}h_3)$. This implies that $y \in g_2H$ because $h_2h_1^{-1}h_3 \in H$. Hence $g_1H \subseteq g_2H$. A similar argument with h_1, h_2 and g_1, g_2 interchanged shows that $g_2H \subseteq g_1H$. Thus the two inclusions imply, that $g_1H = g_2H$. Hence any two left cosets are either disjoint or identical.

We require the following lemma for the proof of Lagrange's theorem.

Lemma 2.2.5

If G is a finite group and $H \leq G$, then for every $g \in G$, $|gH| = |H|$.

Proof

Obviously, H is finite being a subset of a finite set. Without any loss of generality, we can therefore suppose that $H = \{h_1, h_2, \dots, h_n\}$ where n is a positive integer and $h_i \neq h_j$, for $i \neq j$ and $i, j = 1, 2, \dots, n$. Now $gH = \{gh_1, gh_2, \dots, gh_n\}$; and we claim that no two elements of gH are the same. For otherwise, suppose $gh_i = gh_j$ for $i \neq j$. Then since $g \in G$, $g^{-1}gh_i = g^{-1}gh_j$ implies that $h_i = h_j$ for $i \neq j$. This contradicts the

very definition of H . Hence no two elements of gH are equal. This shows that gH also has n distinct elements. That is $|gH| = |H|$.

The following theorem is commonly known as Lagrange's theorem, but that is the name, not an attribution. Although it was J.L.Lagrange who, in a great memoir published in 1770, started the line of thinking that led to finite group theory. His own ideas were very tentative and fell far short of the result that now bears his name. A satisfactory understanding of groups, sub-groups and 'Lagrange's Theorem' (which acquired that name only later, C. 1870) appears to have been achieved first by E.Galois (C. 1830, who was then about 18 years old) and became more widely available in the years 1845-1850.

Theorem 2.2.6

If G is a finite group and $H \leq G$, then $|H|$ divides $|G|$.

Proof

Let there be n distinct left cosets g_1H, g_2H, \dots, g_nH of H in G . Then, by theorem 2.2.4, $G = \bigcup g_iH$ and $g_iH \cap g_jH = \emptyset$ for $i \neq j$ imply that $|G| = |g_1H| + |g_2H| + \dots + |g_nH|$. But due to lemma 2.2.5, $|g_iH| = |H|$, for all $i = 1, 2, \dots, n$. Thus $|G| = |H| + |H| + \dots + |H|$, n -times. This means that $|G| = n|H|$; and so $|H|$ divides $|G|$.

The number n is called the index of H in G and is denoted by $|H : G|$. It obviously means the number of left cosets of H in G . Thus, under this new notation, theorem 2.2.6 takes the form $|G| = |H : G||H|$.

Let us consider a few simple examples to see the implications of theorem 2.2.6.

Example 2.2.7

Reconsider the group $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$ and its subgroups (determined in example 1.5.2), namely $\{1\}, \{1, x\}, \{1, y, y^2\}, \{1, xy\}, \{1, xy^2\}, S_3$. These subgroups are of order 1, 2, 3, 2, 2, and 6 respectively. The orders of these subgroups are of course divisors of $|S_3| = 6$.

Example 2.2.8

The dihedral group $D_8 = \langle x, y : x^2 = y^4 = (xy)^2 = 1 \rangle$, of order 8, does not have a subgroup of order 3 because 3 is not a divisor of $|D_8| = 8$. The subgroups of D_8 are: $\{1, x\}, \{1, y^2\}, \{1, xy\}, \{1, xy^2\}, \{1, xy^3\}, \{1, y, y^2, y^3\}, \{1, y^2, x, xy^2\}, \{1, y^2, xy, xy^3\}$.

Example 2.2.9

The set $Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ is a group under addition (the non-zero elements of Z_5 form a group under multiplication also). The only subgroups of Z_5 are $\{0\}$ and $\{Z_5\}$ because $|Z_5| = 5$ and 5 being a prime number has no positive divisors other than 1 and 5.

It is important to note here that the converse of Lagrange's theorem is not true in general. That is, if G is a group of finite order and d is a divisor of $|G|$ then it is not necessary that G will contain a subgroup H such that $|H| = d$. The following example shows that the converse of Lagrange's theorem is not true in general.

Example 2.2.10

If $x = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, y = \begin{bmatrix} \omega & 0 \\ 0 & \omega^2 \end{bmatrix}$ where $i^2 = -1$ and $\omega^3 = 1$, then the group $M = \langle x, y : x^4 = y^3 = 1, yx = xy^2 \rangle$ is of order 12 and has one subgroup of order 3, necessarily cyclic and three non-cyclic subgroups of order 4, and two improper subgroups of course. Note that 6 divides $|M|$ but M does not have a subgroup of order 6. This shows that the converse of Lagrange's theorem is not true in general.

Lagrange's theorem has some important and useful corollaries. Before we present these we consider the following class of groups. Applications of Lagrange's theorem in this class of groups yield interesting results.

3. CYCLIC GROUPS

A group generated by a single element is called a cyclic group. If x is a generator of a group G then the cyclic group G can be expressed as $\langle x \rangle$. The group G will contain powers of x . That is $G = \langle x \rangle = \{x^i : i = 0, 1, 2, \dots\}$. If G is finite, of order n , then the finite presentation of G will be $\langle x : x^n = 1 \rangle$. Thus for every positive integer n , there always corresponds a cyclic group of order n .

The following examples will highlight some of the features of finite and infinite cyclic groups.

Example 2.3.1

For every positive integer n , the set of complex n -th roots of 1, namely $C_n = \{1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \dots, e^{\frac{2(n-1)\pi i}{n}}\}$, forms a subgroup C_n of a group C^\times of non-zero complex numbers under multiplication. The group C_n is of order n and it is generated by $e^{\frac{2\pi i}{n}}$. That is, $C_n = \{e^{\frac{2\pi mi}{n}} : m = 0, 1, 2, \dots, n-1\}$.

How an infinite cyclic group can be constructed is explained in the following example.

Example 2.3.2

For any $z \in C^\times \setminus \bigcup_{n=1}^{\infty} C_n$, the cyclic subgroup $\langle z \rangle$ of C^\times is infinite. Sometimes an infinite cyclic group is denoted by C_∞ . Notice that $1 \in C_\infty$ and $1 \in \bigcup_{n=1}^{\infty} C_n$. Since 1 is the multiplicative identity therefore it has no finite order and so belongs to C_∞ .

Example 2.3.3

The set of integers \mathbb{Z}^+ is a cyclic group (under addition) of infinite order and $\mathbb{Z}^+ = \langle 1 \rangle$.

A generator of a cyclic group may not be unique, as can be seen from the following example.

Example 2.3.4

The group $G = \{1, -1, i, -i\}$, as considered in example 1.2.6, is a cyclic group of order 4 and its generator is i or $-i$. That is $G = \langle i \rangle$ or $G = \langle -i \rangle$.

We have already made several references to cyclic groups, and are now going to investigate them thoroughly. It is important to note that all the finite cyclic groups may be divided into two kinds: those for which the order is prime, and those for which it is composite. The former, like C_5 , are in most respects less interesting, chiefly because they have no subgroups. Cyclic groups of composite order are more rewarding to study.

Theorem 2.3.5

Every cyclic group is Abelian.

Proof

Let G be a cyclic group generated by x . If $g_1, g_2 \in G$, then g_1 and g_2 are powers of x . That is, $g_1 = x^n$ and $g_2 = x^m$ for some positive integers n and m . Thus $g_1 g_2 = x^n x^m = x^{n+m} = x^{m+n} = x^m x^n = g_2 g_1$ show that G is Abelian.

The following theorem is significant due to its wide uses. It also explains the structure of subgroups of a cyclic group.

Theorem 2.3.6

- (i) Every subgroup of a cyclic group $\langle x \rangle$ is cyclic.
- (ii) there is just one cyclic subgroup C_m of C_n for each divisor m of n ,

(iii) $C_m = \langle x^{\frac{n}{m}} \rangle$ and these are all the subgroups of C_n .

Proof

(i) Suppose G is a cyclic group generated by x and $H \leq G$. If $H = \{1\}$, then H is trivially cyclic. Let $H \neq \{1\}$ and $y \neq 1 \in H$. Then $y = x^s$ for some integer s , and $y^{-1} = x^{-s} \in H$. Thus there are positive integers t such that $x^t \in H$. Choose least positive integer l . Let $y \in H$. Then $y = x^s$ for some s . Write $s = ql + r$, $0 \leq r < l$. Then $y = x^{ql+r} = x^{ql}x^r$ implies that $x^r = x^{-ql}y = (x^l)^{-q}y \in H$. If $r \neq 0$, then $r < l$ contradicts the choice of l . Thus $r = 0$. Then $y = (x^l)^q$ implies that $y \in \langle x^l \rangle$. That is $H \subseteq \langle x^l \rangle$.

Conversely, $x^l \in H$ implies that $\langle x^l \rangle \subseteq H$. Combining the two inclusions, we conclude that $H = \langle x^l \rangle$.

(ii) If $G = \langle x \rangle$ is of finite order n , we can use our standard notation to denote it by C_n . Now, $x^n = 1 \in H$, and so by taking $s = n$ in the above equation, $n = ml$ for some m . Hence $l = \frac{n}{m}$ and the order of x^l is m . Thus H is of order m , whence $H = C_m = \langle x^{\frac{n}{m}} \rangle$.

(iii) Now suppose m divides n . Then $\{x^{\frac{n}{m}}, x^{\frac{2n}{m}}, \dots, x^{\frac{mn}{m}} = 1\}$ is a cyclic subgroup of order m . Hence to each divisor m of n , there corresponds just one subgroup $C_m = \langle x^{\frac{n}{m}} \rangle$ of order m . The above argument shows that these are all the subgroups of C_n .

Let us illustrate theorem 2.3.6 through the following examples.

Example 2.3.7

Consider the cyclic group C_{24} . Corresponding to the divisors 1,2,3,4,6,8,12,24 of 24 we have the subgroups $C_1, C_2, C_3, C_4, C_6, C_8, C_{12}$ and C_{24} of C_{24} .

Example 2.3.8

The group $Z_7 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$ is a cyclic group of order 7 under the operation of addition modulo 7. The group Z_7 has no proper subgroup because 7 has no divisors other than 1 and 7. Note also that $Z_7 = \langle \bar{1} \rangle = \langle \bar{2} \rangle = \langle \bar{3} \rangle = \langle \bar{4} \rangle = \langle \bar{5} \rangle = \langle \bar{6} \rangle$.

Example 2.3.9

Reconsider the cyclic group $G = \{1, -1, i, -i\}$. Recall that $G = \langle i \rangle$. Now, corresponding to the divisors 1,2,4 of $|G|$ the subgroups of G are: $\{1\}, \{1, -1\}, \{1, -1, i, -i\}$. Also, $\{1, -1\} = \langle i^2 \rangle$.

It is important to note that if we have a set of say n objects which satisfy all the requirements of a group, then if one of the elements is of order n , we can be sure that the group is C_n . Here is a theorem to this effect.

Theorem 2.3.10

If $G = \langle x \rangle$ is of finite order then $|G| = \text{ord}(x)$.

Proof

If we let $\text{ord}(x) = n$, then $x^n = 1$. This means that the group G , which contains the powers of x , has at most n elements. If it should actually have fewer than n elements, then $x^i = x^j$ for some integers i, j such that $0 \leq i < j < n$. Then $x^{j-i} = 1$, yet $0 < j-i < n$ which would contradict the very meaning of order of x . Thus $|G| = n$, that is, $|G| = \text{ord}(x)$.

Lagrange's theorem yields another interesting and useful result.

Theorem 2.3.11

The order of an element of a finite group G divides the order of G .

Proof

Suppose $|G| = n$, and $x \in G$. Then $\langle x \rangle \leq G$. By Lagrange's theorem, $|\langle x \rangle| = \text{ord}(x)$ divides $|G|$.

As an illustration of this theorem, recall from example 2.2.7 that S_3 has elements $1, x, y, y^2, xy, xy^2$ of orders $1, 2, 3, 3, 2, 2$; which of course are the divisors of $|S_3| = 6$.

The theorem 2.3.11 has the following easy corollary.

Corollary 2.3.12

If G is a finite group and $x \in G$ then $x^{|G|} = 1$.

Proof

By theorem 2.3.11, $\text{ord}(x)$ divides $|G|$ and so $|G| = m \text{ord}(x)$. Thus $x^{|G|} = x^{m \text{ord}(x)} = (x^{\text{ord}(x)})^m = 1^m = 1$.

Experience has shown that application of group theoretic techniques to problems in other disciplines has often made things easier. Before we show how this goes in the following result of number theory, we need to know that what we mean by Euler's φ -function.

The Euler's φ -function, $\varphi(n)$, is defined for all positive integers n . If $n = 1$, then $\varphi(1) = 1$ and if $n > 1$, then $\varphi(n)$ is the number of positive integers less than n and relatively prime to n . Thus, for example, $\varphi(6) = 2$, since only 1 and 5 are the numbers less than 6 which are relatively prime to 6.

Theorem 2.3.13

If n is a positive integer and x is relatively prime to n , then $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Proof

Note that the positive integers less than n and relatively prime to n form a group under multiplication modulo n . This group, of course, has order $\varphi(n)$. If we apply corollary 2.3.12 to this group, we obtain $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Theorem 2.3.14

If G is a finite group of prime order then G is cyclic.

Proof

Let p be a prime number and $|G| = p$. Suppose $x \neq 1 \in G$ and $H = \langle x \rangle$. Then $H \leq G$ and $H \neq \{1\}$ because $x \neq 1 \in H$. Now, by Lagrange's theorem, $|H|$ divides p . This means that either $|H| = 1$ or $|H| = p$. But $|H| \neq 1$ because $H \neq \{1\}$. Thus, $H = G$. This shows that G is cyclic being generated by a single element x .

The concept of normal subgroup dominates the whole group theory. This is due to the E. Galois who recognized the importance of such subgroups. The following section is devoted to normal subgroups.

4. NORMAL SUBGROUPS

If G is a large group and we want to reduce it to a smaller group, we need a subgroup of G which is normal in G . It is well known that every subgroup can be viewed as a factor group of a bigger group (in fact a *free* group). In order to define a factor group we need to define a normal subgroup. For instance, if we form a collection of all left cosets of H (subgroup of G) in G and want to show that it is group, first we need to define an operation $aHbH = abH$. But this operation is well defined if and only if and only if $bH = Hb$. Thus, we define the following notion. If G is a group and $H \leq G$ such that $aH = Ha$ for all $a \in G$ then H is called a normal subgroup of G . We

express this fact symbolically as: $H \trianglelefteq G$. Note that improper subgroups are always normal in the group. That is, $\{1\} \trianglelefteq G$ and $G \trianglelefteq G$. A group which has no proper normal subgroups is called a simple group. For example, all cyclic groups of prime order are simple groups.

Let us explain the concept of normality by considering the following examples.

Example 2.4.1

The subgroup $nZ = \{0, \pm n, \pm 2n, \pm 3n, \dots\}$ is a normal subgroup of Z for all $n \in Z^+$. (One can refer to theorem 2.4.6 for a second proof).

Example 2.4.2

We have discussed in chapter 1, the direct product of groups. In the end of the chapter, we constructed a subgroup $G_i = \{(1, 1, \dots, 1, g_i, 1, 1, \dots, 1) : g_i \in G\}$ of $G = G_1 \times G_2 \times \dots \times G_n$. It is not hard to show that $G_i \trianglelefteq G$.

Example 2.4.3

The group $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$ has $C_3 = \{1, y, y^2\}$ as its only proper normal subgroup.

Example 2.4.4

Let $GL(2, R)$ denote the group, under multiplication, of all non-singular 2×2 matrices with entries from the real line R . If $SL(2, R)$ is a subset of $GL(2, R)$ containing those matrices which have determinant equal to 1 then $SL(2, R) \trianglelefteq GL(2, R)$. This is so because $\det(A^{-1}BA) = \det(A)^{-1} \det(B) \det(A) = \det(B) = 1$ as $B \in SL(2, R)$ and $A \in GL(2, R)$.

The following is another version of the concept of the normality.

Theorem 2.4.5

A subgroup H of a group G is normal in G if and only if $gHg^{-1} = H$ for all $g \in G$.

Proof

If $H \trianglelefteq G$, then for any $g \in G$

$$g^{-1}Hg = \{g^{-1}hg : h \in H\} \subseteq H. \quad (i)$$

Also, $gHg^{-1} = (g^{-1})^{-1}Hg^{-1} \subseteq H$, from which it is easy to see that

$$H \subseteq g^{-1}Hg, \quad (ii)$$

From (i) and (ii), we obtain $gHg^{-1} = H$.

If conversely, $gHg^{-1} = H$ for every $g \in G$ then certainly $H \trianglelefteq G$.

Abelian groups and normal subgroups are strongly related as, for example, can be seen here.

Theorem 2.4.6

Every subgroup of an Abelian group is a normal subgroup.

Proof

Let G be an Abelian group and $H \leq G$. If $g \in G$ and $h \in H$, then $g^{-1}hg = h$ because G is Abelian and $gh = hg$. So, $g^{-1}hg \in H$ as $h \in H$. Also $g^{-1}hg \in g^{-1}Hg$ and $g^{-1}hg = h$. Thus $g^{-1}Hg = H$ and so by theorem 2.4.5, $H \trianglelefteq G$.

Finite Abelian groups are classified through the following result.

Theorem 2.4.7

The only Abelian simple groups are the groups of prime order.

Proof

If G is a group of prime order, then, by Lagrange's theorem, the only subgroups of G are $\{1\}$, G ; and so G is simple. On the other hand, if G is Abelian simple group

then the only normal subgroups of G are $\{1\}$ and G . Suppose H is a proper subgroup of G . Since G is Abelian, by theorem 2.4.6, H is a normal subgroup of G . But this contradicts the fact that G is simple and so it has no proper normal subgroups. This implies that G has no subgroups other than $\{1\}$ and G . This shows that the only positive divisors of $|G|$ are 1 and $|G|$. Thus G is of prime order.

Theorem 2.4.8

If G is a group and $H \trianglelefteq G$, $K \trianglelefteq G$, then $H \cap K \trianglelefteq G$.

Proof

The proof is trivial.

Theorem 2.4.9

If G is a group, $K \trianglelefteq G$ and $K \leq H \leq G$, then $K \trianglelefteq H$.

Proof

The assertion is immediate from the definition of normality.

Theorem 2.4.10

Let G be a group.

- (i) If $H \leq G$ and $K \trianglelefteq G$, then $HK \leq G$.
- (ii) If $H \trianglelefteq G$ and $K \trianglelefteq G$, then $HK \trianglelefteq G$.

Proof

(i) If $x, y \in HK$, then $x = h_1 k_1$ and $y = h_2 k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Now $xy^{-1} = (h_1 k_1)(h_2 k_2)^{-1} = (h_1 k_1)(k_2^{-1} h_2^{-1}) = h_1(h_2^{-1} h_2)(k_1 k_2^{-1})h_2^{-1} = (h_1 h_2^{-1})(h_2(k_1 k_2^{-1})h_2^{-1}) = hk$, where $h_1 h_2^{-1} = h$ and $h_2(k_1 k_2^{-1})h_2^{-1} = k$. As $H \leq G$ and $K \trianglelefteq G$, we have $h \in H$ and $k \in K$, and so $hk \in HK$. That is, $xy^{-1} \in HK$. Thus, by theorem 1.5.10, $HK \leq G$.

- (ii) By (i), $HK \leq G$, so we need only to show that HK is normal in G . Suppose $g \in G$ and $x \in HK$. Then $x = hk$ for some $h \in H$ and $k \in K$. Now

$g x g^{-1} = g(hk)g^{-1} = gh(g^{-1}g)kg^{-1} = (ghg^{-1})(gkg^{-1})$. Since $H \trianglelefteq G$ and $K \trianglelefteq G$, we have $ghg^{-1} \in H$ and $gkg^{-1} \in K$. This shows that $g x g^{-1} \in HK$. Thus $HK \trianglelefteq G$.

If G is a group, $K \trianglelefteq G$ and $K \leq H \leq G$ then we have seen, in theorem 2.4.9 that $K \trianglelefteq H$. It is important to note that H may not be normal in G . For example, if we consider $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$, $H = \{1, x\}$ and $K = \{1\}$, then it is clear that $K \trianglelefteq G$ and $K \trianglelefteq H$ but H is not normal in G .

Note that it can happen that $K \trianglelefteq H \trianglelefteq G$, with K not necessarily normal in G . For instance, if we consider S_3 and $C_2 = \langle x : x^2 = 1 \rangle$, then it is easy to verify that $C_2 \times C_2 \trianglelefteq S_3 \times S_3$; where the multiplication is defined as in section 6 of chapter 1. Now $C_2 \times C_2$ is Abelian and so, by theorem 2.4.6, $K = \langle (x, y) : (x, y)^2 = (1, 1) \rangle$, being a subgroup of $C_2 \times C_2$ is normal in $C_2 \times C_2$. Hence $K \trianglelefteq C_2 \times C_2 \trianglelefteq S_3 \times S_3$, where as K is not normal in $S_3 \times S_3$, where as K is not normal in $S_3 \times S_3$ because $(x, y)^{-1} (y, y) (x, y) = (x^{-1} y x, y^{-1} y y) = (y^2, y) \notin K$.

Next we show how a group G can be factorized with the help of its normal subgroup.

Theorem 2.4.11

If G is group and $H \trianglelefteq G$ then $G/H = \{gH : g \in G\}$ is a group under coset multiplication.

Proof

Let $g_1 H, g_2 H$ be arbitrary elements of G/H . If $x \in (g_1 H)(g_2 H)$, then $x = (g_1 h_1)(g_2 h_2)$ for some $h_1, h_2 \in H$. Now, $x = (g_1 h_1)(g_2 h_2) = g_1(h_1 g_2)h_2 = g_1(g_2 h_3)h_2$ because $h_1 g_2 = g_2 h_3$ due to the fact that $H \trianglelefteq G$. Thus $x = (g_1 g_2)(h_3 h_2) \in (g_1 g_2)H$ implying that $(g_1 H)(g_2 H) \subseteq (g_1 g_2)H$. Conversely, if $x \in (g_1 g_2)H$ then $x = (g_1 g_2)h$ and because $H \trianglelefteq G$, we have $x = (g_1 g_2)h = g_1(g_2 h) = g_1(h_1 g_2) = (g_1 h_1)g_2 = (g_1 h_1)(g_2 1) \in (g_1 H)(g_2 H)$. Thus, $(g_1 H)(g_2 H) \subseteq (g_1 g_2)H$. Thus $(g_1 H)(g_2 H) = (g_1 g_2)H$.

$H)(g_2 H) = (g_1 g_2) H$ implies that G/H is closed under the coset multiplication. Through routine calculations one can show that G/H is associative, $1 H = H$ is the identity element of G/H and $a^{-1} H$ is the inverse of aH . This proves our assertion that G/H is a group.

The group G/H is called a factor (or quotient) group. The elements of G/H , which we know are called left cosets, depend upon the type of H . Due to the fact that $H \trianglelefteq G$, we can take Ha instead of aH because $aH = Ha$ for all $a \in G$. Thus it makes no differences whether we consider G/H as a collection of left cosets or of right cosets. Furthermore, the size of G/H depends upon the size of H , in fact, it is inversely proportional to the size of H . In the next theorem we calculate the size of G/H .

Theorem 2.4.12

If G is a finite group and $H \trianglelefteq G$, then $|G/H| = \frac{|G|}{|H|}$.

Proof

By Lagrange's theorem $|G| = |H : G| |H|$. That is, $\frac{|G|}{|H|} = |H : G|$. But $|H : G|$, the index of H in G , is the number of left cosets of H in G ; and so $|G/H| = |H : G|$. Thus $|G/H| = \frac{|G|}{|H|}$.

We illustrate this theorem through the following example.

Example: 2.4.13

The group $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$ has only one proper normal subgroup and, that is, $C_3 = \langle y : y^3 = 1 \rangle$. Thus, we can factorize S_3 by C_3 to obtain

$S_3/C_3 = \{ C_3, xC_3 \}$. Hence $\left| \frac{S_3}{C_3} \right| = 2$. But we can also use theorem 2.4.12 to calculate the order of the factor group S_3/C_3 as $\left| \frac{S_3}{C_3} \right| = \frac{|S_3|}{|C_3|} = \frac{6}{3} = 2$.

We can, of course, factorise an infinite group as well.

Example 2.4.14

We know that Z is an infinite group under the operation of addition and nZ is normal in Z , (see example 2.4.1). Thus Z can be factorized by nZ to obtain the factor group Z/nZ .

The structural properties of a factor group G/H depends upon the structural properties of the normal subgroup H . The last section of this chapter is devoted to certain important normal subgroups and consequently some significant factor groups.

5. SOME IMPORTANT FACTOR GROUPS

In constructing a factor group G/H , where $H \trianglelefteq G$, we essentially put every element of G which is in H equal to the identity element, for H forms our new identity element in G/H . This indicates another use for factor groups. Suppose we wish to study the structure of a non-Abelian group G . Since we have theorems which give complete information about the structure of all sufficiently small Abelian groups, it might be of interest to try to form an Abelian group as much like G as possible, by starting with G and then requiring that $xy = yx$ for all x, y in our new group structure. To require that $xy = yx$ is to say that $xyx^{-1}y^{-1} = 1$ in our new group. An element $xyx^{-1}y^{-1}$ is called the commutator of the pair x, y of elements of G . Thus we wish to form a group G by replacing every commutator of G by 1. This means that we should then construct the factor group of G modulo the smallest normal subgroup we can find which contains all commutators of G .

If G is a group with finite presentation.

$\langle g_1, g_2, \dots, g_n : r_1(g_1, g_2, \dots, g_n) = 1, k = 1, 2, \dots, m \rangle$ then the effect of including new relations $g_i^{-1}g_j^{-1}g_i g_j = 1$ is to form the commutator factor group of G , which is the largest Abelian factor group of G .

We shall denote the commutator $x^{-1}y^{-1}xy$ of x, y in a group G by $[x, y]$. We remark that the concept of commutator arises from asking how two elements, x, y can be made to commute. We have the equation $xy = yx \cdot c$, where $c = [x, y]$, and clearly $[x, y] = 1$ if and only if x, y commute; so a group is Abelian if and only if every commutator in it equals 1.

Let us consider the following example:

Example 2.5.1

Every element in the group $\langle x, y : x^2 = y^3 = (xy)^3 = 1 \rangle$ is a commutator.

Example 2.5.2

Every element in the subgroup $C_3 = \langle y : y^3 = 1 \rangle$ of $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$ is a commutator.

Let $H \trianglelefteq G$; then notice that if either x or y lies in H , then $[x, y] \in H$. Suppose next that the group G has normal subgroups H and K with $H \cap K = \{1\}$. Then the concept of commutators allows us to see easily that any element h of H commutes with any element k of K , for $[h, k]$ lies in both H and K and is therefore 1.

Another interesting fact may be mentioned at this point. We state it in a form of a theorem (cf. exercise 8)

Theorem 2.5.3

If every element of a group G is of order 2, then G is Abelian.

Proof

If $x, y \in G$, then by hypothesis $x^2 = 1$, $y^2 = 1$ and $(xy)^2 = 1$. Now $xyx^{-1}y^{-1} = xyxy = (xy)^2 = 1$ implies that $xy = yx$. This proves that G is Abelian.

If G is a group then the derived group (or commutator subgroup) of G is the subgroup generated by all the commutators in G . It is usually denoted by G' . We emphasize that $G' \leq G$ and G' is not merely a subset of G . In examples 2.5.1, 2.5.2 and 2.2.8 the derived groups are $\langle x, y : x^2 = y^3 = (xy)^3 = 1 \rangle$, C_3 and $\{1, y^2\}$. The order of G' represents a measure of how many elements of G commute with each other. The smaller G' is, the larger the portion of G containing the commuting elements. Thus, a group G is non-Abelian if and only if $G' \neq \{1\}$, and we shall see that there do exist non-trivial groups with this property. For instance, the one considered in example 2.5.1 or $\langle x, y : x^2 = y^3 = (xy)^5 = 1 \rangle$.

The following theorem is in order.

Theorem 2.5.4

If G is a group, then $G' \trianglelefteq G$.

Proof

First, we show that if h is a commutator then so is ghg^{-1} where $g \in G'$. If $h \in G'$, then $h = x^{-1}y^{-1}xy$ for some x, y in G . Now if we let $g \in G$, then $ghg^{-1} = g(x^{-1}y^{-1}xy)g^{-1} = gx^{-1}(g^{-1}g)y^{-1}(g^{-1}g)x(g^{-1}g)yg^{-1} = (gx^{-1}g^{-1})(gy^{-1}g^{-1})(g x g^{-1})(g y g^{-1}) = x^{-1}y^{-1}x y = [x, y]$, where $x_1 = gxg^{-1}$ and $y_1 = gyg^{-1}$. Now h , being an element of G' , is a product of commutators and their inverses; and as an inverse of a commutator is a commutator h is a product of commutators c_1, c_2, \dots, c_k , and so $ghg^{-1} = g(c_1 c_2 \dots c_k)g^{-1} = (gc_1 g^{-1})(gc_2 g^{-1}) \dots (gc_k g^{-1}) = d_1 d_2 \dots d_k$ where d_i is $gc_i g^{-1}$ for $i = 1, 2, \dots, k$. But, we have just shown that each d_i is a commutator. Hence, if $h \in G'$ then $ghg^{-1} \in G'$ and so $G' \trianglelefteq G$.

Theorem 2.5.5

A group G is Abelian if $G' = \{1\}$.

Proof

The proof is trivially true.

Theorem 2.5.6

If G is a group and $H \trianglelefteq G$, then G/H is Abelian if and only if $G' \subseteq H$.

Proof

Suppose that G/H is Abelian. Thus, for all $x, y \in G$, $xH yH = yH xH$ implies that $xyH = yxH$. Since $H \trianglelefteq G$, we have $x^{-1}y^{-1}xyH = H$; and so $x^{-1}y^{-1}xy \in H$. This shows that $G' \subseteq H$ because H contains $x^{-1}y^{-1}xy$ if and only if H contains all commutators. By revising the steps, one can very easily show that if $G' \subseteq H$ then G/H is Abelian.

Corollary 2.5.7

If G is a group, then G/G' is Abelian.

Proof

By theorem 2.5.4, $G' \trianglelefteq G$. Now, direct application of theorem 2.5.6 completes the proof.

There is another measure for checking whether a group is Abelian or not. Before we deal with it, we need to define another interesting notion.

The centre of a group G contains those elements of G which commute with every element of G . The centre of a group G is usually denoted by $Z(G)$. For instance, if we refer to example 2.2.8, we see that $Z(D_3) = \{1, y^2\}$. Let us determine the centre of the following group.

Example 2.5.8

If $G = \left\{ \begin{bmatrix} a & c \\ b & d \end{bmatrix} \neq 0 \text{ and } a, b, c, d \in \mathbb{Z}_5 \right\}$ is the group under consideration, then

the centre, $Z(G)$, of G contains all the scalar matrices in G .

A group G is obviously Abelian if and only if $Z(G) = G$.

Theorem 2.5.9

If G is a group and $H \leq G$ such that $H \subseteq Z(G)$, then H is a normal, Abelian subgroup of G .

Proof

Since each element of G commutes with each element of $Z(G)$, therefore each element of $Z(G)$ commutes with each element of H . Thus $H \trianglelefteq G$. Now H , being a subset of $Z(G)$, is obviously Abelian.

Theorem 2.5.10

If G is a group, then $Z(G) \trianglelefteq G$.

Proof

First we show that $Z(G) \neq \phi$. Since $1x = x1 = x$ for all $x \in G$, therefore $1 \in Z(G)$. Next we show that $Z(G) \leq G$. Let $x, y \in Z(G)$. This means that $z(xy^{-1}) = (xz)y^{-1} = x(zy^{-1}) = x(y^{-1}z) = (xy^{-1}z)$. As $zy = yz$, $y^{-1}z = zy^{-1}$. It follows that $Z(G) \leq G$ because xy^{-1} commutes with every $z \in G$.

Since $Z(G) \leq G$ and $Z(G) \subseteq Z(G)$, it follows from theorem 2.5.9, that $Z(G) \trianglelefteq G$. Recall that the group G is Abelian if and only if $G = Z(G)$. The size of $G/Z(G)$, therefore, gives us another measure of the fact whether G is non-Abelian. The antithesis of an Abelian group would be a group G for which $Z(G) = \{1\}$, that is, the group with trivial centre. For instance, the group S_3 is non-Abelian. On the other hand, since V_4 is Abelian $Z(V_4) = V_4$.

Next is a beautiful result which links the three notions, namely, Abelian group, Cyclic group and the centre.

Theorem 2.5.11

A group G is Abelian if and only if $G/Z(G)$ is cyclic.

Proof

Suppose that G is Abelian. Then $G = Z(G)$ and so $G/Z(G) = \{G\}$ implies that $G/Z(G)$ is cyclic.

Conversely, suppose that $G/Z(G)$ is cyclic. Then $G/Z(G) = \langle x Z(G) \rangle$ for some $x \in G$. The general element of $G/Z(G)$ will be of the form $x^n Z(G)$ for some positive integer n . Thus if $y_1, y_2 \in G$ then $y_1 = x^n z_1$ and $y_2 = x^m z_2$ for some $z_1, z_2 \in Z(G)$ where n, m are positive integers. Hence

$$\begin{aligned} (x^n z_1)(x^m z_2) &= x^n (z_1 x^m) z_2 = x^n (x^m z_1) z_2 = (x^n x^m) (z_1 z_2) \\ &= x^{n+m} (z_2 z_1) = x^{n+m} (x^n z_2) z_1 = x^m (z_2 x^n) z_1 = (x^m z_2) (x^n z_1) \end{aligned}$$

thus, G is Abelian.

6. Exercises

1. Find the left cosets of a subgroup of V_4 , and show that they form a partition of V_4 by the subgroup.
2. Show that the powers of any element of a finite group form a subgroup.
3. Prove that all subgroups of quaternion group Q_8 are normal in Q_8 .
4. If a cyclic group H is normal in a group G , then prove that every subgroup of H is normal in G .
5. Prove that Z_5 is a cyclic group.
6. Find all the subgroups of C_{18} .
7. If H is a subgroup of an Abelian group G , then show that every left coset of H in G is also a right coset of H in G .
8. If G is a group and $H \leq G$ such that the product of any two left cosets of H in G is again a left coset of H in G , then prove that $H \trianglelefteq G$.
9. Let G be a group and $N \leq G$, $K \leq G$ such that $N \trianglelefteq K$. Then prove that $K/N \trianglelefteq G/N$.
10. Prove that $\{1, y, y^2, \dots, y^{n-1}\}$ is a normal subgroup of $D_{2n} = \langle x, y : x^2 = y^n (xy)^2 = 1 \rangle$.
11. Let $G = \langle x, y : x^2 = y^2 = (xy)^3 = 1 \rangle$. Find a normal subgroup H of G of order 4.
12. Determine G/H where G and H are defined as in exercise 11.
13. Determine all the normal subgroups of D_8 .
14. Show that $SL(2, \mathbb{R}) \trianglelefteq GL(2, \mathbb{R})$.
15. Suppose G is a finite group and p is the smallest prime divisor of $|G|$. If $H \leq G$ such that $|H : G| = p$, then prove that $H \trianglelefteq G$.
16. If H is a normal subgroup of G and $x \in G$ is of order m then prove that the order of xH is a factor of m .
17. If H is a normal subgroup of a group G , Then prove that $Z(H) \trianglelefteq G$.
18. Determine $Z(Q_8)$.
19. Determine $Z(G)$ and G' , where $G = \{[a_{ij}] : a_{ij} \in \mathbb{Z}_3, \det([a_{ij}]) \neq 0 \text{ and } i, j = 1, 2\}$.

20. Let x be a non-empty subset of the group G , and define the relation $x R y$ between the elements x, y to mean that $xy^{-1} \in X$. Prove that $X \leq G$ if R is an equivalence relation.

21. Let G be a group and $H \leq G$. for $x, y \in G$, $X \equiv y \pmod{H}$ if and only if $xy^{-1} \in H$.
Prove that ' \equiv ' is an equivalence relation.

22. If G is a group and $H \leq G$, then prove that $Ha = \{x \in G: a \equiv x \pmod{H}\}$.

23. Let $G = \{x_0, x_1, \dots, x_6\}$ and define the binary operation $(.)$ in G as:

$$x_i \cdot x_j = \begin{cases} x_{i+j} & \text{if } i+j < 7 \\ x_{i+j-7} & \text{if } i+j \geq 7. \end{cases}$$

Then prove that G is a cyclic group.