

CHAPTER FOUR

PERMUTATION REPRESENTATIONS

1. INTRODUCTION

In group theory, the objects of study are the equivalence classes of isomorphic groups and the relations between these classes. Such a class is called an abstract group. It embodies the structure common to many groups because the isomorphism relation preserves structure in a certain sense. The groups in a class may, of course, be quite different in the nature of their elements. In 1854, a Cayley proved that permutations can be considered as a elements of an abstract group, that is, every group is isomorphic to a group of permutations. This chapter is devoted to the study of permutations and permutations groups.

2. PERMUTATION GROUPS

If X is a set, then a one-to-one mapping from X onto X is called a permutation on X . If we let $\text{Sym}(X) = \{f: f \text{ is a permutation on } X\}$, then it is not hard to prove the $\text{Sym}(X)$ is a group under the composition (see example 1.2.4) of mappings. The identity element in $\text{Sym}(X)$ is the identity mapping $i: X \rightarrow X$, defined by $(X) \ I = x$, for all $x \in X$. Since $\in \text{Sym}(X)$ is a one-to-one and onto mapping, the inverse f^{-1} of f , exists in $\text{Sym}(X)$. The composition of mappings is always associative. The group $\text{Sym}(X)$ is called a symmetric group. It is important to note that if there is a one-to-one mapping from a set X onto a set X' , then the groups $\text{Sym}(X)$ and $\text{Sym}(X')$ are isomorphic. In fact, if $h: X \rightarrow X'$ is a bijection then the mapping $\phi: \text{Sym}(X) \rightarrow \text{Sym}(X')$ defined by $(f)\phi = h^{-1} f h$ for all $f \in \text{Sym}(X)$, is an isomorphism. As an abstract group therefore $\text{Sym}(X)$ is determined by the cardinality of X . In particular if X is finite, and has n

elements, then we write S_n for $\text{Sym}(X)$ and call it a symmetric group of degree n . Of course S_n is also finite, but before we calculate the order of S_n , we consider some special notations and properties of permutations defined on finite set X . If X is finite, there is not loss or generality in taking the objects of X to be $1, 2, \dots, n$. Let f be a permutation on X . It is customary to represent f by

$$\begin{pmatrix} 1 & 2 & \dots & n \\ (1)f & (2)f & \dots & (n)f \end{pmatrix} \text{ where, of course, } (1)f, (2)f, \dots, (n)f \text{ are } 1, 2, 3, \dots,$$

n in some order. Note that the image $(i)f, (2)f, \dots, (n)f$ are $1, 2, 3, \dots, n$ in some order. Note that the image $(i)f$, of i under f , is positioned immediately below i . In fact the order of the numbers in the top row does not matter as long as the right

image $(i)f$, is below i . Thus, we could write $\begin{pmatrix} 3 & 1 & 2 & \dots & n \\ (3)f & (1)f & (2)f & \dots & (n)f \end{pmatrix}$ for

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ (1)f & (2)f & (3)f & \dots & (n)f \end{pmatrix}$$

For instance, if $X = \{1, 2, 3\}$ and $f: X \rightarrow X$ is defined as $(1)f = 3, (2)f = 2,$

$(3)f = 1$, then the permutation f can be written as $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. This could also be

written as $\begin{pmatrix} 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. The product of two permutations

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ (1)f & (2)f & (3)f & \dots & (n)f \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ (1)g & (2)g & (3)g & \dots & (n)g \end{pmatrix}$$

is defined

$$\begin{aligned} & \text{as } \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ (1)f & (2)f & (3)f & \dots & (n)f \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ (1)g & (2)g & (3)g & \dots & (n)g \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ (1)fg & (2)fg & (3)fg & \dots & (n)fg \end{pmatrix}. \end{aligned}$$

For instance, the product of two permutations, namely $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \text{ is } \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}. \text{ Note that } \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \text{ and}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \text{implies} \quad \text{that}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}. \quad \text{Thus, in general, permutations}$$

are non-commutative. The inverse of $\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ (1)f & (2)f & (3)f & \dots & (n)f \end{pmatrix}$ will be

$$\begin{pmatrix} (1)f & (2)f & (3)f & \dots & (n)f \\ 1 & 2 & 3 & \dots & n \end{pmatrix}.$$

Thus, the inverse of $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ will be $\begin{pmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \end{pmatrix}$ which is, in fact, the permutation

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}. \quad \text{It is cumbersome to multiply permutation and besides it gives no insight}$$

into the structure of the permutation. To overcome these defects one uses the cyclic

notation. A cycle is a permutation f of the type $\begin{pmatrix} 1 & (1)f & (1)f^2 & \dots & (1)f^{n-1} \\ (1)f & (1)f^2 & (1)f^3 & \dots & 1 \end{pmatrix}$, where f

is defined on a set of n objects and f^i is the composition of i number of f . For instance,

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \text{are cycles. A Cycle is usually written as } (1 \ (1)f \ (1)f^2) \dots$$

$(1)f^r)$, where $r \leq n$. The number r is called the length of the cycle. In the example above,

we write $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ as $(1 \ 2 \ 3)$. It is a cycle of length 3, whereas the cycle

$$\begin{pmatrix} 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \text{which can be written as } (1 \ 3), \quad \text{is of length 2. Note that the cycles of length 1}$$

mean that the symbols involved are left fixed. Thus (X) denotes that the symbol X is

fixed in the permutation. Such cycles are often omitted when describing the permutation.

A cycle of length 2 is called a transposition. For example, the cycle $(1 \ 3)$ is a transposition.

The following two results describe the structure of permutations.

Theorem 4.2.1

Every permutation is the product of its cycles.

Proof:

If f is a permutation, then its cycles are of the form $(X \ Xf \ Xf^2 \ Xf^3 \ \dots \ Xf^{r-1})$. By the multiplication of cycle, as in the case of bijections, and since the cycle of f are disjoint, the image of $x' \in X$ under f , which is $x'f$, is the same as the image of x' under the product, g , of all the distinct cycle of f . So f, g have the same effect on every element of X , hence $f = g$, which completes the proof of the theorem.

Consider the r -cycle $(1 \ 2 \dots r)$. A simple computation shows that $(1 \ 2 \dots R) = (1 \ 2) (1 \ 3) \dots (1 \ r)$. More generally, $(X_1 \ X_2 \dots X_r) = (X_1 \ X_2) (X_1 \ X_3) \dots (X_1 \ X_r)$. This leads us to the following theorem.

Theorem 4.2.2

Every cycle is a product of transpositions.

Proof

We use induction on the length of a cycle to prove this theorem.

Note that

$$\begin{aligned} (x^1 \ x^2) (x^1 \ x^3) &= \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_2 & x_1 \end{pmatrix} \\ &= \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix} (x^1 \ x^2 \ x^3) \end{aligned}$$

$$\begin{aligned} &\text{Similarly } (x_1 \ x_2) (x_1 \ x_3) (x_1 \ x_4) \\ &= \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_1 & x_3 & x_4 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_1 & x_2 & x_3 & x_4 \\ x_3 & x_2 & x_1 & x_4 & x_4 & x_2 & x_3 & x_1 \end{pmatrix} \\ &= \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_1 & x_4 \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_4 & x_2 & x_3 & x_1 \end{pmatrix} \\ &= \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ x_2 & x_3 & x_4 & x_1 \end{pmatrix} = (x_1 \ x_2 \ x_3 \ x_4) \end{aligned}$$

In general, if $(x_1 \ x_2) (x_1 \ x_3) \dots (x_1 \ x_k) = (x_1 \ x_2 \ x_3 \ x_4 \dots x_k)$, then

$$(x_1 \ x_2) (x_1 \ x_3) \dots (x_1 \ x_k) (x_1 \ x_{k+1}) = (x_1 \ x_2 \dots x_k) (x_1 \ x_{k+1})$$

$$\begin{aligned}
&= \begin{pmatrix} x_1 & x_2 & \dots & x_k & x_{k+1} \\ x_2 & x_3 & \dots & x_1 & x_{k+1} \end{pmatrix} \begin{pmatrix} x_1 & x_2 & \dots & x_k & x_{k+1} \\ x_{k+1} & x_2 & \dots & x_k & x_1 \end{pmatrix} \\
&= \begin{pmatrix} x_1 & x_2 & \dots & x_k & x_{k+1} \\ x_2 & x_3 & \dots & x_{k+1} & x_1 \end{pmatrix} = (x_1 \ x_2 \dots x_k \ x_{k+1}) \text{ Hence by induction}
\end{aligned}$$

$(x_1 \ x_2 \dots x_n) = (x_1 \ x_2)(x_1 \ x_3) \dots (x_1 \ x_n)$ for all values of n. Furthermore,

$(x_i \ x_j)(x_j \ x_i) = (x_j \ x_i)(x_i \ x_j) = (x_i \ x_j)(x_j \ x_i) = 1$. This concludes the proof.

Corollary 4.2.3

Every permutation is a product of transpositions.

Proof

The proof follows directly from theorems 4.2.1 and 4.2.2.

It is important to note that the expression of a permutation as a product of transpositions is not unique.

The notion of a permutation group, that is, a group of permutation, is useful because it provides a method of representing group elements from which the whole structure of the group can in principle be recovered. This makes it important to know what groups occur as permutation groups. In fact all groups do; this is the content of the following theorem, best known as Cayley's theorem.

Theorem 4.2.4

Every group is isomorphic to a group of permutations on a suitable set.

Proof

Let G be a group. In order to construct $\text{Sym}(X)$, we choose $X = G$ and define the elements of $\text{Sym}(G)$ as follows.

Let a be a fixed element of G , and define the mapping ρ_a of G into G by setting

$(x)\rho_a = xa$, for every $x \in G$. First, we show that ρ_a is a permutation. The mapping $\rho_a : G \rightarrow G$ is one-to-one because if $x, y \in G$ such that $(x)\rho_a = (y)\rho_a$ then $xa = ya$ implies that

$x = y$. The mapping ρ_a is onto because for every $y \in G$ there exists $ya^{-1} \in G$ such that

$(ya^{-1})\rho_a = (ya^{-1})a = y(a^{-1}a) = y$. Thus, ρ_a is a permutation.

Next, we show that $\text{Sym}(G)$ is a group under the usual multiplication of mappings. If $\rho_a, \rho_b \in \text{Sym}(G)$, then $(X)\rho_a \rho_b = (xa)_{\rho_b} = (xa)b = x(ab) = (x)_{\rho_{ab}}$ for every $X \in G$, implies that $\text{Sym}(G)$ is closed under the operation of multiplication of mappings. The permutation ρ_1 is the identity element in $\text{Sym}(G)$ and the inverse of ρ_a is the permutation $\rho_{a^{-1}}$. Moreover, $(\rho_a \rho_b) \rho_c = \rho_{ab} \rho_c = \rho_{(a b) c} = \rho_{a (bc)} = \rho_a \rho_{bc} = \rho_a (\rho_b \rho_c)$, for every $a, b, c \in G$. This proves that $\text{Sym}(G)$ is a group.

Finally, we show that G is isomorphic to $\text{Sym}(G)$. Let us define a mapping $\phi: G \rightarrow \text{Sym}(G)$ by $(a) \phi = \rho_a$, for every $a \in G$. then, ϕ is well-defined because $a = b$ implies that $xa = xb$ for $x \in G$ and so $(x) \rho_a = (x) \rho_b$. This shows that $\rho_a = \rho_b$ because X was an arbitrary element of G . Hence $(a) \phi = (b) \phi$.

Also, $(ab) \phi = \rho_{ab} = \rho_a \rho_b = (a) \phi (b) \phi$, for every $a, b \in G$, implies that ϕ is a homomorphism. Obviously, ϕ is a Monomorphism because $(a) \phi = (b) \phi$ implies that $\rho_a = \rho_b$, and so $xa = xb$ or $a = b$.

Of course, ϕ is an epimorphism because for every $\rho_a \in \text{Sym}(G)$ there exists $a \in G$ such that $(a) \phi = \rho_a$. Thus, $G \cong \text{Sym}(G)$. This completes the proof.

While proving Cayley's theorem, we consider G to be an infinite group. If we take G to be a finite group, then by Cayley's theorem G will be isomorphic to a subgroup of S_n for some suitable n . If this is the case, G is embedded in S_n . Since every group can be considered as a subgroup of S_n , there are only finitely many isomorphic groups.

We illustrate Cayley's theorem through the following examples.

Example 4.2.5

The Cayley table for the Klein group $V_4 = \langle x, y: x^2 = y^2 = (xy)^2 = 1 \rangle$ is, of course, as below:

		1	x	y	xy
1		1	x	y	xy
x		x	1	x	y
y		y	xy	1	x
xy		xy	y	x	1

Then $\rho_1 = \begin{pmatrix} 1 & x & y & xy \\ 1 & x & y & xy \end{pmatrix}$, $\rho_x = \begin{pmatrix} 1 & x & y & xy \\ x & 1 & xy & y \end{pmatrix}$,

$$\rho_y = \begin{pmatrix} 1 & x & y & xy \\ y & xy & 1 & x \end{pmatrix}, \quad \text{and} \quad \rho_{xy} = \begin{pmatrix} 1 & x & y & xy \\ xy & y & x & 1 \end{pmatrix},$$

form the group $\text{Sym}(V_4) = \{\rho_1, \rho_x, \rho_y, \rho_{xy}\}$. If we define $\phi: V_4 \rightarrow \text{Sym}(V_4)$ by $(a)\phi = \rho_a$, for every $a \in V_4$ can also be visualized as a group of permutations (1), (12), (3 4) and (1 2) (3 4).

Example 4.2.6

The groups $\langle x, y: x^2 = y^3 = (xy)^2 = 1 \rangle$ and $\langle x, y: x^2 = y^3 = (xy)^3 = 1 \rangle$, described in examples 1.2.1 and 2. 5. 1, are respectively the permutation groups S_3 and A_4 . The determination of all subgroups of S_n depends upon the order of S_n . In the following theorem we calculate the order of S_n .

Theorem 4.2.7

For any positive integer n , $|S_n| = n!$

Proof

If $f \in S_n$, then (1) is one of the n elements of the set on which the permutation f is defined. Since f is one-to-one, $(1)f \neq (2)f$ and so $(2)f$ is one of the $n-1$ elements as $(1)f$ has already been chosen. Similarly, $(3)f$ is one of the $n-2$ elements because $(1)f \neq (3)f$, $(2)f \neq (3)f$ and f is one-to-one and $(1)f$, $(2)f$ have already been chosen. Continuing in this way, we conclude that there are $n(n-1)(n-2)\dots 3 \cdot 2 \cdot 1 = n!$ elements of S_n . That is, $|S_n| = n!$.

Thus, for instance, the symmetric groups S_1, S_2, S_3 and S_4 have orders 1, 2, 6 and 24.

Recall that, by results 4.2.1, 4.2.2 and 4.2.3, every permutation on a finite set can be expressed as a product of number of transpositions. If the number of transpositions is even then the permutation is called an even permutation, whereas if the number of transpositions is odd then the permutation is called an odd permutation.

Note that:

- (i) the product of two even permutations is an even permutation;
- (ii) the product of two odd permutations is an even permutation; and
- (iii) the product of an even permutation and an odd is an odd permutation.
- (iv) the parity of a permutation, whether it is even or odd, is well-defined.

The parity of a permutation, whether it is even or odd, is well defined.

Let A_n be the subset of S_n consisting of all the even permutations in S_n . The next result establishes a relationship between A_n and S_n .

Theorem 4.2.8

For any positive integer n , $A_n \trianglelefteq S_n$ and $|A_n| = \frac{n!}{2}$.

Proof

Let $\phi: S_n \rightarrow \{1, -1\}$ be defined by:

$$(\phi(f)) = \begin{cases} 1, & \text{if } f \text{ is even permutation.} \\ -1, & \text{if } f \text{ is odd permutation.} \end{cases}$$

Then, it is not hard to show that ϕ is an epimorphism. Since $\text{Ker } \phi = A_n$, therefore, by theorem 3.2.8, $A_n \trianglelefteq S_n$. Now, by theorems 3.2.9(i), 2.2.6 and 4.2.7, $S_n/A_n \cong \{1, -1\}$

and so $2 = |\{1, -1\}| = |S_n/A_n| = \frac{|S_n|}{|A_n|} = \frac{n!}{|A_n|}$. Thus, $|A_n| = \frac{n!}{2}$.

The group A_n is called an alternating group. For instance, the subgroup $\{1, y, y^2\}$ of $S_3 = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$ is an alternating group A_3 and $|A_3| = \frac{|S_3|}{2} = \frac{6}{2} = 3$, of course. The group $\langle x, y : x^2 = y^3 = (xy)^3 = 1 \rangle$ is A^4 , and of course is of order 12.

From theorem 4.2.8, we observe that the number of odd permutations in S_n is equal to the number of even permutations in S_n . While on the topic of the symmetric group of degree n , we prove a simple result which has extensive application.

Theorem 4.2.9

For any positive integer n , S_n is generated by the cycles $(1\ 2\ \dots\ n)$ and $(1\ 2)$.

Proof

If $x = (1\ 2\ \dots\ n)$ and $y = (1\ 2)$ generate a group G , then G contains $x^{-1}yx = (2\ 3)$, $x^{-1}(2\ 3)x = (3\ 4)$, ... and so contains all transpositions $(m\ m+1)$. Also, G contains $(1\ 2)(2\ 3)(1\ 2) = (1\ 3)$, $(1\ 3)(3\ 4)(1\ 3) = (1\ 4)$, ... and hence contains all transpositions $(1\ m)$. But, by corollary 4.2.3, every element of S_n is a product of transpositions. Thus, $G = S_n$.

Let us illustrate theorem 4.2.9 by considering the group S_5 .

Example 4.2.10

The group S_5 is generated by the cycles $(1\ 2\ 3\ 4\ 5)$ and $(1\ 2)$. If we let $x = (1\ 2)$ and $y = (1\ 2\ 3\ 4\ 5)$, then $x^2 = 1$, $y^5 = 1$, $(xy)^4 = 1$ and $(xy^{-1}xy)^2 = 1$ implies that $S_5 = \langle x, y : x^2 = y^5 = (xy)^4 (xy^{-1}xy)^2 = 1 \rangle$.

Finite alternating and symmetric groups have a special place in the theory of groups. Study of these groups have indeed yielded interesting and significant results, especially in the efforts to classify all finite simple groups. The following study, will give same insight into the study of their structural behavior.

Theorem 4.2.11

If $n \geq 3$, then $Z(S_n) = \{1\}$.

Proof

Let us suppose that $Z(S_n)$ contains a non-identity element x . By theorem 4.2.1, x can be expressed as a product of disjoint non-identity cycles, such as, $s = s_1 x_2 \dots x_k$ where $x_1 = (a_1\ a_2 \dots a_m)$, say. If $m = 2$, let $y = (a_1\ a_2)$. Then $x^{-1}yx \neq y$ implies that $x \notin Z(S_n)$. If $m = 3$, let $y = (a_1\ a_2\ a_3)$. Then $x^{-1}yx = (a_1\ x\ a_2\ x\ a_3\ x) = (a_2\ a_1\ b)$ where $b = a_3x$ and $b \neq a_1$ or a_2 . Thus $x^{-1}yx \neq y$ because $a_2y = a_3$ and $a_2x^{-1}yx = a_1$. This proves that our supposition was false and so $Z(S_n)$ contains no non-identity element. That is, $Z(S_n) = \{1\}$ for $n \geq 3$.

We may mention that $Z(S_1) = \{1\}$ and $Z(S_2) = S_2$.

Next we show that A_n has no proper normal subgroup for $n \geq 5$. We will require that following sequence of lemmas for this. But before we proceed further, we may recall that by an r -cycle we mean a cycle of length r .

Theorem 4.2.12

A_n is generated by 3-cycles.

Proof

The equations $(a_1\ a_2)(a_3\ a_4) = (a_1\ a_2\ a_3)(a_3\ a_1\ a_4)$ and $(a_1\ a_2)(a_1\ a_3) = (a_1\ a_2\ a_3)(a_4\ a_5\ a_1)^{-1}(a_5\ a_2\ a_3)(a_4\ a_5\ a_1)$, $(a_5\ a_2\ a_3) = (a_4\ a_5\ a_2)^{-1}(a_4\ a_5\ a_3)(a_4\ a_5\ a_2)$ and $(a_4\ a_2\ a_3) = (a_4\ a_5\ a_3)(a_5\ a_2\ a_3)(a_4\ a_5\ a_2) = (a_4\ a_5\ a_3)(a_4\ a_5\ a_2)(a_4\ a_5\ a_3)^{-1}$ imply that any 3-cycle can be expressed in terms of the cycles $(a_4\ a_5\ a_1)$.

Lemma 4.2.13

If $\{1\} \neq H$ is a normal subgroup of A_n , $n \geq 5$, and the 3 cycles $(a_1 a_2 a_3) \in H$, then $H = A_n$.

Proof

Let $(a'_1 a'_2 a'_3)$ be another 3 cycle and put $x = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & \dots \\ a'_1 & a'_2 & a'_3 & a'_4 & a'_5 & \dots \end{pmatrix}$

since $n \geq 5$, we have at least five symbols available. If x is an odd permutation, it can be made even by interchanging a'_4 and a'_5 in the bottom row. Then $x^{-1}(a_1 a_2 a_3)x = (a_1 a_2 a_3)$ and so $(a_1 a_2 a_3) \in H$ since $H \trianglelefteq A_n$. Thus H contains all 3-cycles and so by lemma 4.2.12, $A_n \subseteq H$. Consequently, $H = A_n$.

Lemma 4.2.14

If $\{1\} \neq H$, $H \trianglelefteq A_n$ and H contains the product of two disjoint transpositions, then $H = A_n$ for $n \geq 5$.

Proof

Suppose $x = (a_2 a_3)(a_4 a_5) \in H$. Since $n \geq 5$, there exists a_i such that $i = 5, 6, \dots, n$. If $y = (a_1 a_2 a_i)$, then $y \in A_n$ and $y^{-1}xy = (a_2 a_i)(a_4 a_5)$. Also, $x^{-1}y^{-1}xy = (a_1 a_2)(a_3 a_4)(a_2 a_i)(a_4 a_5) = (a_1 a_2)(a_2 a_i) = (a_1 a_i a_2)$. Thus, H contains a 3-cycle and consequently the result follows from lemma 4.2.13.

Theorem 4.2.15

A_n is simple for $n \geq 5$.

Proof

If $H \neq \{1\}$ and $H \trianglelefteq A_n$, then H contains an element $x \neq 1$. By theorem 4.2.1, x can be decomposed into disjoint cycles such as $x = x_1 x_2 \dots, x_k$ where $x_1 x_2 \dots, x_k$ are disjoint cycles. We may suppose without loss of generality that x_1, x_2, \dots, x_k are arranged so that the length of x_i is greater or equal to the length of x_{i+1} for $i = 1, 2, \dots, k-1$, as the cycles x_1, x_2, \dots, x_k commute.

Case (i)

Suppose $x_1 = (a_1 a_2 \dots a_m)$ with $m > 3$ and $y = (a_1 a_2 a_3)$. Indeed $y \in A_n$ and it commutes with x_2, x_3, \dots, x_k . As $y^{-1} \in A_n$ and $H \trianglelefteq A_n$ we have $z = x^{-1}y^{-1}xy \in H$. Then

$Y^{-1}xy = (a_2 \ a_3 \ a_1 \ a_4 \ \dots \ a_m) x_2 \dots x_k$ and $z = x_k^{-1} x_{k-1}^{-1} \dots x_1^{-1} (a_2 \ a_3 \ a_1 \ a_4 \ \dots \ a_m) x_2 \dots x_k = x_k^{-1} (a_2 \ a_3 \ a_1 \ a_4 \ \dots \ a_m) = (a_m \ a_{m-1} \ \dots \ a_1) (a_2 \ a_3 \ a_1 \ a_4 \ \dots \ a_m) = (a_1 \ a_2 \ a_4)$

Case (ii)

Suppose $m = 3$ and x_2 is a 3-cycle. If $x_1 = (a_1 \ a_2 \ a_3)$, $x_2 = (a_4 \ a_5 \ a_6)$ and $y = (a_2 \ a_3 \ a_4) \in A_n$, then H contains $x^{-1} y^{-1} xy = x_1^{-1} x_2^{-1} \dots x_k^{-1} (y^{-1} x_1 y) (y^{-1} x_2 y) x_3 \dots x_k = x_1^{-1} x_2^{-1} (y^{-1} x_1 y) (y^{-1} x_2 y) = x_1^{-1} x_2^{-1} (a_1 \ a_3 \ a_4) (a_2 \ a_5 \ a_6) = (a_3 \ a_2 \ a_1) (a_6 \ a_5 \ a_4) (a_1 \ a_3 \ a_4) (a_2 \ a_5 \ a_6) = (a_1 \ a_4 \ a_2 \ a_3 \ a_5)$, and hence the result follows from case (i).

Case (iii)

Suppose $m = 3$ and x_2, \dots, x_k are transpositions. If $x_1 = (a_1 \ a_2 \ a_3)$, then $x^2 (a_1 \ a_2 \ a_3) x_1 x_2 \dots x_k (a_1 \ a_2 \ a_3) x_1 x_2 \dots x_k = (a_1 \ a_2 \ a_3)^2 x_1^2 x_2^2 \dots x_k^2 = (a_1 \ a_2 \ a_3)^2 = (a_1 \ a_2 \ a_3)$ and the result follows from lemma 4.2.13.

Case (iv)

If all the x_i are transpositions, then m is even and $x_1 = (a_1 \ a_2)$, $x_2 = (a_3 \ a_4)$. If $y = (a_2 \ a_3 \ a_4)$ then H contains $y^{-1} xy = (a_1 \ a_3) (a_4 \ a_2) x_3 x_4 \dots x_k$. Thus $y^{-1} xyx^{-1} = (a_1 \ a_4) (a_2 \ a_3) \in H$, and the result follows from lemma 4.2.14. This concludes the proof.

This simplicity of A_n , for $n \geq 5$, has many uses. Before we use this property of A_n in studying A_n , and S_n , we should notice that $A_n, n \geq 3$ is non-Abelian because, for instance, $(1 \ 2 \ 3) (3 \ 4 \ 5) \neq (3 \ 4 \ 5) (1 \ 2 \ 3)$.

Let us determine the centre of A_n , for $n \geq 5$.

Theorem 4.2.16

If $n \geq 5$, then $z(A_n) = \{1\}$.

Proof

By theorem 2.5.10, $Z(A_n) \trianglelefteq A_n$ and since A_n , according to theorem 4.2.15, has no proper normal subgroup for $n \geq 5$, therefore either $Z(A_n) = \{1\}$ or $Z(A_n) = A_n$. since A_n is non-Abelian therefore $Z(A_n) \neq A_n$ and so $Z(A_n) = \{1\}$.

Theorem 4.2.17

If $n \geq 5$, then $A'_n = A_n$

Proof

By theorem 2.5.4, $A'_n \trianglelefteq A_n$. As A_n for $n \geq 5$, is simple, therefore either $A'_n = \{1\}$ or $A'_n = A_n$. Since A_n is non-Abelian therefore, by theorem 2.5.5, $A'_n \neq \{1\}$. Thus, $A'_n = A_n$

Notice that both A_1 and A_2 are trivial groups and so are simple. The group A_3 is of order 3 and so being cyclic it is simple. As $V_4 \trianglelefteq A_4$, the group A_4 is not simple. The next result determines the only normal subgroup of S_n , where $n \geq 5$.

Theorem 4.2.18

If $n \geq 5$, then the only proper normal subgroup of S_n is the group A_n .

Proof

If $H \trianglelefteq S_n$, then $H \cap A_n \trianglelefteq A_n$ and so either $A_n \cap H = A_n$, or $A_n \cap H = \{1\}$ as A_n (for $n \leq 5$) is simple due to theorem 4.2.15. If $A_n \cap H = A_n$, then $A_n \subseteq H$. If $H \neq A_n$, then by theorem 4.2.8, $H = S_n$ because A_n is of index 2 in S_n .

If $A_n \cap H = \{1\}$, then suppose that $H \neq \{1\}$. If $1 \neq h_1 \in H$, then h_1 is odd. As h_1^2 is even, $h_1^2 \in H \cap A_n$ and so $h_1^2 = 1$. Let $1 \neq h_2 \in H$. Then h_2 is odd and as $h_1 h_2$ is even, $h_2 = h_1^{-1} = h_1$. Hence H consists of only two elements, 1 and h_1 . As $Z(S_n) = \{1\}$ by theorem 4.2.11, there exists $h_3 \in S_n$ such that $h_3^{-1} h_1 h_3 \neq h_1$. But $h_3^{-1} h_1 h_3 \in H$ as $H \trianglelefteq S_n$; and since $H = \{1, h_1\}$, this is impossible. This contradicts the assumption that $H \neq \{1\}$. Thus A_n is the only proper normal subgroup of S_n .

Theorem 4.2.19

If $n \geq 5$, then $S'_n = A_n$.

Proof

Since S_n/A_n is group of prime order 2, it is cyclic and hence is Abelian. So by theorem 2.5.6 $S'_n \subseteq A_n$. As S_n is not Abelian, $S'_n \neq \{1\}$ by theorem 2.5.5. But by theorem 2.5.4, $S'_n \trianglelefteq S_n$. Hence $S'_n = A_n$ because of theorem 4.2.18. This completes the proof.

A transformation which preserves the structure of a space, that would mean that it carries any two congruent figures into two congruent ones, is called an automorphism. G. W. Leibniz recognized that this is the idea underlying the geometric concept of similarity. The next section is devoted to concept of automorphism and its prominent influence in the theory of groups.

3. AUTOMORPHISM

In the preceding sections we considered bijections from a set X onto itself and formed the group $\text{Sym}(X)$. In this section we intend to define a group structure on X and instead of bijections we consider isomorphism defined on X . In other words, we propose to study the symmetric group $\text{Sym}(G)$, where G is a group.

An isomorphism from a group G onto itself is called a automorphism. A set $\text{Aut}(G)$, containing all the automorphism defined on G , can easily be verified as a group. It is called a group of automorphisms of G . For instance, if G is an Abelian group then we can always define an automorphism $\phi: G \rightarrow G$, by $(x) \phi = x^{-1}$ for all $x \in G$.

As illustrations, let us determine the automorphism groups of A_3 and C_7 .

Example 4.3.1

Consider the alternating group $A_3 = \{1, (1\ 2\ 3), (3\ 1\ 2)\}$. There are only two automorphisms, which one can define on A_3 , namely $i: A_3 \rightarrow A_3$ and $f: A_3 \rightarrow A_3$, defined by $(x) i = x$ and $(x) f = x^2$ for all $x \in A_3$. Thus, the automorphism group of A_3 , namely $\text{Aut}(A_3)$, is $\{i, f\}$.

Example 4.3.2

Consider the group $C_7 = \langle x: x^7 = 1 \rangle$. It can be verified easily that the mapping $f: C_7 \rightarrow C_7$, defined by $(x^i)f = x^{2i}$ for all $x \in C_7$, is an automorphism and that f^3 is the identity automorphism. Thus, the Automorphism group, $\text{Aut}(C_7)$, is isomorphic to C_3 .

It is worth-noticing that if G is group and ϕ is an automorphism of G then the order of $x \in G$ is equal to the order of $(x)\phi$. Hence the following theorem.

Theorem 4.3.3

If G is a group and ϕ is an automorphism, then $\text{ord}(x) = \text{ord}((x)\phi)$ for all $x \in G$.

Proof

Suppose $x \in G$ and $\text{ord}(x) = n$. Then $((x)\phi)^n = ((x^n)\phi) = (1)\phi = 1$. On the other hand if $((x)\phi)^m = 1$ for some $0 < m < n$, then $(x^m)\phi = ((x)\phi)^m = 1$. As ϕ is one-to-one, therefore $x^m = 1$. This contradicts the assumption that $\text{ord}(x) = n$. Thus $\text{ord}((x)\phi) = \text{ord}(x)$.

If G is a group, then with each $a \in G$ there is associated an automorphism i_a of G , defined as follows.

For all $x \in G$, $(x) i_a = a^{-1} x a$. The element $(x) i_a = a^{-1} x a$ is called the conjugate of x by a . Certainly, i_a is a well-defined mapping of G into itself; and if $x_1, x_2, a \in G$, Then $(x_1, x_2) i_a = a^{-1} (x_1, x_2) a = a^{-1} x_1 (a a^{-1}) x_2 a = (a^{-1} x_1 a) (a^{-1} x_2 a) = (x_1) i_a (x_2) i_a$ implies that i_a is a homomorphism. If $(x_1) i_a = (x_2) i_a$, then $a^{-1} x_1 a = a^{-1} x_2 a$ shows that $x_1 = x_2$. Hence i_a is a monomorphism. Now i_a is onto because for every $y \in G$, there exists a ya^{-1} in G such that $(aya^{-1}) i_a = a^{-1} (aya^{-1}) a = (a^{-1} a) y (a^{-1} a) = 1y1 = y$. Thus showing that i_a is an automorphism of G . This automorphism is called the inner automorphism of G induced by a . (Sometimes it is known as the conjugation of G by a .)

An automorphism, which is not an inner automorphism is called an outer automorphism of G . For example, if we consider the automorphism defined in the beginning of this section, namely $\phi: G \rightarrow G$. (Here $(x)\phi = x^{-1}$, for all $x \in G$ and G is an Abelian group containing no element of order 1 or 2.)

Let $\text{In}(G)$ denote the set of all inner automorphisms of the group G . Then:

Theorem 4.3.4

If G is group, then $\text{In}(G) \leq \text{Aut}(G) \leq \text{Sym}(G)$.

Proof

Let us define $\phi : G \rightarrow \text{Sym}(G)$ by $(x) \phi = ix$, for all $x \in G$. Thus, if $x_1, x_2 \in G$, then $(x) i_{g_1} i_{g_2} = ((x) i_{g_1}) i_{g_2} = (g_1^{-1} x g_1) i_{g_2} = g_2^{-1} (g_1^{-1} x g_1) g_2 = (g_2^{-1} g_1^{-1}) x (g_1 g_2) = (g_1 g_2)^{-1} x (g_1 g_2) = (x) i_{g_1 g_2}$. That is, $(x) i_{g_1} i_{g_2} = (x) i_{g_1 g_2}$ for all $x \in G$. This shows that $i_{g_1} i_{g_2} = i_{g_1 g_2}$. Now ϕ is a homomorphism because for every $g_1, g_2 \in G$, $(g_1 g_2) \phi = i_{g_1 g_2} = i_{g_1} i_{g_2} = (g_1) \phi (g_2) \phi$. Moreover, $\text{Im } \phi = \{i_g : g \in G\} \leq \text{Aut}(G)$. But $\text{Im } \phi = \text{In}(G)$. Thus, $\text{In}(G) \leq \text{Aut}(G) \leq \text{Sym}(G)$.

The following theorem establishes a relationship between an Abelian group and the group of inner automorphisms.

Theorem 4.3.5

Let G be a group. Then $\text{In}(G) = \{1\}$ if and only if G is Abelian.

Proof

First, suppose that $\text{In}(G) = \{1\}$. This means that for every $g \in G$, there exists an inner automorphism i_g such that $i_g = 1$. Thus for every $x \in G$, $(x) i_g = (x) 1$ implies that $g^{-1} x g = x$. that is, $xg = gx$ for every $x, g \in G$. This proves that G is Abelian.

Conversely, suppose that G is Abelian. Thus $sg = gx$, for all $x, g \in G$.

Conversely, suppose that G is Abelian. Thus $xg = gx$, for all $x, g \in G$, implies that $g^{-1} x g = x$. This further implies that $(x) i_g = (x) 1$ for all $x \in G$. thus, $i_g = 1$ implies that $\text{In}(G) = \{1\}$.

An inner automorphism is called trivial if it leaves every element of the group fixed. The next result shows that non-Abelian groups may have non-trivial inner automorphisms.

Theorem 4.3.6

If G is a group, then $\text{In}(G)$ is isomorphic to $G/Z(G)$.

Proof

If $\phi : G \rightarrow \text{In}(G)$ is defined by $(g)\phi = i_g$, for every $g \in G$, then it is easy to check that ϕ is an epimorphism. (See theorem 4.3.4)

Next, we intend to show that $\text{Ker } \phi = Z(G)$. now if $g \in \text{Ker } \phi$, then $(g)\phi = 1$ where 1 is the identity in $\text{In}(G)$. But $\phi(g) = i_g - 1$ and so $(x)i_g = x$ implies that $xg = gx$ for every $x \in G$. Thus, $g \in Z(G)$. this shows that $\text{Ker } \phi \subseteq Z(G)$. Similarly, by reversing the argument, it is easy to show that $Z(G) \subseteq \text{Ker } \phi$. The two inclusions, thus, imply that $\text{Ker } \phi = Z(G)$. Now, the application of theorem 3.2.10(i) yields the result that $G/Z(G)$ is isomorphic to $\text{In}(G)$.

In the light of theorem 4.3.4, one can easily prove that $\text{In}(G) \trianglelefteq A(G)$ and so $A(G)/\text{In}(G)$ is group. This group is called the automorphism class group and the elements of it are the outer automorphism of G .

A characteristic subgroup of a group G is a subgroup that is mapped onto itself by every automorphism of G . This means that the subgroup as a whole is left fixed. In general, automorphism will permute the individual elements of the subgroup. It is an immediate consequence of the definitions that a characteristic subgroup is normal.

Thus,

Theorem 4.3.7

A subgroup H of a group G is a normal subgroup of G if and only if H is left invariant by every inner automorphism of G .

Proof

If $H \trianglelefteq G$, then $g^{-1}Hg = H$ for all $g \in G$ by theorem 2.4.5. So $g^{-1}hg = h'$, for all $h, h' \in H$ and $g \in G$, implies that $(h)_{i_g} = h'$. Thus $(H)_{i_g} = H$ for all $g \in G$.

The converse follows directly by reversing the argument.

Indeed, the normal subgroups of a group G are just those which are left fixed by the elements of $\text{In}(G)$.

There are certain subgroups of a group which are always invariant. The following theorem aims at singling out these groups.

Theorem 4.3.8

If G is a group, then G and $Z(G)$ are characteristic in G .

Proof

If α is an automorphism of G , then for all $x, y \in G$: $(x^{-1}y^{-1}xy)\alpha = (x^{-1})\alpha(y^{-1})\alpha(x)\alpha(y)\alpha = (x\alpha)^{-1}(y\alpha)^{-1}(x\alpha)(y\alpha)$ implies that $[x, y]\alpha = [x\alpha, y\alpha]$. This shows that α maps G' onto G' , that is, G' is characteristic.

Next, if $z \in Z(G)$, then $xz = zx$ for every $x \in G$ and so $(x\alpha)(z\alpha) = (z\alpha)(x\alpha)$. Now $x\alpha$ is as arbitrary an element of G as was x because α is an epimorphism. Thus $z\alpha \in Z(G)$. We thus have $(Z(G))\alpha \subseteq Z(G)$, and the reverse inclusion follows from the fact that α^{-1} is an automorphism. Thus $Z(G)$ is invariant by α and so is a characteristic subgroup of G .

If we observe more closely the automorphism group determined in example 4.3.2, we notice that it is Abelian. Is it so because it is the automorphism group of a cyclic group? The next theorem provides the answer.

Theorem 4.3.9

The automorphism group of a cyclic group is Abelian.

Proof

If $G = \langle x \rangle$ and α, β are automorphisms of G , then $(x)\alpha = x^m$, $(x)\beta = x^n$ for some integers m and n . It follows that $(x)\alpha\beta = ((x)\alpha)\beta = (x^m)\beta = x^{mn} = x^{nm} = ((x)\beta)\alpha = (x)\beta\alpha$. Thus, $\text{Aut}(G)$ is Abelian.

Let m be an integer greater than 1. The set of residue classes module m , where the representative of each class is a positive integer less than and relatively prime to m , is of special interest. Routine calculations show that the set of such classes, denoted by G_m , is an Abelian group under the usual multiplication of residue classes. It is now reasonable to ask for the structure of $G_m = \{ \bar{n} : 1 \leq n \leq m \text{ and } n, m \text{ are relatively prime} \}$.

Theorem 4.3.10

$\text{Aut}(Z_m)$ is isomorphic to G_m .

Proof

Corresponding to each positive integer n (less than and relatively prime to m), there exists an automorphism $\alpha_n : Z_m \rightarrow Z_m$ such that $(x)\alpha_n = x^n$ for all $x \in Z_m = \langle z \rangle$, then $(z^k)\alpha_n = (z\alpha_n)^k$ implies that $\text{Aut}(Z_m) = \{ \alpha_n : 1 \leq n < m \text{ and } n, m \text{ are relatively prime} \}$.

If we define a mapping $\phi : \text{Aut}(Z_m) \rightarrow G_m$ by $(\alpha_n)\phi = \bar{n}$, for all $\alpha_n \in \text{Aut}(Z_m)$, then it is easy to verify that ϕ is an isomorphism.

Automorphisms of groups can be used as a means of constructing new groups from the original group. Before going into the details, we consider a particular case first.

Example 4.3.11

Reconsider the groups C_7 and $\text{Aut}(C_7)$ defined in example 4.3.2. Let y be such that $y^3 = 1$, $y^{-1} x^i y = (x^i)\phi = x^{2i}$, and consider all formal words $y^i x^j$, where $i = 0, 1, 2$ and $j = 0, 1, 2, \dots$

6. We claim that $y^i x^j = y^k x^l$ if and only if $i \equiv k \pmod{3}$ and $j \equiv l \pmod{7}$. We multiply these words using the relations $y^3 = x^7 = 1$, $y^{-1}xy = x^2$. in this way, we obtain the group $\langle x, y : x^7 = y^3 = 1, y^{-1}xy = x^2 \rangle$ of order 21.

Generally, if G is a group and α is an automorphism (of order n) of G which is not an outer automorphism, then choose x and consider all words $x^i y$, $i \in \mathbb{Z}$, $y \in G$ subject to $x^i y = x^j y$ if and only if $i \equiv j \pmod{n}$, $y = z$ and $x^{-1} y^i x = y \alpha^i$ for all i . This way, we obtain a larger group $G \cup \{\alpha\}$ such that $G \trianglelefteq G \cup \{\alpha\}$ and $G \cup \{\alpha\}/G$ is isomorphic to the cyclic group $\langle \alpha : \alpha^n = 1 \rangle$.

More formally,

Theorem 4.3.12

If groups F and N are given such that $\phi: F \rightarrow \text{Aut}(N)$ is a homomorphism, then there exists a group G containing a normal subgroup \bar{N} and a subgroup \bar{F} such that

- (i) \bar{F} is isomorphic to F and \bar{N} is isomorphic to N ,
- (ii) G/\bar{N} is isomorphic to F , and
- (iii) The automorphism of \bar{N} induced by conjugation with $x \in \bar{F}$ is automorphism of N defined by $x\phi$, elements of F and \bar{F} and N and \bar{N} being identified in the natural way.

Proof

Define a set $\{x_i : i \in F\}$ by establishing a one-to-one correspondence between the symbols x_i and i . next, we construct the set $G = \{(x_i, n) : i \in F \text{ and } n \in N\}$ and for all $(x_i, n_1), (x_j, n_2) \in G$, we define the multiplication as $(x_i, n_1)(x_j, n_2) = (x_{ij}, (n_1(j\phi))n_2)$. Through routine calculations, one can verify that G is associative. The element $(x_{1_F}, 1_N)$, where 1_F and 1_N are the identity elements in F and N respectively, is the identity element in G . The inverse of (x_i, n) is the element $(x_i^{-1}, n^{-1}(i^{-1}\phi))$. This shows that G is a group.

Note that $\bar{F} = \{(x_i, 1_N) : i \in F\} \leq G$ and $\bar{N} = \{(x_{1_F}, n) : n \in N\} \trianglelefteq G$.

- (i) We can, now, define $\psi : F \rightarrow \bar{F}$ and $\chi : N \rightarrow \bar{N}$ by (i) $\psi(i) = (x_i, 1_N)$ for all $i \in F$ and (ii) $\chi(n) = (x_{1_F}, n)$ for all $n \in N$. It is easy to verify that ψ and χ are isomorphisms.
- (ii) If we define $\phi : G \rightarrow F$ by $(x_i, n)\phi = i$ for all $(x_i, n) \in G$, then it is easy to show that ϕ is an epimorphism and $\text{Ker } \phi = \bar{N}$. Thus, by theorem 3.2.10 (i), G/\bar{N} is isomorphic to F .
- (iii) We observe that $(x_i, 1_N)^{-1} (x_{1_F}, n)(x_i, 1_N) = (x_{1_F}, n(i\phi))$ follows from the definitions. Thus it proves (iii). This completes the proof of the theorem.

The group $G = \{(x_i, n) : i \in F \text{ and } n \in N\}$ is called a split extension of F by N , or a semi-direct product of F by N . For instance, D_{2n} can be constructed from its subgroups $H = \langle x : x^2 = 1 \rangle$ and $K = \langle y : y^n = 1 \rangle$ by taking their semi-direct product as follows.

Define a homomorphism $\phi : K \rightarrow \text{Aut}(H)$ by $(x)\phi = \alpha$, where $\alpha \in \text{Aut}(H)$ is defined by $(y)\alpha = y^{-1}$, for all $x \in K$. Then $H \rtimes K$ forms a group when the product of its elements $(h, k), (h', k')$ is defined as: $(h, k)(h', k') = (h(k)\phi(h'), k k')$. The group $H \rtimes K$ is isomorphic to D_{2n} .

Notice that if ϕ maps the whole of K onto the identity element in $\text{Aut}(H)$, we get the direct product of H and K . In constructing a group G from simpler groups H and K , it is hoped that some of the properties of G can be deduced from those of H and K and the nature of construction. Thus, what we have established in theorem 4.3.12 is the following.

Given a group F and group N we can find a group G such that N is a normal subgroup of G and G/N is isomorphic to F . This is the extension problem. The group G is called an extension of N by F . The theory of such constructions has been extensively studied since O. Schreier first considered the problem in about 1920.

4. Exercises

1. Prove that every permutation, except the identity permutation displaces at least two symbols.
2. Determine the order of $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 0 & 1 \end{pmatrix}$.
3. Describe the permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 4 & 7 & 3 & 6 & 5 & 10 & 8 & 9 \end{pmatrix}$.
4. Calculate xy where $x = (1 \ 2 \ 3 \ 4) (5 \ 6 \ 7) (8 \ 9)$ and $y = (1 \ 10) (2 \ 5 \ 9) (3 \ 4 \ 6 \ 7)$.
5. Find the order of xy in exercise 4.
6. Find the inverse of $\begin{pmatrix} a & b & c & d & e & f & g \\ e & g & f & d & a & b & c \end{pmatrix}$ and $(a \ b \ c \ d \ e \ f \ g \ h) (i \ j \ k \ l)$.
7. Prove that any permutation on $\{1, 2, \dots, n\}$ can be expressed as the product of transpositions of the form $(1 \ 2), (1 \ 3), \dots, (1 \ n)$.
8. Prove that a cycle is odd or even according as its order is even or odd.
9. Let $\text{Hom}(S_3, Z_8)$ denote the group of all homomorphisms from the group S_3 to the group Z_8 . Determine the order of $\text{Hom}(S_3, Z_8)$.
10. If G_1 and G_2 are isomorphic groups then prove that $\text{Aut}(G_1)$ is isomorphic to $\text{Aut}(G_2)$ and $\text{In}(G_1)$ is isomorphic to $\text{In}(G_2)$.
11. If G is a group, $\alpha \in \text{Aut}(G)$ and $x \in G$ then prove that $\text{order}((x)\alpha) = \text{order}(x)$.
12. Find the group of all the automorphisms of S_3 .
13. Prove that $\text{Aut}(Z^+)$ is isomorphic to Z^\times .

14. Prove that $\text{Aut}(Z_n^+)$ is isomorphic to Z_n^+ for every positive integer n .
15. Find the permutation representation of A_4 .
16. Prove that $\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(3\ 2)\}$ form a normal subgroup of A_4 .
17. Prove that C_4 is isomorphic to $\text{Sym}(C_4)$.
18. Let G be a group. Prove that $\text{In}(G) \trianglelefteq A(G)$.
19. Compute and identify S_3/A_3 .
20. Compute and identify A_4/V_4 .
21. Show that the group $\langle a, b: a^3 = b^2 = (ab)^3 = 1 \rangle$ is isomorphic to A_4 .
22. Prove that the subgroup of S_4 generated by the permutations $(a\ 2\ 3\ 4)$ and $(1\ 3)$ is isomorphic to D_4 .