

## CHAPTER THREE

### STRUCTURE PRESERVING MAPPING

#### 1. INTRODUCTION

Given a group and normal subgroup  $K$  of  $G$ , we have learnt how to construct the factor group  $G/K$ . What about the converse of this? That is, if we are given a group  $K$  and group  $H$ , can we find a group  $G$  such that  $K$  is a normal subgroup of  $G$  and  $G/K$  is similar to  $H$ ? This is known as the extension problem; the group  $G$  is said to be an extension of  $K$  by  $H$ . The theory of such extensions has been extensively studied since O. Schreier first considered the problem in the problem in the 1920s.

In the chapter, we will consider certain structure preserving mappings, which are prerequisite for the answer of the above-mentioned question. Specifically, we will study homomorphism, isomorphisms, automorphisms, and some of their uses.

#### 2. HOMOMORPHISM

If we can show that the group  $G$  in which we are interested is isomorphic to a group whose structure is known, then  $G$  can be identified with the known group. Hence the structure of  $G$  is also known. The identification of  $G$  with a known group is done through an isomorphism. However, it is not always possible to obtain an isomorphism. Usually, we have to be content with a mapping (between  $G$  and some known group) which is neither one-to-one nor onto but which still preserves the structure. Formally, it means:

Let  $G$  and  $H$  be groups and  $\phi$  be a mapping from  $G$  to  $H$ . Then  $\phi$  is called a homomorphism if it preserves the group structure, that is,  $(xy)\phi = (x)\phi(y)\phi$ , for all  $x, y \in G$ .

For instance:

##### **Example 3.2.1**

Let us consider the group  $GL(2, \mathbf{R})$ , under matrix multiplication, of non-singular  $2 \times 2$  matrices with entries from the real line  $\mathbf{R}$ . We define a mapping  $\phi$  from  $GL(2, \mathbf{R})$  to the multiplicative group  $\mathbf{R}^*$  of non-zero real numbers by setting  $(M)\phi = \text{DET}(M)$  for all  $M \in GL(2, \mathbf{R})$ . Then  $\phi$  is a homomorphism because  $(MN)\phi = \text{DET}(MN) = \text{DET}(M) \text{DET}(N) = (M)\phi (N)\phi$  for all  $M, N \in GL(2, \mathbf{R})$ .

### Example 3.2.2

Define a mapping  $\phi$  from a group of integers under addition and the group of integers modulo  $n$  (see example 1.2.9) under addition by  $(z)\phi = \bar{z}$ , for all  $z \in \mathbf{Z}$ . Then, it is quite easy to see that it is a homomorphism.

### Example 3.2.3

Let  $a \in \mathbf{R}$ . Then  $\lambda_a: \mathbf{R} \rightarrow \mathbf{R}$  and  $\rho_a: \mathbf{R} \rightarrow \mathbf{R}$ , defined by  $(x)\lambda_a = ax$  and  $(x)\rho_a = xa$  for all  $x \in \mathbf{R}$  are homomorphisms, because  $(x + y)\rho_a = a(x + y) = ax + ay = (x)\rho_a + (y)\rho_a$ , and  $(x + y)\rho_a = (x + y)a = xa + ya = (x)\rho_a + (y)\rho_a$ , for all  $x, y \in \mathbf{R}$ .

If there is a one-to-one homomorphism between two groups, then the homomorphism is called a monomorphism. If  $\phi$  is a monomorphism from a group  $G$  to a group  $H$  then  $G$  is said to be embedded in  $H$ . For every two groups  $G$  and  $H$  there is at least one homomorphism  $\phi: G \rightarrow H$  defined by  $(x)\phi = 1$  for all  $x \in G$ . This homomorphism is known as a trivial homomorphism. A homomorphism which is onto is called an epimorphism. For instance the mapping defined in the example below is an epimorphism.

### Example 3.2.4

Let  $H$  and  $K$  be any two groups. Define a mapping  $\pi: H \times K \rightarrow H$  by  $(h, k)\pi = h$ , for all  $(h, k) \in H \times K$ . Then it is easy to prove that  $\pi$  is an epimorphism. This epimorphism  $\pi$  is called a projection from the direct product  $H \times K$  onto  $H$ . Note that, similarly we can define a projection from  $H \times K$  onto  $K$ .

A homomorphism which is one-to-one and onto is called an isomorphism. If there is an isomorphism between groups  $G$  and  $H$ , then the groups  $G$  and  $H$  are called isomorphic. If  $G$  and  $H$  are isomorphic, then we write it as:  $G \cong H$ . The mapping  $1: G \rightarrow G$ , defined by  $(x)1 = x$  for all  $x \in G$ , is an isomorphism and is called the identity isomorphism and is called the identity isomorphism. Also, it is fairly easy to see that the composition of two isomorphisms is again an isomorphism. Moreover, because an

isomorphism is a one-to-one and onto mapping, its inverse exists. It is also easy to see that isomorphisms satisfy the associative law. This shows that the set of isomorphisms from a group under the operation of composition of mappings.

It is important to mention that ' $\cong$ ' is an equivalence relation and consequently partitions the collection of groups into non-empty disjoint equivalent classes of groups.

Notice the following natural properties of a homomorphism from a group  $G$  into a group  $H$ .

- (i)  $(1)\phi = 1'$ , where  $1$  is the identity in  $G$  and  $1'$  is identity in  $H$ .
- (ii)  $(x^{-1})\phi = ((x)\phi)^{-1}$ , for every  $x \in G$ .
- (iii)  $\text{Im}(\phi) = \{ y \in H : (x)\phi = y \} \leq H$ .

Let us now consider a few examples of isomorphisms.

### Example 3.2.5

Let  $C^x$  be the group under multiplication of non-zero complex numbers and let  $G$  be the group under matrix multiplication of matrices of the form  $\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ , where  $a, b$  are real numbers not both zero. Define  $\phi: C^x \rightarrow G$  by  $(a + ib)\phi = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ , for every  $a + ib \in C^x$ . then it can be easily verified that  $\phi$  is an isomorphism. Thus  $C^x \cong G$ .

All the finite cyclic groups of order  $n$  can be identified with the cyclic group  $Z_n$  whereas all the infinite cyclic groups can be identified with the infinite cyclic group  $Z$ . We show this, through the following examples.

### Example 3.2.6

We assert that all the cyclic groups of order  $n$  are isomorphic to the group  $Z_n^+ = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$  under addition.

Let  $C_n = \{1, x, x^2, \dots, x^{n-1}\} = \langle x : x^n = 1 \rangle$ . Define a mapping  $\phi: C_n \rightarrow Z_n^+$  by  $(x^r)\phi = \bar{r}$ , for all  $x^r \in C_n$ . Then  $(1)\phi = \bar{0}$ ,  $(x)\phi = \bar{1}$ ,  $(x^2)\phi = \bar{2}$ ,  $\dots$ ,  $(x^{n-1})\phi = \overline{n-1}$ . It is not difficult to see from here that  $\phi$  is a well-defined, one-to-one and an onto mapping. If  $0 \leq r \leq n-1$  and  $0 \leq s \leq n-1$ , then  $(x^r, x^s)\phi = (x^{r+s})\phi = (x^t)\phi$ , where  $0 \leq t \leq n-1$  and  $r + s \equiv t \pmod{n}$ . Now because  $r + s \equiv t \pmod{n}$ ,  $(x^t)\phi = \bar{t} = \bar{r} + \bar{s} = (x^r)\phi + (x^s)\phi$ . Thus  $\phi$  is an isomorphism from  $C_n$  onto  $Z_n^+$  implying that  $C_n \cong Z_n^+$ .

Example claim that all infinite cyclic groups are isomorphic to  $\mathbb{Z}$  group of integers under addition. Let us denote  $C_\infty$  to be an infinite cyclic group:

$\{1, x^{\pm 1}, x^{\pm 2}, \dots, x^{\pm r}, \dots\} = \langle x \rangle$ . Define a mapping  $\phi: C_\infty \rightarrow \mathbb{Z}^+$  by  $(x^r)\phi = r$  for all  $x^r \in C_\infty$ . Then it is simple to show that  $\phi$  is well defined, one-to-one and onto. Moreover,  $(x^r \cdot x^s) \in C_\infty$ . Thus  $\phi$  is an isomorphism; and so  $C_\infty \cong \mathbb{Z}^+$ .

If  $\phi$  is a homomorphism from a group  $G$  into a group  $H$  then the kernel of  $\phi$ , denoted by  $\text{Ker } \phi$ , is defined as:

If  $\phi$  is a homomorphism from a group  $G$  into a group  $H$  then the kernel of  $\phi$ , denoted by  $\text{Ker } \phi$ , is defined as:

$$\text{Ker } \phi = \{x \in G \mid (x)\phi = 1', \text{ where } 1' \text{ is the identity of } H\}.$$

As an illustration we indicate the kernel of the homomorphism  $\phi$  from  $\text{GL}(2, \mathbb{R})$  to  $\mathbb{R}^\times$  described in example 3.2.1. If  $M \in \text{GL}(2, \mathbb{R})$  then  $(M)\phi = \det(M)$ ; therefore the kernel of  $\phi$  consists of those matrices  $M$  which have determinant 1.

Next, we investigate the structure of the Kernel of a homomorphism.

### Theorem 3.2.8

If  $\phi$  is a homomorphism from a group  $G$  into a group  $h$ , then  $\text{Ker } \phi \trianglelefteq G$ .

#### Proof

First, note that  $\text{Ker } \phi$  is non-empty because  $(1)\phi = 1'$  implies that  $1 \in \text{Ker } \phi$ .

Now, if  $x, y \in \text{Ker } \phi$  then  $(x)\phi = 1'$  and  $(y)\phi = 1'$  so,  $(xy^{-1})\phi = (x)\phi(y^{-1})\phi = (x)\phi(y)\phi^{-1} = 1'$  implies that  $xy^{-1} \in \text{Ker } \phi$ . Thus, theorem 1.5.10,  $\text{Ker } \phi \leq G$ .

Now, if  $x \in G$  and  $k \in K$  then  $(k)\phi = 1'$  and so  $(xhx^{-1})\phi = (x)\phi(k)\phi(x^{-1})\phi = (x)\phi(1'((x)\phi)^{-1}) = 1'$ . Thus  $xkx^{-1} \in \text{Ker } \phi$  and so, by theorem 2.4.4,  $\text{Ker } \phi \trianglelefteq G$ .

One way of knowing the structural properties of a group  $G$  is to identify it with some known group  $H$ . This can be done by defining a homomorphism  $\phi$  between  $G$  and  $H$  and showing that  $\phi$  is one-to-one and onto. The following result shows that the smaller the Kernel of  $\phi$  is, the more isomorphism-like  $\phi$  will be.

### Theorem 3.2.9

A homomorphism  $\phi$  from a group  $G$  into a group  $H$  is a monomorphism if and only if  $\text{Ker } \phi = \{1\}$ .

**Proof**

First, suppose that  $\phi : G \rightarrow H$  is a monomorphism. If we let  $x \in \text{Ker } \phi$ , then  $(x)\phi = 1'$  and so  $(1)\phi = 1'$  implies that  $(x)\phi = (1)\phi$ . Since  $\phi$  is one-to-one it implies that  $x = 1$ . Thus  $\text{ker } \phi = \{1\}$ .

Conversely, suppose that  $\text{Ker } \phi = \{1\}$  and  $(x)\phi = (y)\phi$  for arbitrary  $x, y \in G$ . This means that  $(x)\phi((y)\phi)^{-1} = 1'$ . That is,  $(x)\phi(y^{-1})\phi = (xy^{-1})\phi = 1'$  and so  $xy^{-1} \in \text{Ker } \phi = \{1\}$ . Thus,  $xy^{-1} = 1$  implies that  $x = y$ . This shows that  $\phi$  is a monomorphism.

We have seen earlier that with any homomorphism  $\phi : G \rightarrow H$  there is associated a normal subgroup, namely  $\text{Ker } \phi$ . The next theorem which is often known as the first isomorphism theorem, and is attributed to E. Neithier, shows that  $G$  is an extension of  $\text{Ker } \phi$  by  $H$ .

**Theorem 3.2.10**

- (i) Let  $\phi$  be a homomorphism from a group  $G$  into a group  $H$  and  $K = \text{Ker } \phi$ . Then  $\phi$  defined by  $(xK)\phi = (x)\phi$ , for all  $xK \in G/K$ , is isomorphism from  $G/K$  to  $\text{Im}(\phi)$ .
- (ii) If  $K \trianglelefteq G$  then there is a natural epimorphism  $\pi$  from  $G$  onto  $G/K$  such that  $\text{Ker } \pi = K$ .
- (iii)  $\phi = \pi \phi$ .

**Proof**

- (i) If  $xK, yK \in G/K$  and  $xK = yK$ , then  $y^{-1}x \in K$ . This implies that  $(y^{-1}x)\phi = 1'$ , where  $1'$  is the identity in  $H$ . Thus  $(y^{-1}x)\phi(y^{-1})\phi(x)\phi = ((y\phi)^{-1}(x)\phi) = 1'$  implies that  $(x)\phi = (y)\phi$ , that is,  $(xK)\phi = (yK)\phi$ . This shows that  $\phi$  is well-defined.

If  $xK, yK \in G/K$  and  $(xK)\phi = (yK)\phi$ , then  $(x)\phi = (y)\phi$  implies that  $((y)\phi)^{-1}(x)\phi = (y^{-1})\phi(x)\phi = (y^{-1}x)\phi = 1$ . This shows that  $y^{-1}x \in K$ . That is  $xK = yK$ . This shows that  $\phi$  is one-to-one.

If  $y \in \text{Im } \phi$ , then there exists  $x \in G$  such that  $(x)\phi = y$ . This implies that for every  $y \in \text{Im } \phi$ , there exists  $xK \in G/K$  such that  $(xK)\phi = (x)\phi = y$ . This shows that  $\phi$  is onto.

If  $xK, yK \in G/K$ , then  $(xKyK)\phi = ((xy)K)\phi = (xy)\phi = (x)\phi(y)\phi = (xK)\phi(yK)\phi$ . This shows that  $\phi$  is a homomorphism. This completes the proof of (i).

(ii) Define a mapping  $\pi: G \rightarrow G/K$  by  $(x)\pi = xK$ , for all  $x \in G$ . Then it is fairly simple to show that  $\pi$  is an epimorphism. (note that this mapping is known as the natural (or canonical) epimorphism.

If  $x \in \ker \pi$ , then  $(x)\pi = K$ , as  $K$  is the identity in  $G/K$ . But  $(x)\pi = xK$ , by definition, and so  $xK = K$ . This shows that  $x \in K$ . That is  $\ker \pi \subseteq K$ . On the other hand, if  $x \in K$ , then  $(x)\pi = xK = K$  implies that  $x \in \ker \pi$ . That is  $K \subseteq \ker \pi$ . The two inclusions, thus, imply that  $K = \ker \pi$ . This proves (ii).

(iv) By (i), we have  $G/K \cong \text{Im } \phi$ . In order to check that  $\phi = \pi\phi$ , we let  $x \in G$ . Then  $(x)\pi\phi = ((x)\pi)\phi = (xK)\phi = (x)\phi$ . This is true for all  $x \in G$ . Thus  $\pi\phi = \phi$ . This concludes the theorem.

The following examples illustrate the afore-mentioned theorem.

### Example 3.2.11

Let  $F$  be a field,  $F^\times = F \setminus \{0\}$  and  $GL(3, F)$  denote the group (under multiplication) of  $3 \times 3$  non singular matrices with entries from the field  $F$ . Define a mapping  $\phi: GL(3, F) \rightarrow F^\times$  by  $(M)\phi = \det(M)$ , for all  $M \in GL(3, F)$ . Then it is not hard to see that  $\phi$  is an epimorphism and  $\ker \phi = \{M \in GL(3, F) : \det(M) = 1\}$  (This normal subgroup of  $GL(3, F)$  is denoted by  $SL(3, F)$  and is known as the special linear group of degree 3 over  $F$ . A detailed description of this will be given in the last chapter. By theorem 3.2.10,  $GL(3, F)/SL(3, F) \cong F^\times$ .

### Example 3.2.12

For a positive integer  $n$ , define a mapping  $v_n$  from a group  $Z^\times$ , of integers under addition and the cyclic group  $C_n$  of order  $n$  by  $(z)v_n = e^{2\pi i z/n}$ , for all  $z \in Z^+$ . It can be proved easily that  $\ker v_n = \{nz : z \in Z^+\} = nZ^+$ . By theorem 3.2.10, this implies that  $C_n = \text{Im } v_n \cong Z^+/\ker v_n \cong Z^+/nZ^+$ . Thus,  $Z^+$  has a factor group of order  $n$  corresponding to every positive integer  $n$ .

Next, we prove the second isomorphism theorem which describes the structure of a factor group.

### Theorem 3.2.13

If  $G$  is a group,  $K \trianglelefteq G$  and  $K \leq H \trianglelefteq G$ , then  $G/K \big/_{H/K}$  is isomorphic to  $G/H$ .

**Proof**

First, note that since  $K \trianglelefteq G$  and  $K \leq H \leq G$ , therefore, by theorem 2.4.9,  $K \trianglelefteq H$  and so we can define the factor groups  $G/K$ ,  $H/K$  and  $G/H$ .

Define a mapping  $\phi: G/K \rightarrow G/H$  by  $(xK)\phi = xH$  for all  $xK \in G/K$ . The mapping  $\phi$  is obviously well-defined because if  $xK = yK$ , then  $y^{-1}x \in K$  implies that  $y^{-1} \in K$  implies that  $y^{-1}x \in H$ , as  $K \leq H$ , and so  $xH = yH$ .

If  $xK, yK \in G/K$ , then  $(xKyK)\phi = ((xy)K)\phi = (xy)H = xHyH = (xK)\phi(yK)\phi$  implies that  $\phi$  is a homomorphism.

The homomorphism  $\phi$  is obviously an epimorphism because for every  $xH \in G/H$ , there exists  $xK \in G/K$  such that  $(xK)\phi = xH$ .

If  $xK \in \text{Ker } \phi$ , then  $(xK)\phi = H$  because  $H$  is the identity in  $G/H$ . Now  $(xK)\phi = xH$ , for all  $xK \in G/K$ , implies that  $xH = H$ . This, of course, means that  $x \in H$ . Thus  $xK \in H/K$  and so  $\text{Ker } \phi \subseteq H/K$ . Conversely, if  $xK \in H/K$ , then  $(xK)\phi = xH$  and so  $x \in H$  implies that  $(xK)\phi = xH = H$ . This implies that  $xK \in \text{Ker } \phi$ , showing that  $H/K \subseteq \text{Ker } \phi$ . The two inclusions, thus, imply that  $\text{Ker } \phi = H/K$ . Hence, by theorem 3.2.10(i),  $G/K \big/_{H/K}$  is isomorphic to  $G/H$ . Although we have classified all the cyclic groups already, here is another way of looking at the classification. In examples 3.2.6 and 3.2.7 we have seen that

$C_n \cong Z_n^+ \cong Z^+ /_{nZ^+}$  and  $C_\infty \cong Z^+$  whereas here we use the isomorphism theorems to classify all subgroups and all factor groups of  $Z^+$ .

**Example 3.2.14**

If  $\lambda_n: Z^+ \rightarrow Z^+$  is defined by  $(Z)\lambda_n = nz$ , for all  $z \in Z^+$  and  $n$  a positive integer, then it is obvious that  $\lambda_n$  is a monomorphism and  $\text{Im } \lambda_n = nZ^+ \cong Z^+$ . We know already, by example 3.2.12, that  $Z^+ /_{nZ^+} \cong C_n$ ; and of course  $Z^+ / \{0\} \cong Z^+$ . Note that every subgroup and every factor group of  $Z^+$  is cyclic and also that each subgroup is either finite, in which case it is  $\{0\}$ , or has a finite factor group.

It is easy to see that  $nZ^+$  is cyclic and also that each subgroup is either finite, in which case it is  $\{0\}$ , or has a finite factor group.

It is easy to see that  $nZ^+ \trianglelefteq mZ^+$  if and only if  $m$  divides  $n$ . Hence the subgroups of  $Z^+/nZ^+$  are just the subgroups  $Z^+/mZ^+$ , one for each divisor  $m$  of  $n$ . By theorem 3.2.13,

when  $m$  is a divisor of  $n$ , we have  $Z^+/nZ^+ / (mZ^+/nZ^+) \cong Z^+/mZ^+ \cong C_m$ .

Moreover, since  $|Z^+/nZ^+| = n$  and  $|Z^+/mZ^+| = m$ , therefore, by Lagrange's theorem  $|mZ^+/nZ^+| = n/m$ . Also,  $mZ^+ \cong Z^+$  and since every factor group of  $Z^+$  is cyclic,  $mZ^+/nZ^+$  is cyclic thus every subgroup  $Z^+/nZ^+$  is cyclic.

The following example shows another interesting use of theorem 3.2.13.

### Example 3.2.15

We consider a homomorphism  $\phi$  from a group  $G$  onto any Abelian group  $A$ , with particular reference to theorem 2.5.6. Thus  $\text{Ker } \phi = M$  contains  $G'$  and by theorem 3.2.13, we obtain  $G/M \cong G/G' / M/G'$ .

In other words,  $\phi = \phi_1 \circ \phi_2$  where  $\phi_1$  is the natural homomorphism of  $G$  onto  $G/G'$  and  $\phi_2$  is the natural homomorphism of  $G/G'$  onto  $G/G' / M/G'$ . Thus every homomorphism of  $G$  onto  $A$  may be expressed as the product of  $\phi_1$  and a suitable homomorphism of  $G/G'$ .

Next, we prove that third isomorphism theorem.



**Theorem 3.2.16**

If  $G$  is a group,  $H \leq G$  and  $K \trianglelefteq G$ , then  $H/H \cap K \cong HK/K$ .

**Proof**

First, note that  $HK$  is defined as in Section 1.5 and that  $H \cap K \trianglelefteq H$  by theorem 2.4.8; implying that  $H/H \cap K$  is well-defined.

The set  $HK = \{hk : h \in H \text{ and } k \in K\}$  is non-empty because  $1 \in HK$ . If  $h_1, h_2 \in H$  and  $k_1, k_2 \in K$ , then  $(h_1, h_2)^{-1} = h_1^{-1} k_1^{-1} k_2^{-1} h_2^{-1} = h_1^{-1} (h_2^{-1} h_2) k_1^{-1} k_2^{-1} h_2^{-1} = (h_1^{-1} h_2^{-1}) (h_2 k_1 k_2^{-1} h_2^{-1}) \in HK$  because  $h_1^{-1} h_2^{-1} \in H$ ,  $k_1^{-1} k_2^{-1} \in K$ ,  $h_2 (h_2^{-1})^{-1} = 1$  and  $K \trianglelefteq G$ . Thus the factor group  $HK/K$  is well-defined.

Let  $\pi_H$  be the restriction of the natural epimorphism  $\pi: G \rightarrow G/K$  to  $H$ . The  $\pi_H: H \rightarrow G/K$  is a homomorphism with  $\text{Ker } \pi_H = \{h \in H : h \in \text{Ker } \pi\} = H \cap K$  by theorem 3.2.10,  $H/H \cap K \cong \text{Im } \pi_H$ . Now,  $K \trianglelefteq HK \leq G$  and for each  $h \in H$ ,  $(h)\pi = hK \in HK/K$ . Moreover, each element of  $HK/K$  is of the form  $hkK = hK = h\pi_H$ , with  $h \in H$  and  $k \in K$ . Thus  $\text{Im } \pi_H = HK/K$  implies that  $H/H \cap K \cong HK/K$ .

The following example illustrates the afore-mentioned theorem.

**Example 3.2.17**

Let  $\mathbb{Q}^\times$  denote the group of rationals under multiplication,  $K = \{1, -1\}$  and  $H = \langle 1/2 \rangle$ . Then  $HK = \{hk : h \in H \text{ and } k \in K\} = \{\pm h : h \in H\} = \{\pm (1/2)^r : \text{for all } r \in \mathbb{Z}\}$ . An element of  $HK/K$  is of the form  $xK = \{x, -x\}$  where  $x \in HK$ . Now if  $x \in HK$ ,  $x = \pm (1/2)^r$ . Hence each coset is of the form  $\{(1/2)^r, -(1/2)^r\}$  and so each coset of  $K$  in  $HK$  is a power of  $(1/2)K$ . Thus  $\langle (1/2)K \rangle = HK/K$ ; and since  $(1/2)^r \notin K$  for  $r \neq 0$ ,  $HK/K$  is the infinite cyclic group. Now,  $H \cap K = \{x : x = (1/2)^r \text{ for some } r \text{ and } x = \pm 1\} = \{1\}$ . Hence  $H/H \cap K \cong H$ . But  $H$  is an infinite cyclic group; thus we have verified that  $H/H \cap K \cong HK/K$ .

If  $G$  is a group and  $H, K \leq G$  then, by using an isomorphism, we show in the proceeding theorem that the two structures, namely  $H \times K$  and  $HK$ , are similar under certain conditions.

**Theorem 3.2.18**

If  $H, K$  are groups such that  $H \cap K = \{1\}$  and  $HK = KH$ , then  $HK \cong H \times K$ .

**Proof**

If  $x \in HK$ , then  $x = hk$  for some  $h \in H$  and  $k \in K$ . Suppose that  $x$  has another form such as  $= h_1 k_1$  where  $h_1 \in H$  and  $k_1 \in K$ . So  $hk = h_1 k_1$  implies that  $h_1^{-1} h = k_1^{-1} k$  and so  $h_1^{-1} h = k_1 k^{-1} = 1$  belongs to  $H \cap K = \{1\}$  implies that  $h_1^{-1} h = k_1 k^{-1} = 1$ . This shows that  $h = h_1$  and  $k = k_1$ . Thus  $x$  has a unique presentation.

If  $\phi : HK \rightarrow H \times K$  is defined by  $(x)\phi = (hk)\phi = (h, k)$ , for all  $x \in HK$ , then  $\phi$  is well-defined. For, if  $x, y \in HK$  such that  $x = y$ , then  $x = hk$  and  $y = h_1 k_1$  for some  $h, h_1 \in H$  and  $k, k_1 \in K$ . Since  $x = y$  has unique presentation,  $h = h_1$  and  $k = k_1$  so  $(x)\phi = (hk)\phi = (h, k) = (h_1, k_1) = (y)\phi$  implies that  $\phi$  is well-defined.

If  $x, y \in HK$ , then  $x = hk$  and  $y = h_1 k_1$  for some  $h, h_1 \in H$  and  $k, k_1 \in K$ . Now  $(x)\phi = (y)\phi$  implies that  $(h, k) = (h_1, k_1)$ , and so  $h = h_1$ ,  $k = k_1$ . This shows that  $x = y$ , that is,  $\phi$  is one-to-one.

Also, if  $x, y \in HK$ , then  $x = hk$  and  $y = h_1 k_1$  (for some  $h, h_1 \in H$  and  $k, k_1 \in K$ ) imply that  $(xy)\phi = (hkh_1 k_1)\phi = (hh_1 k k_1)\phi$  because every element of  $H$  commutes with every element of  $K$ . Thus,  $(xy)\phi = (hh_1 k k_1)\phi = (hh_1, k k_1) = (h, k)(h_1, k_1) = (hk)\phi(h_1, k_1) = (x)\phi(y)\phi$ , for all  $x, y \in HK$ . This shows that  $\phi$  is a homomorphism.

Now,  $\phi$  is obviously an epimorphism because for every  $(h, k) \in H \times K$ , there exists  $hk \in HK$  such that  $(hk)\phi = (h, k)$ . This proves that  $\phi$  is an isomorphism, that is,  $HK \cong H \times K$ .

The example given below, illustrates theorem 3.2.18.

### Example 3.2.19

Consider the groups  $C_2 = \langle x : x^2 = 1 \rangle$  and  $C_3 = \langle y : y^3 = 1 \rangle$ . Then  $C_2 \cap C_3 = \{1\}$  and  $C_2 C_3 = C_2 C_3 = C_3 C_2 = \{1, x, y, y^2 xy, xy^2\}$ . On the other hand,  $C_2 \times C_3 = \{(1, 1), (x, 1), (1, y), (1, y^2), (x, y), (x, y^2)\}$ . If a mapping  $\phi : C_2 C_3 \rightarrow C_2 \times C_3$  is defined by  $(ab)\phi = (a, b)$  for all  $a \in C_2$  and  $b \in C_3$ , then through routine calculations one can show very easily that  $\phi$  is an isomorphism.

### 3. Conjugacy Classes

In section 2.5, we have considered some important factor groups. One of them occupies an important position in group theory. We will discuss it in this section with emphasis on its application in the theory of finite groups.

If  $G$  is a group, then by theorem 2.5.10, the centre of  $G$ , namely  $Z(G)$ , is normal in  $G$ . This means that we can factor the group  $G$  by  $Z(G)$ . The factor group  $G/Z(G)$  is isomorphic to a group of special types of isomorphisms. We will discuss it in detail in the next chapter but here we will look at it from a different point of view.

If  $z \in Z(G)$  then  $zg = gz$  for every  $g \in G$ . This means that  $g^{-1}zg = z$  for all  $g \in G$ . We can generalize this notion in the following fashion. We call  $x, y \in G$  to be conjugates of each other if and only if  $x = g^{-1}yg$  for some  $g \in G$ . If  $x, y \in G$  and ' $x$  is conjugate' then we denote this fact by  $x \sim y$ . Thus  $x \sim y$  if and only if there exists some  $g \in G$  such that  $x = g^{-1}yg$ . Let  $N_G(x)$  denote the set containing all those elements of  $G$  which commute with  $x$ . The set  $N_G(x)$  is called the centralizer of  $x$  in  $G$ .

### **Theorem 3.3.1**

If  $G$  is a group and  $x \in G$ , then  $N_G(x) \leq G$ .

#### **Proof**

If  $y, z \in N_G(x)$ , then  $y x^{-1} y x$  and  $z = x^{-1} z x$ , and so  $yz^{-1} = (x^{-1} y x) (x^{-1} z x)^{-1} = (x^{-1} y x) (x^{-1} z^{-1} x) = x^{-1} y (x x^{-1}) z^{-1} x = (x^{-1} y^{-1}) (z^{-1} x) = x^{-1} (y z^{-1}) x$  implies that  $y z^{-1} \in N_G(x)$ . Thus by theorem 1.5.10.  $N_G(x) \leq G$ .

The relation  $\sim$  defined in the beginning of this section is an equivalence relation and partitions  $G$  into non-empty and disjoint equivalent classes. These classes are called Conjugacy classes. Before we discuss the nature of these Conjugacy classes, we prove the following theorem.

### **Theorem 3.3.2**

If  $G$  is a group, then the relation  $\sim$  is an equivalence relation.

#### **Proof**

Since  $x = 1^{-1} x$ , therefore,  $x \sim x$  and so  $\sim$  is reflexive. If  $x \sim y$  then there exists an element  $g \in G$  such that  $x = g^{-1} y g$ , and so  $y = g x g^{-1} = (g^{-1})^{-1} x g^{-1}$  implies that  $y \sim x$ . This shows that  $\sim$  is symmetric. Next, if  $x \sim y$  and  $y \sim z$ , then there exist  $g, h \in G$  such that  $x = g^{-1} y g$  and  $y = h^{-1} z h$ , and so  $x = g^{-1} y g = g^{-1} (h^{-1} z h) g = g^{-1} h^{-1} z (h g) = (h g)^{-1} z (h g)$  implies that  $x \sim z$ . This shows that  $\sim$  is transitive; thus implying that  $\sim$  is an equivalence relation.

If  $a \in G$ , then  $[a] = \{x \in G: X \sim a\}$  is called the conjugacy class of  $a \in G$  under the relation  $\sim$ . It consists of all distinct elements of the form  $y^{-1}ay$  as  $y$  ranges over  $G$ . since, by theorem 3.3.2,  $\sim$  is an equivalence relation, it partitions  $G$  into non-empty and disjoint equivalence classes.

Here we point out the following properties of elements of a Conjugacy class.

**Lemma 3.3.3**

If  $G$  is a group and  $a \in G$ , then all elements in  $[a]$  have the same order.

**Proof**

If  $x \in [a]$ , then  $x = y^{-1}ay$ . If  $\text{ord}(x) = n$  and  $\text{ord}(a) = m$ , then  $x^m = (y^{-1}ay)^m = (y^{-1}ay) \dots (y^{-1}ay)$ ,  $m$ -times, implies that  $x^m = y^{-1}a^m y$ . Since  $\text{ord}(a) = m$ , we obtain  $x^m = y^{-1}1y = y^{-1}y = 1$ . This implies that  $n \leq m$ . Similarly,  $1 = x^n = (y^{-1}ay)^n = (y^{-1}ay)(y^{-1}ay) \dots (y^{-1}ay) = y^{-1}a^n y$  implies that  $1 = y^{-1}a^n y$ . That is,  $a^n = 1$ . This implies that  $m \leq n$ . The two inequalities together imply that  $m = n$ . Hence the result.

**Lemma 3.3.4**

If  $G$  is a group and  $H \leq G$  then  $H \trianglelefteq G$  if and only if  $H$  consists of the union of complete Conjugacy classes.

**Proof**

Suppose that  $H \trianglelefteq G$ . if  $x$  is conjugate to an element  $h \in H$ , then  $x = g^{-1}hg \in H$  and so  $H$  consists of complete Conjugacy classes.

Conversely, suppose that  $H$  consists of complete Conjugacy classes. If  $h \in H$  and  $g \in G$  then  $g^{-1}hg$  is conjugate to  $h$  and hence belongs to  $\{h\} \subseteq H$ . Thus  $g^{-1}H$  implies that  $H \trianglelefteq G$ .

Notice that  $x$  is alone in its Conjugacy class if and only if  $x = g^{-1}xg$  for all  $g$  belonging to a group  $G$ . The collection of all such elements is the centre of  $G$ , which we have already talked about in section 2.5.

The groups whose orders are powers of primes occupy special position in the theory of finite simple groups. In the following results, we explain how the order of the centre of a group can be used to determine the order of the group whose order is a power of a prime.

**Theorem 3.3.5**

If  $G$  is a finite group, then

- (i)  $|G| = |Z(G)| + \sum_{i=1}^r h_i$  where  $h_i > 1$  and  $h_i = [x_i]$  and  $h_i = |G : N_G(x_i)|$  for any element  $x_i$  in the  $i$ -th Conjugacy class.
- (ii) if  $|G| = p^r$ , for some prime  $p$ , then  $|Z(G)| = p^s > 1$ .

**Proof**

- (i) Because the Conjugacy classes form a partition of  $G$ , it follows that

$|G| = 1 + 1 + \dots + 1 + \sum_{i=1}^r h_i$ , where the number of 1 in the equation represent the number of Conjugacy classes containing a single element. Note that these are precisely the elements in the center of  $G$ .

Thus  $|Z(G)| = 1 + 1 + \dots + 1$  implies that  $|G| = |Z(G)| + \sum_{i=1}^r h_i$ , where  $h_i > 1$  and  $h_i = [x_i]$ .

- (ii) If  $|G| = p^r$ , for some prime  $p$ , then by (i)  $p^r = |Z(G)| + \sum_{i=1}^r h_i$ , with  $h_i > 1$ . since  $h_i = |G : N_G(x_i)| = \frac{|G|}{|N_G(x_i)|}$ ,  $h_i$  divides  $|G| = p^r$ , where  $h_i > 1$ . Thus  $h_i = p^{l_i}$  for some  $l_i \geq 1$ . Thus  $|Z(G)| = p^r - h_1 - h_2 - \dots - h_r = p^r - p^{l_1} - p^{l_2} - \dots - p^{l_r}$ , where  $r \geq 1, l_i \geq 1$ . Now  $p$  divides  $|Z(G)|$  and, since  $Z(G)$  is a subgroup of  $G$ , Lagrange's 2.2.6 assures that  $|Z(G)|$  divides  $|G|$ . It follows from these two results that  $|Z(G)| = p^r > 1$ .

If  $G$  is a finite group of order  $p^r$ , where  $p$  is a prime number then  $G$  is called a  $p$ -group or a group of prime order, or prime-power group. For instance, the group  $V_4, Q_8,$

$D_8$  are 2-group of order 4, 8, 8. The equation  $|G| = |Z(G)| + \sum_{i=1}^r h_i$ , where  $h_i =$

$|G : N_G(x_i)| = [x_i]$ , is called the class equation.

Let us see how these ideas work out in the particular case of  $S_3$ . It is the smallest non-Abelian group and is, therefore, the simplest which give non-trivial example of most of the ideas that we have discussed or will discuss.

### Example 3.3.6

Let us determine the Conjugacy classes of  $S_3$ . The identity element 1 in  $S_3$  is the only element which commutes with every element of  $S_3$ , and so  $1 \in Z(S_3)$ . This implies that 1 is the only element in its Conjugacy classes. The elements  $x, xy, xy^2$  are of order 2 and the elements  $y, y^2$  are of order 3, and so, by lemma 3.3.3., they form two separate Conjugacy classes, namely  $\{x, xy, xy^2\}$  and  $\{y, y^2\}$ . Therefore the class equation will be  $|S_3| = |Z(S_3)| + h_1 + h_2$ , where  $h_1 = |\{x, xy, xy^2\}|$  and  $h_2 = |\{y, y^2\}|$ . Thus, the class equation is  $6 = 1 + 3 + 2$ . Note the  $Z(S_3)$  is trivial.

In the following, we show how the class equation can be used to determine some of the structural properties of a group.

### Theorem 3.3.7

If  $p$  is a prime number and  $G$  is a finite group of order  $p^2$ , then  $G$  is Abelian.

#### Proof

By Lagrange's Theorem,  $|Z(G)|$  divides  $|G| = p^2$ . But  $|Z(G)|$  is a prime-power, by theorem 3.3.5. Thus, either  $|Z(G)| = p$  or  $|Z(G)| = p^2$ . If  $|Z(G)| = p^2$ , then  $Z(G) = G$  and so  $G$  is Abelian on the other hand, if  $|Z(G)| = p$ , then by theorem 2.5.10,  $Z(G) \trianglelefteq G$  and we can construct  $G/Z(G)$  whose order by theorem 2.4.12, will be  $p$ . Then, by theorem 2.3.14,  $G/Z(G)$  is cyclic and hence due to theorem 2.5.11,  $G$  is Abelian.

### Example 3.3.8

The groups  $C_1, C_4, V_4, C_9$  are the Abelian groups of order 1,  $2^2$ ,  $2^2$  and  $3^2$ .

#### 4. Exercise

1. Let  $G = \langle x, y : x^2 = y^3 = (xy)^2 = 1 \rangle$  and  $H = \{1, -1\}$ . Define a homomorphism  $\phi$  between  $G$  and  $H$  and show that  $G/\text{Ker } \phi$  is isomorphic to  $H$ .
2. Define an epimorphism from  $GL(2, Z_3)$  to  $Z_3$ . Find the Kernel of this homomorphism. If  $K$  denotes the Kernel, then show that  $GL(2, Z_3)/K$  is isomorphic to  $Z_3$ .
3. If  $G$  is a group, then prove that  $G/\{1\}$  is isomorphic to  $\{1\}$  and  $G/\{1\}$  is isomorphic to  $G$ .
4. Prove that the composition of two isomorphisms is an isomorphism.

5. If  $G, H$  are groups and  $\phi : G \rightarrow H$  is a homomorphism, then prove that:
  - (i)  $(1) \phi = 1'$ , where  $1$  and  $1'$  are the identities in  $G$  and  $H$  respectively.
  - (ii)  $(x^{-1}) \phi = ((x) \phi)^{-1}$  for every  $x \in G$ .
  - (iii)  $\text{Im}(\phi) = \{y \in H : (x) \phi = y\} \leq H$ .
6. Prove that  $C_7$  and  $Z_7$  are isomorphic.
7. Let  $n$  be a positive integer. Prove that  $\phi : Z \rightarrow C_n$ , define by  $(x) \phi = e^{2\pi i x/n}$  for all  $x \in Z$ , is an epimorphism. Determine the  $\text{Ker } \phi$  and show that  $C_n$  is isomorphic to  $Z/\text{Ker } \phi$ .
8. Let  $U$  denote the circle group  $\{z \in C^x : |z| = 1\}$ . Define  $\phi : R^+ \rightarrow U$  by  $(x) \phi = e^{2\pi i x}$  for all  $x \in R^+$ . Show that  $\phi$  is an epimorphism. Determine the  $\text{Ker } \phi$  and show that  $U$  is isomorphic to  $R^+/Z^+$ .
9. Given the group  $V_4$  and  $C_3$ , find a group  $G$  such that  $V_4 \trianglelefteq G$  and  $G/V_4$  is isomorphic to  $C_3$ .
10. If  $G$  is a non-Abelian group of order 6, then prove that  $G$  is isomorphic to  $S_3$ .
11. Let  $H, K$  be normal subgroups of a group  $G$  and  $K \subseteq H$ . If  $G/H$  is cyclic and  $|H/K| = 2$ , then prove that  $G/K$  is Abelian.
12. Prove that  $\phi : R \rightarrow R^+$ , defined by  $(x)\phi = e^x$  for all  $x \in R$ , is an isomorphism from an additive group  $R$  and the multiplicative group  $R^+$ .
13. For any group  $G, H$  and  $K$ , prove that  $G \times (H \times K)$  is isomorphic to  $(G \times H) \times K$ .
14. Let  $G$  be group and  $H \trianglelefteq G, K \trianglelefteq G$ . Prove that  $\phi : G/H \cap K \rightarrow G/H \times G/H, \phi$  defined by  $(g(H \cap K)) \phi = (gH, gK)$  for all  $g(H \cap K) \in G/H \cap K$ , is a monomorphism.
15. If  $H, K$  are groups and  $J \trianglelefteq H, L \trianglelefteq K$ ; then prove that  $(J \times L) \trianglelefteq (H \times K)/(J \times L)$  is isomorphic to  $(H/J) \times (K/L)$ .
16. Prove that  $C \setminus \{10\}$  is isomorphic to  $C^+/Z^+$ .
17. Let  $n \geq 3$ . Prove that  $|D_{2n}/D'_{2n}| = 1$  if  $n$  is odd.
18. If  $V$  is a finite  $n$ -dimensional vector space over a field  $F$ , then prove that  $V$ , as Abelian group, is isomorphic to  $F \times F \times \dots \times F$ .
19. Show that  $C_3$  is isomorphic to  $Z^+/6Z^+/3Z^+/6Z^+$  and this group is isomorphic to  $Z^+/3Z^+$ .

20. Let  $C_{12} = \langle a \rangle$ ,  $M = \langle a^2 \rangle$  and  $N = \langle a^6 \rangle$ . Consider  $C_{12}/N$  and  $M/N$ . Find

$(C_{12}/N)/(M/N)$  explicitly and verify that it is isomorphic to  $C_{12}/M$ .

21. Prove that the multiplicative group  $\mathbb{R}^\times$  is isomorphic to the additive group  $\mathbb{R}^+$ .

(Define an isomorphism from  $\mathbb{R}^\times$  to  $\mathbb{R}^+$ ).

22.