1

Introduction

We observe objects in nature to have some pattern or symmetry. In fact, the symmetries inherent in any physical system play a very crucial role in the study of such systems. Group theory is a branch of mathematics that facilitates classification of these symmetries. Hence learning the group theory tools will prove useful to studying applications in physics. Readers will particularly appreciate the power and elegance of the group theoretical techniques in reproducing the experimental observations.

Before delving into its applications, it is important to understand the concept of an abstract group from a purely mathematical standpoint. In this chapter, we present the formal definition of a group and also the notations which will be followed in the rest of the book.

1.1 Definition of a Group

Definition 1. A group G is a set on which is defined a binary operation called the *product* having the following properties:

1. Closure: For all a and b in G, the product ab is in G. Here a and b need not be distinct.
2. Associativity: $(ab)c = a(bc)$ for all a, b and c in G.
3. Existence of Identity: There exists a unique e in G such that $ae = ea = a$ for all a in G. e is called the identity element of the group.
4. Existence of Inverse: For every a in G there exists a unique b in G such that $ab = ba = e$. b is called the inverse of a and is conventionally denoted by a^{-1}.

In addition to the above mentioned axioms, if it is also true that $ab = ba$ for all a and b in G, then G is said to be an *abelian group*. It must be noted that the property of being abelian is special in the sense that not all groups need be abelian. In any group, it is trivial to prove the following statements:

$$\begin{aligned} ax &= bx \Rightarrow a = b \\ xa &= xb \Rightarrow a = b \\ (ab)^{-1} &= b^{-1}a^{-1}. \end{aligned} \tag{1.1.1}$$

Due to the obvious simplicity of the definition, many familiar sets in mathematics are indeed seen to be examples of groups.

Example 1. The set of all integers Z is a group if the group product is taken to be the usual addition of integers. This group is clearly abelian and has an infinite number of elements. □

Example 2. The set of all complex numbers C is a group under addition of complex numbers. This group again is abelian and infinite. □

Example 3. The set $C - \{0\}$ is an infinite abelian group under the usual multiplication of complex numbers. □

Example 4. The set of all 2×2 matrices with complex entries is an infinite abelian group under matrix addition. □

Example 5. The set of all invertible 2×2 matrices with complex entries is an infinite *non-abelian* group under matrix multiplication. □

A group G that contains a finite number of elements is called a *finite group*. The number of elements in a finite group G is called the *order* of the group and is denoted by $|G|$. For any element a in a group and a positive integer n, a^n represents $aa...a$ where there are n factors in the product. Similarly a^{-n} represents $(a^{-1})^n$. Before looking at some examples of finite groups, the following definition may be noted.

Definition 2. A subset S of elements of a group G is said to generate G if every element of G can be expressed as a finite product of finite powers of elements (or their inverses) of S in some order. If the set S is finite then the group G is said to be *finitely generated*. The elements of the minimal set S that generates a group G are called the *generators* of the group and S itself is called the *generating set*. A group whose generating set contains a single element is said to be a *cyclic group*.

A group is completely specified if its generators are known along with all the relations that exist between them. It is important to realize that a group may have more than one generating set. In case of finite groups though, the number of elements in all possible generating sets is the same.

Table 1.1 Klein-4 Group V

V	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

Example 6. The set $\{e\}$ along with the relation $e^2 = e$ generates the trivial group $\{e\}$ called the identity group of order 1. Henceforth, this group would be represented by the symbol E. □

Example 7. The set $\{a\}$ along with the relation $a^2 = e$ generates the group $\{e, a\}$ of order 2. □

Example 8. The set $\{a\}$ along with the relation $a^n = e$ (n being a positive integer) generates the cyclic group $\{e, a, a^2, \ldots, a^{n-1}\}$ of order n. Henceforth, this group would be represented by the symbol C_n. □

Example 9. The set $\{a, b\}$ along with the relations $a^2 = b^2 = e$ and $ab = ba$ generates the abelian group $V = \{e, a, b, ab\}$. The group V is called the Klein-4 group. It is useful to depict this group in the form of a multiplication table showing all possible products of various group elements as in Table 1.1. Such a table can be drawn for all finite groups. □

Example 10. A slightly less trivial example is that of a finite group generated by the set $\{a, b\}$ where a and b satisfy the relations $a^2 = b^3 = e$ and $ab = b^2a$. The generated group $\mathfrak{S}(3) = \{e, a, b, b^2, ab, ab^2\}$ is of order 6 and is non-abelian (Table 1.2). Any product involving a finite number of a's and b's can be reduced to one of the elements of $\mathfrak{S}(3)$ by use of the relations on a and b. The notation $\mathfrak{S}(3)$ will be clarified later. □

Table 1.2 Symmetric Group $\mathfrak{S}(3)$

$\mathfrak{S}(3)$	e	a	b	b^2	ab	ab^2
e	e	a	b	b^2	ab	ab^2
a	a	e	ab	ab^2	b	b^2
b	b	ab^2	b^2	e	a	ab
b^2	b^2	ab	e	b	ab^2	a
ab	ab	b^2	ab^2	a	e	b
ab^2	ab^2	b	a	ab	b^2	e

1.2 Subgroups

Definition 3. A subset H of a group G is called a subgroup if H is a group under the product operation defined on G. The identity group E and the group G are both subsets of the group G and are called the *trivial subgroups* of G. Other subgroups of G are called *non-trivial subgroups*.

For a subset H of a group G to be a subgroup, H must satisfy all the axioms stated in the Definition 1. If H is closed under the group product and every element of H has its inverse in H, then other axioms are automatically satisfied since H is merely a subset of the group G. If G is a finite group, then the condition on H to be a subgroup of G is even simpler: H would then just have to be closed under the group product.

Given a finite group G, it is easy to find cyclic subgroups of G. For example, if a is an element of G, all positive integral powers of a are also elements of G. G being a finite group implies that there are only finitely many integral powers of a which are distinct elements of G. This could happen only if there was some minimum positive integer n for which $a^n = e$, so that further powers of a would merely be repetitions of elements in the set $H = \{e, a, \ldots, a^{n-1}\}$. But then we have generated a cyclic subgroup H of G. The order of the subgroup generated by a is also called the order of the element a. Evidently, the order of every element of a finite group is finite.

Example 11. $\mathfrak{S}(3)$ has $\{e, a\}, \{e, ab\}, \{e, ab^2\}, \{e, b, b^2\}$ as its cyclic subgroups. □

Two subsets of a group G are said to be equal if they contain the same elements. If A and B are two subsets of G, then AB is the set of all elements of G which are equal to the product of an element of A with an element of B in that order. It is worth noting that AB and BA need not be equal sets. Suppose that H is a subgroup of G. If a is any element of G, Ha denotes a subset of G containing elements of the form ha where h runs through all the elements of H. Then Ha is called a *left coset* of the subgroup H. In the same way, a *right coset* aH can be defined. From hereon, by a coset we mean a left coset. It is evident that $H = He$, and therefore H is one of the cosets of H. Every element of G belongs to some coset of H because the coset Ha definitely contains a which could be any arbitrary element of G. Thus each and every coset of H contains every possible element of G. It is possible that two distinct elements a, b of G may belong to the same coset of H. This can happen only if there is some h in H such that $ha = b$, or in other words, ab^{-1} is in H. Also, two different cosets of H are disjoint. Suppose the two cosets had a common element a, then both the cosets must be equal to the coset Ha indicating that the intersection between two different cosets must be a null set. Hence for the finite group G, all the cosets of H contain same number of elements and are disjoint whose union is equal to G. This proves the important *Lagrange's theorem* which states that the order of every subgroup H of a finite group G divides the order of G. Lagrange's theorem does not imply that a subset of a finite group is definitely a subgroup if the number of elements in the subset divides the group order.

A group G may have several subgroups of various orders. Let H be a non-trivial subgroup of G. If a is an element of G, then aHa^{-1} is a set which contains elements of form aha^{-1} for every h in H. It can be verified that aHa^{-1} is also a subgroup of G. By choosing a different a each time, we can generate all possible subgroups of the form aHa^{-1}. Such subgroups are called *conjugate subgroups*. It is possible that one may get the same subgroup for different choices of a. If it turns out that for every choice of a, $aHa^{-1} = H$, then H is said to be a *normal subgroup* or *invariant subgroup*. Normal subgroups are special in the sense that they are invariant under conjugation by all the elements of the group, i.e., if k is an element of a normal subgroup K, then for all a in G, aka^{-1} is again an element of K. Further $aKa^{-1} = K \Rightarrow aK = Ka$, i.e., the left and right cosets of a normal subgroup are identical. The trivial subgroups of G are clearly normal. If G is abelian then every subgroup of G is normal. In case G has no non-trivial normal subgroups then G is said to be a *simple group*. Groups of prime order are examples of simple groups.

Example 12. Consider the group $\mathfrak{S}(3)$. With the notation $H_a = \{e, a\}$ for the cyclic subgroup generated by a and using the relations on the generators a and b, the following can be verified

$$aH_aa^{-1} = H_a;\ (ab)H_a(ab)^{-1} = H_{ab^2};\ (ab^2)H_a(ab^2)^{-1} = H_{ab}.$$

Thus H_a, H_{ab}, H_{ab^2} are conjugate subgroups. Also, H_b can be seen to be a normal subgroup of $\mathfrak{S}(3)$ and hence $\mathfrak{S}(3)$ is not a simple group. In fact H_b is the only non-trivial normal subgroup of $\mathfrak{S}(3)$. □

The non-trivial normal subgroups of a group play an important role in the study of the group's structure. If K is a normal subgroup of the group G, then the set of cosets of K is also a group, called the *factor group* of G with K. The factor group is denoted as G/K. Let Ka and Kb be two cosets of K. Defining the product of the two cosets $(Ka)(Kb)$ to be the set that contains elements of G which are equal to the product of an element of Ka with an element of Kb in that order. Then the elements of $(Ka)(Kb)$ have the form $k_1ak_2b = k_1ak_2a^{-1}ab = k_1k_3ab = k_4\ ab$. When k_1 takes all values in K, k_4 also takes all values in K. Thus $(Ka)(Kb) = Kab$ and we have closure in the set of cosets of K under the defined product. Associativity follows from $(KaKb)Kc = KabKc = K(ab)c = Ka(bc) = KaKbc = Ka(KbKc)$. The coset K serves as the identity in G/K and $(Ka)^{-1} = Ka^{-1}$. This proves G/K is a group.

1.3 Conjugacy Classes

Suppose a is an element of a group G. The set of all elements of G which are equal to gag^{-1} for some choice of g in G is called the *conjugacy class* of the element a. The elements of a conjugacy class are said to be conjugate elements of G. Conjugate elements, even though distinct, have important common properties. One

such property is that if a and b are conjugate then both must have same order. For instance, if a has order n and $b = gag^{-1}$ for some g, then

$$b^m = \underbrace{(gag^{-1})(gag^{-1})\dots(gag^{-1})}_{m \text{ factors}} = ga^m g^{-1}. \tag{1.3.1}$$

The smallest positive integer m for which $ga^m g^{-1}$ is equal to e is clearly n. Hence b has the same order as a. The above expression also proves that if a and b are conjugate then so are their equal powers. Additionally, if a is conjugate to $b(a = gbg^{-1})$ and b is conjugate to $c(b = hch^{-1})$, then $a = ghch^{-1}g^{-1} = (gh)c(gh)^{-1}$. It follows that a is conjugate to c. The property of being conjugate is for this reason *transitive*.

The conjugate elements of G belong to the same conjugacy class. As every element of G is in its own conjugacy class $(a = eae^{-1})$, the whole group G can be divided into several conjugacy classes. It is important that two different conjugacy classes cannot have a common element. For if there was a common element, then that element would be conjugate to all the elements in both the conjugacy classes. By the transitivity property, it follows that the elements in the two classes would be conjugate and therefore must belong to the one and same class. The conjugacy classes of a group decompose the group into mutually exclusive sets. In case of an abelian group, the conjugacy classes consist of the individual group elements.

Example 13. Consider $\mathfrak{S}(3)$. Since $geg^{-1} = e$ for all g in $\mathfrak{S}(3)$, $\{e\}$ forms a conjugacy class. Also $bab^{-1} = bab^2 = ab^4 = ab$ and $(b^2)a(b^2)^{-1} = b^2ab = b^4a = ba = ab^2$, thus $\{a,\ ab,\ ab^2\}$ is a conjugacy class. $aba^{-1} = aba = b^2 \cdot a^2 = b^2$, and it follows $\{b,\ b^2\}$ is a conjugacy class. We note finally that

$$\mathfrak{S}(3) = \{e\} \cup \{a,\ ab,\ ab^2\} \cup \{b,\ b^2\}. \qquad \square$$

1.4 Further Examples of Groups

Two important groups are considered here in light of the concepts introduced in previous sections. They are namely: the *Quaternion Group* and the *Dihedral Group*. The quaternion group is a group structure on algebraic entities called *quaternions*. Quaternions were first considered in connection to classical mechanics. They have deep significance as regards mathematical constructs in various physical theories. We do not intend to explore this significance, but we would like to understand what quaternions are in principle. The dihedral group is of importance in the study of symmetries of a regular polygon. We will often encounter the dihedral group in later chapters.

The Quaternion Group Q

The quaternion group Q has 8 elements. Explicitly, the group $Q = \{e, s, i, j, k, si, sj, sk\}$. Various elements satisfy the relationships

$$s^2 = e; i^2 = j^2 = k^2 = ijk = s.$$

The symbols $i,\ j,\ k$ can be regarded as imaginary units, e as the real unit and s as negative e. The defining relations specify the group completely. The relation $i^2 = ijk$ implies $i = jk$. Likewise, $j = ki$ and $k = ij$. One may note the cyclic nature of these equalities. Furthermore, $i^2 = j^2 \Rightarrow (ji)(ij) = e$. Because $ij = k$ and $(sk)k = e$, it follows $ij = sji$. Likewise, $jk = skj$ and $ki = sik$. The identity element e obviously commutes with all the elements of Q, but so does the element s. For example, $i = jk \Rightarrow si = sjk$ and $ijk = s \Rightarrow sjk = is$. It follows that $si = is$. In a similar fashion it may be shown s commutes with j and k and hence with all the elements of Q. To sum up, we may note the relations that follow from the defining relationships.

$$\begin{aligned} i = jk, &\quad j = ki, &\quad k = ij, \\ ij = sji, &\quad jk = skj, &\quad ki = sik, \\ si = is, &\quad sj = js, &\quad sk = ks. \end{aligned}$$

The non-trivial subgroups of Q can be of order 2 or 4. The subgroup of order 2 is $\{e,\ s\}$. The three subgroups of order 4 are $\{e,\ s,\ i,\ si\}$, $\{e,\ s,\ j,\ sj\}$ and $\{e,\ s,\ k,\ sk\}$. Each of the order-4 subgroups is isomorphic to the cyclic group C_4. It can be verified that all the subgroups of Q are normal in Q. The conjugacy classes of Q can be found from the relationships given above. Since e and s commute with all the elements, they are the only elements in their respective classes. Since $jij^{-1} = sijj^{-1} = si$, it follows i and si are conjugate. Similarly, j and sj are conjugate, and also k and sk are conjugate. The decomposition of Q in conjugacy classes is.

$$Q = \{e\} \cup \{s\} \cup \{i,\ si\} \cup \{j,\ sj\} \cup \{k,\ sk\}.$$

The Dihedral Group $D_n (n \geq 3)$

The dihedral group D_n has $2n$ elements. It can be generated by the symbols r and s satisfying the relationships as under

$$r^n = s^2 = e,\ sr = r^{-1}s.$$

Explicitly, $D_n = \{e,\ s,\ r,\ r^2,\ \ldots r^{n-1},\ sr,\ sr^2,\ \ldots sr^{n-1}\}$. Any product of a finite number of r's and s's can be reduced to one of the group elements using the defining relationships. Consider

$$r^k s = \underbrace{rr\ldots r}_{k \text{ factors}} \quad s = \underbrace{rr\ldots r}_{k-1 \text{ factors}} \quad sr^{-1} = sr^{-k} = sr^{n-k},$$

and likewise in other cases. The subgroup $\{e,\ s\}$ is the smallest non-trivial subgroup. The cyclic subgroup generated by r, $\{e,\ r,\ r^2,\ \ldots r^{n-1}\}$ is a normal subgroup of D_n. If a

positive integer k is a divisor of n then r^k will generate a cyclic subgroup of D_n. In order to calculate the conjugacy classes, the following relationships are useful:

$$sr^k s = r^{-k},$$
$$r^{-k} s r^k = s r^{2k},$$
$$(sr^t) r^k (sr^t)^{-1} = s r^t r^k r^{-t} s = r^{-k}.$$

In the case when n is $2p+1$, there are $p+2$ classes. The decomposition of D_{2p+1} into classes is

$$D_{2p+1} = \{e\} \cup \underbrace{\{r, r^{2p}\} \cup \{r^2, r^{2p-1}\} \cup \ldots \{r^p, r^{p+1}\} \cup}_{p \text{ classes}} \cup \{s, sr, sr^2, \ldots sr^{2p}\}. \tag{1.4.1}$$

In the case when n is $2p$, there are $p+3$ classes. The decomposition of D_{2p} is seen to be

$$D_{2p} = \{e\} \cup \{r^p\} \cup \underbrace{\{r, r^{2p-1}\} \cup \ldots \{r^{p-1}, r^{p+1}\} \cup}_{p-1 \text{ classes}} \cup \{s, sr^2, \ldots sr^{2p-2}\} \cup \{sr, sr^3, \ldots sr^{2p-1}\}. \tag{1.4.2}$$

1.5 Homomorphism of Groups

A *homomorphism* between two groups is a function from one to the other that preserves products. More specifically, a function φ from a group G to a group T is a homomorphism if for all $a,\ b$ in G

$$\varphi(ab) = \varphi(a)\varphi(b). \tag{1.5.1}$$

Here the notation $\varphi(a)$ stands for the member of T which is the image of a under the function φ. If a and b are both chosen to be identity element e of G then $\varphi(e) = [\varphi(e)]^2$ and it follows that the identity of G is mapped to the identity of T. Also, if $b = a^{-1}$, then $\varphi(e) = \varphi(a)\varphi(a^{-1})$ and it follows that $\varphi(a^{-1}) = [\varphi(a)]^{-1}$. In other words, under a homomorphism, identity is mapped to identity and inverse is mapped to inverse. The subset K of G which contains all the elements which are mapped to the identity of T is called the *kernel* of the homomorphism φ. It can be shown that the kernel K is a normal subgroup of G. In fact all the normal subgroups of G would cause a homomorphism of G into some group. It can be also shown that all elements of a coset of K are mapped to the same element of T.

Example 14. Let $C_2 = \{E,\ A\}$ where C_2 is the cyclic group of order 2 in our notation and E here is the identity element of C_2. Consider a function φ from $\mathfrak{S}(3)$ to C_2 defined as

$$\varphi(e) = \varphi(b) = \varphi(b^2) = E,$$

$$\varphi(a) = \varphi(ab) = \varphi(ab^2) = A.$$

Then φ is a homomorphism. The kernel of this homomorphism is the normal subgroup H_b. □

When the kernel of a homomorphism is simply the trivial group E, then the homomorphism is one to one. In this case the two groups are said to be *isomorphic*. Isomorphic groups are essentially the same group and differ merely in the manner of labelling of their elements. In the study of *point groups*, it will be seen that some of them are isomorphic groups. In case of the group $\mathfrak{S}(3)$, the factor group $\mathfrak{S}(3)/H_b$ is isomorphic to the group C_2. In notation,

$$C_2 \cong \mathfrak{S}(3)/H_b. \tag{1.5.2}$$

Suppose now that φ_1 is a homomorphism from G_0 into G_1 and that φ_2 is a homomorphism from G_1 into G_2. It is then possible to compose φ_1 and φ_2 together to give a homomorphism ψ from G_0 into G_2. For $a \in G_0$, define ψ so that

$$\psi(a) = \varphi_2(\varphi_1(a)).$$

It is easy to show that with the above definition, ψ is a homomorphism from G_0 into G_2.

1.6 The Symmetric Group

Consider a set of n distinct letters $\{1, 2, \ldots n\}$ arranged in that order. Any rearrangement of this set of elements is called a *permutation*. For example, if $n = 3$, then all the permutations are

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; \quad \pi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}; \quad \pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\pi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}; \quad \pi_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

A permutation that leaves the positions of all the letters unchanged is called the identity permutation. In the example above, π_1 is the identity permutation. Remember that the exchange amongst columns in the above elements denote the same permutation operation. That is,

$$\pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

A product operation may be defined in the set of permutations so that the product of two permutations is another permutation. The operation of forming the product of two permutations can be most easily understood by considering the concrete case of $n = 3$. Consider the product $\pi_2\pi_5$. π_2 takes 1 to 2 and π_5 takes 2 to 3, thus $\pi_2\pi_5$ takes 1 to 3. In this manner the action of $\pi_2\pi_5$ can be ascertained on all the letters

$$\pi_2\pi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 2 & 1 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \pi_4,$$

$$\pi_5\pi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 & 1 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \pi_3.$$

Similarly, one may verify that the product so defined is associative. Also $(\pi_2)^{-1} = \pi_2$, $(\pi_3)^{-1} = \pi_3$, $(\pi_4)^{-1} = \pi_4$, $(\pi_5)^{-1} = (\pi_5)^2 = \pi_6$, $(\pi_6)^{-1} = (\pi_6)^2 = \pi_5$. Thus the set of permutations on three letters is a group. In fact, this is the same group as $\mathfrak{S}(3)$ if we identify π_1 with e, π_2 with a, π_5 with b, π_6 with b^2, π_4 with ab and π_3 with ab^2. Since $\mathfrak{S}(3)$ is the group of all permutations on 3 letters, it is called the *symmetric group* of degree 3. In the general case of permutations on n letters, $\mathfrak{S}(n)$ is called the symmetric group of degree n. The order of $\mathfrak{S}(n)$ is $n!$, the total number of permutations of n letters. Subgroups of $\mathfrak{S}(n)$ are called *permutation groups*. The very important *Cayley's Theorem* states that every group is isomorphic to a permutation group which is embedded in some symmetric group. In particular, if G is a group of order n, then it is isomorphic to a subgroup of $\mathfrak{S}(n)$. In order to see this, label the elements of G so that $G = \{g_1(= e), g_2, \ldots g_n\}$. Let g be some element of G. If every element of G is multiplied with g from right, then we have a permutation π_g induced on the letters $\{g_1, g_2, \ldots g_n\}$ which can be written as

$$\pi_g = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1g & g_2g & \cdots & g_ng \end{pmatrix}.$$

Another element h of G induces a permutation π_h so that the product $\pi_g\pi_h$ is given by

$$\pi_g\pi_h = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1g & g_2g & \cdots & g_ng \end{pmatrix}\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1h & g_2h & \cdots & g_nh \end{pmatrix}$$

$$\Rightarrow \quad \pi_g\pi_h = \begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ g_1gh & g_2gh & \cdots & g_ngh \end{pmatrix}$$

$$\Rightarrow \quad \pi_g\pi_h = \pi_{gh}.$$

This proves that the mapping $g \to \pi_g$ is a homomorphism (Equation 1.5.1). Because two distinct elements of G induce distinct permutations, it follows that the group G and the set of permutations $\{\pi_{g_1}, \pi_{g_2}, \ldots \pi_{g_n}\}$ are isomorphic. This proves the Cayley's Theorem for finite groups.