CHAPTER 6

LINEAR SPACES

[*This chapter is based on the lectures of Professor K.S.S. Nambooripad, Director-in-Charge, Centre for Mathematical Sciences, Trivandrum Campus. Since this publication is only a preprint the author is free to publish the material elsewhere.*]

In this section we collect a few general definitions and results about vector spaces over arbitrary fields for convenience of later reference and to set up notations. We assume that the reader is familiar with the basic concepts like groups, rings, fields, vector spaces etc. For details, the reader may refer to books such as Herstein (1975), Artin (1990) etc., on algebra in general and Halmos (1958), Hoffman and Kunze (1971) for linear algebra in particular.

6.1. Algebraic Preliminaries

Here we shall briefly discuss those algebraic concepts needed for our discussion of linear algebra and symmetries. For a more extensive discussion of these the reader may consult Artin (1990).

6.1.1. Preliminary definitions

We assume that the reader is familiar with elementary set theory, number systems and their basic properties. We shall use the following notations to denote various number systems:

$$\begin{aligned}
&\mathbb{R} = \text{Real number system;}\\
&\mathbb{C} = \text{Complex number system;}\\
&\mathbb{Q} = \text{Rational number system;}\\
&\mathbb{Z} = \text{System of integers;} \qquad \text{and}\\
&\mathbb{N} = \{0, 1, \dots\} = \text{Set of natural numbers.}
\end{aligned} \tag{6.1.1}$$

If $\Bbbk$ is any one of the system of numbers then we shall write $\Bbbk^*$ for the set of non-zero numbers in $\Bbbk$:

$$\Bbbk^* = \Bbbk - \{0\}. \tag{6.1.2}$$

We also assume that the reader is familiar with elementary coordinate geometry (of plane and space) and matrix theory, we may use some of these for illustrative purposes in this chapter.

Recall Herstein (1975) that a function (mapping) $f : X \to Y$ from the set X to the set Y is a subset of the Cartesian product $X \times Y = \{(x, y) : x \in X,\ y \in Y\}$ such that

F1: if $(x, y), (x, y') \in f$ implies $y = y'$; and

F2: for all $x \in X$ there is some $y \in Y$ with $(x, y) \in f$.

It follows that for each $x \in X$ there is a unique $y \in Y$ with $(x, y) \in f$. The set X [Y] is called the *domain* [*codomain*] of f and is denoted by $\operatorname{dom} f$ [$\operatorname{cod} f$]. As in Herstein (1975) we shall adopt the "left-right" composition rule for functions. Thus if $f : X \to Y$ and $g : Y \to Z$ are functions the composite of these functions is written as $f \circ g$ or simply fg. The function fg acts on X as follows: for any $x \in X$ the value $x(fg)$ of fg at x is written so that the left function f acts first on the argument x. In this situation, it will be more natural to write the argument on the left (see, for example, Herstein (1975)) often without parenthesis. Thus for any $x \in X$, the value $x(fg)$ of fg at x is given by

$$x(fg) = (xf)g. \tag{6.1.3}$$

We refer to the composition order adopted here as *figure order* since it is possible to represent it as the following diagram:

$$\begin{tikzcd} & Z \\ X \arrow[r, "f"'] \arrow[ur, "fg"] & Y \arrow[u, "g"'] \end{tikzcd} \qquad \begin{tikzcd} x(fg) \arrow[r, equal] & (xf)g \\ x \arrow[u, mapsto] \arrow[r, mapsto] & xf \arrow[u, mapsto] \end{tikzcd} \tag{D.g}$$

However, there are situations where, for various reasons, it may be necessary or convenient to write the functional argument on the right. We shall use the same composition rule even in this case:

$$(fg)(x) = g\,(f(x))\,. \tag{6.1.4}$$

It is clear that the functions f and g are *composable*, (that is, the composite function fg exists) if and only if $\operatorname{cod} f = \operatorname{dom} g$.

Remark 6.1.1: The composition rule used in many books is "right-left"; that is, the rule given by $(g \circ f)(x) = g(f(x))$ (see for example Artin (1990)).

Let X be a set. A function $F : X \times X \to X$ from the Cartesian product $X \times X = \{(x, x') : x, x' \in X\}$ to X is called a *binary operation* (or a *binary composition*) in X.

The most important and familiar examples of binary operations are basic arithmetic operations on numbers: the addition + and multiplication ×. To indicate an abstract binary composition on a set X, we usually employ notations resembling multiplication or addition. For $x, y \in X$, we use one of the following to indicate the composite z of x and y under the given operation:

$$xy, \quad x \times y, \quad x \cdot y \quad x \circ y \quad x * y, \quad x + y, \ldots$$

and so on. Also, depending on the notation used, the element z will be called *composite, product*, *sum*, etc.

Important properties of a binary composition that we shall be concerned with here are the following. For simplicity, the composite is indicated by juxtaposition (which is multiplicative notation). The binary composition is said to be *associative* if

$$(xy)z = x(yz) \quad (\textit{Associative law}) \tag{6.1.5}$$

holds for all $x, y, z \in X$ and *commutative* if

$$xy = yx \qquad (\textit{Commutative law}) \tag{6.1.6}$$

for all $x, y \in X$. A set with an associative binary operation is called a *semigroup*. In addition, we shall also be interested in the existence or otherwise of certain special elements. An element $e \in X$ satisfying the following conditions

$$ex = xe = x \quad (\textit{Identity}) \tag{6.1.7}$$

for all $x \in X$ is called *identity* of X with respect to the given composition (or simply, identity of X if the composition is clear from the context). It is clear that there can be utmost one identity in X. Similarly, $z \in X$ satisfying the following

$$zx = xz = z \quad (\textit{Zero}) \tag{6.1.8}$$

is called the *zero* of X which, if exists, is also unique. Let e be identity for F. An element $x' \in X$ is an *inverse* of x if

$$xx' = x'x = e \quad (\textit{Inverse of } x) \tag{6.1.9}$$

A semigroup having identity is called a *monoid*.

Note that the equations above will look different if the notation for the composition is changed. For example, using additive notation, the identity law becomes

$$e + x = x + e = x.$$

As a convention, we use 1 and 0 for identity and zero along with multiplicative notation. Inverse of x is denoted by x^{-1}. In the additive notation, identity is denoted by 0 and inverse of x is denoted by $-x$. Thus, in additive notation, Equation (6.1.9) becomes

$$x - x = -x + x = 0.$$

Notice that we have written $x - y$ for $x + (-y)$.

Apart from basic arithmetic operations on numbers, there are two examples of binary compositions that are important in the sequel. These are multiplication of $n \times n$ matrices which will be discussed later in greater detail and the composition of functions on sets. If f and g are functions from X to X, then

$$\operatorname{dom} f = \operatorname{cod} f = \operatorname{dom} g = \operatorname{cod} g = X$$

and so, the composite fg always exist. Thus, if T_X denote the set of all functions from a set X to itself, the composition is a binary operation in T_X (see Exercise 6.2 also).

6.2. Groups

Definition 6.2.1. A group is a pair $(G, \cdot)$ where G is a set and $\cdot$ is a binary operation on G satisfying the following:

G The composition $\cdot$ is associative.

G Identity e exists in G.

G Every $a \in G$ has inverse in G.

The group $(G, \cdot)$ is said to be *abelian* or that G is commutative if

G The composition $\cdot$ is commutative.

To simplify notation, we shall write G, H, etc; for groups and juxtaposition for composition if there is no ambiguity. Identities will be denoted by e, e', etc (or e_G, e_H, etc. if necessary). While multiplicative notation is used generally for both abelian and nonabelian groups, additive notation is seldom used to represent non-abelian groups; in fact abelian groups using additive notation are some times referred to as *additive groups*. This means, in particular, that the identity of an additive group A is denoted by 0 and inverse of $x \in A$ is denoted by $-x$.

Apart from groups of numbers and related systems (see Exercise 6.3 and Exercise 6.8) two most important classes of examples of groups are the following:

Example 6.2.1. Let $GL_n(\mathbb{R})$ denote the set of all non-singular $n \times n$ real matrices. This is a group under matrix multiplication and is called the real *general linear group* of degree n. Similarly, sets of $n \times n$ non-singular complex or rational matrices (denoted respectively by $GL_n(\mathbb{C})$ or $GL_n(\mathbb{Q})$) are also groups under multiplication and are called complex or rational general linear groups of degree n respectively. We will discuss these examples in more detail later.

Example 6.2.2. A bijection $\rho : X \to X$ of a set onto itself will be called a permutation acting on X. ρ is called a finite permutation if X is a finite set. When X is finite, the degree of ρ is defined as the cardinal number of X. The set of all permutations of a set X can be shown to be a group which we denote by $S(X)$. $S(X)$ is called the *symmetric group* on X. Note that symmetric groups $S(X)$ and $S(Y)$ are isomorphic if the cardinal numbers of X and Y are the same (see Exercise 6.4). If X is finite and if $S(X)$ and $S(Y)$ are isomorphic, then X and Y has the same number of elements. If $n \in \mathbb{N}^*$ we denote by S_n the abstract group isomorphic to $S(X)$ for any set X with $|X| = n$. S_n will be called the symmetric group of *degree n*. Cayley's theorem below (Theorem **??**) indicate the importance of symmetric groups in the algebraic theory of groups.

The *order* of a group G, denoted by $o(G)$, is the cardinal number $|G|$ of the set G. This concept is useful in the case where the order is finite. Groups of finite order (or finite groups) are very important in a number of applications.

Definition 6.2.2. (Subgroups). A subset H of a group G is called a *subgroup* if the following holds.

For all $a, b \in H$, $ab \in H$.

If $a \in H$ then $\bar{a}^1 \in H$.

Notice that the statement Sg1 implies that the binary composition of G restricted to H is a binary composition in H and the statement Sg2 then shows that H is a group with respect to the restriction of the composition of G to H. These conditions are independent in the sense that there are subsets of groups for which one of the statement holds but not the other. For, the subset $\mathbb{N}$ of $\mathbb{Z}$ is closed with respect to addition of integers but does not satisfy Sg2. Similarly the subset S^1 of all complex numbers of absolute value 1 is not closed for addition but is closed for taking additive inverses. The two conditions above can be combined as follows: $H \subseteq G$ is a subgroup of G if and only if

$*\quad ab^{-1} \in H$ for all $a, b \in H$.

Subgroups of general linear groups are called matrix groups and subgroups of symmetric groups are called permutation groups.

Let $\{H_i : i \in I\}$ be any family of subgroups of a group G. Suppose that

$$H = \wedge\{H_i : i \in I\} \quad \text{and} \quad K = \vee\{H_i : i \in I\}.$$

denote respectively the largest subgroup of G contained in every H_i (glb with respect to inclusion) and the smallest subgroup of G containing H_i for every $i \in I$ (lub). Then H exists since $\bigcap\{H_i : i \in I\} = H$. It can be shown without difficulty that K also exists. Thus the set $\boldsymbol{Sg}(G)$ of all subgroups of G is a partially ordered set (under inclusion) with the property that any subset of $\boldsymbol{Sg}(G)$ has both glb and lub with respect to inclusion. If e is the identity of G, $\{e\}$ is clearly the smallest subgroup of G; G itself is the largest subgroup. Thus $\boldsymbol{Sg}(G)$ is *complete lattice* under inclusion. A subgroup H of G is said to be *non-trivial* if $H \neq \{e\}$ and H is *proper* if $H \neq G$.

Let H be a subgroup of a group G. For $a \in G$, the sets

$$Ha = \{ha : h \in H\} \quad \text{and} \quad aH = \{ak : k \in H\} \tag{6.2.1}$$

are called the right and left coset of H by a. It is clear that every statement regarding right cosets there is a corresponding statement about left cosets which can be formulated and proved routinely.

Recall that a partition of a set X is a family of pairwise disjoint subsets whose union is X.

Proposition 6.2.1. *Let H be a subgroup of a group G. Any two right cosets of H have the same cardinality and the set*

$$H \wr G = \{Ha : a \in G\}$$

all right cosets of H is a partition of G. Similarly, any two left cosets have the same cardinality and the set

$$G \wr H = \{aH : a \in G\}$$

all left cosets of H is a partition of G. Finally the map

$$\phi : Ha \mapsto a^{-1}H$$

is a bijection of $H \wr G$ onto $G \wr H$.

Proof. To prove the first statement, it is sufficient to show that the map

$$\rho : H \to Ha; h \mapsto ha \quad \text{has inverse} \quad \sigma : Ha \to H; k \mapsto ka^{-1}.$$

This is clear.

Since $a \in Ha$, clearly $\cup_{a \in G} Ha = G$. If $u \in Ha \cap Hb$, then $u = ha = h'b$ for $h, h' \in H$. Hence $a = h^{-1}hb \in Hb$ and so, $Ha \subseteq Hb$. Similarly, $Hb \subseteq Ha$. Thus $Ha = Hb$ if $Ha \cap Hb \neq \emptyset$. Therefore $H \wr G$ is a partition of G. The statement regarding the partition by left cosets is proved similarly.

Now let $(Ha)\phi = a^{-1}H$. This is single-valued map of $H \wr G$ to $G \wr H$. For

$$\begin{aligned} Ha = Hb &\Longrightarrow ha = b \quad \text{for some } h \in H \\ &\Longrightarrow a^{-1}h^{-1} = b^{-1} \Longrightarrow a^{-1}H = b^{-1}H \\ &\Longrightarrow (Ha)\phi = (Hb)\phi. \end{aligned}$$

Moreover, ϕ is one-to-one: if

$$(Ha)\phi = (Hb)\phi \quad \text{then} \quad a^{-1}H = b^{-1}H.$$

This implies that for some $h \in H$

$$a^{-1}h = b^{-1} \Longrightarrow h^{-1}a = b \Longrightarrow Ha = Hb.$$

ϕ is subjective since $(Ha^{-1})\phi = aH$ for any $aH \in G \wr H$. Hence ϕ is a bijection.

The result above shows that the number of sets in the partition of G by right and left cosets of a subgroup H are the same. This common number is called the *index* of H in G and is denoted by $[G : H]$:

$$[G : H] = |H \wr G| = |G \wr H|. \tag{6.2.2}$$

In particular, let H be a subgroup of the finite group G with $o(G) = n$. Then H is also a finite group; let $o(H) = m$. If $k = [G : H]$ then k is the number of (right) cosets of H in G and by the Proposition above, each coset contains exactly m elements. Therefore G has km elements. Thus

$$o(G) = o(H)[G : H] \tag{6.2.3}$$

Hence we have:

Theorem 6.2.1. (Lagranges theorem). *The order of a subgroup divides the order of a finite group.*

If H is an arbitrary subgroup of the group G, then a right coset Ha of H need not be a left coset of H (see Exercise 6.10). Therefore, the partitions $H \wr G$ and $G \wr H$ may be different.

Proposition 6.2.2. *The following conditions are equivalent for a subgroup H of a group G.*

> $\bar{a}^{1}Ha = H$ *for all* $a \in G$.
>
> *Every left coset of H is a right coset of H.*
>
> $H \wr G = G \wr H$.

Proof. Statements 2 and 3 are clearly equivalent. If (1) holds and $a \in G$, then $aH = a(a^{-1}Ha) = Ha$ and so (2) holds. Suppose that (3) holds. Then for any $a \in G$, $aH = Hb$ for some $b \in G$. Then there is $h \in H$ such that $b = ha$ and so $Hb = (Hh)a = Ha$. Hence $aH = Ha$ which gives (1).

A subgroup $N \subseteq G$ satisfying the equivalent conditions of the (Proposition 6.2.2.) above is called a *normal subgroup* of G. Notice that every subgroup of an abelian group is normal.

Definition 6.2.3. A mapping $\phi : G \to H$ from a group G to a group H is called a *homomorphism* if

$$(ab)\phi = (a\phi)(b\phi) \quad \text{for all} \quad a, b \in G.$$

A homomorphism $\phi : G \to G$ is called an *endomorphism*. The set of all endomorphisms of G is denoted by $\mathrm{End}(G)$. A homomorphism $\phi : G \to H$ is an *isomorphism* if there is a group homomorphism $\psi : H \to G$ such that $\phi \circ \psi = 1_G$ and $\psi \circ \phi = 1_H$. An isomorphism of G to itself is called an *automorphism* and the set of all automorphisms of G is denoted by $\mathrm{aut}(G)$.

For any group G, the set $\mathrm{End}(G)$ of all endomorphisms of G is clearly a semigroup under composition (a subsemigroup of T_G) and $\mathrm{aut}(G)$ is a subgroup of $\mathrm{End}(G)$. It can be seen that $\phi : G \to H$ is an isomorphism of groups if and only if ϕ is a bijection. The definition above clearly implies that an isomorphism is a bijection (since $\psi = \phi^{-1}$). On the other hand, if $\phi : G \to H$ is a bijective homomorphism, then $\psi = \phi^{-1} : H \to G$ is a bijection and it is easy to see that ψ must also be a homomorphism.

Proposition 6.2.3. *Let $\phi : G \to H$ be a homomorphism of groups. Then we have the following:*

$\operatorname{Im}\phi = \{g\phi : g \in G\} = G\phi$ *is a subgroup of* H*;*

$\ker\phi = \{g \in G : g\phi = e'\} = e'\phi^{-1}$*, where* $e' = e_H$ *denote the identity in* H*, is a normal subgroup of* G*.*

In particular, ϕ *is surjective if and only if* $\operatorname{Im}\phi = H$ *and injective if and only if* $\ker\phi = \{e\}$*, the trivial subgroup of* G*.*

Proof. The statement (1) and the fact that $K = \ker\phi$ is a subgroup are easy to verify. To show that K is normal, let $a \in G$. Then for any $k \in K$,

$$\begin{aligned}(a^{-1}ka)\phi &= (a^{-1})\phi(k)\phi(a)\phi \\ &= (a^{-1})\phi e'(a)\phi = (a\phi)^{-1}(a\phi) = e'.\end{aligned}$$

Hence $a^{-1}Ka \subseteq K$ for all $a \in G$. But

$$a^{-1}Ka \subseteq K \Longrightarrow K \subseteq aKa^{-1}$$

for all $a \in G$. Hence $a^{-1}Ka = K$ for all $a \in G$ and so K is normal by Proposition 6.2.2.

Again it is clear that ϕ is surjective if and only if $\operatorname{Im}\phi = H$. Now $a\phi = b\phi$ if and only if $k\phi = e'$ where $k = ab^{-1}$. Hence $a = b$ if and only if $k = 1$. Therefore ϕ is one-to-one if and only if $K = \{e\}$.

The result above shows that kernels of homomorphisms are normal subgroups. Conversely, every normal subgroup is the kernel of a suitable homomorphism. If N is a normal subgroup of a group G, by Proposition 6.2.2, we have $N \wr G = G \wr N$; the unique partition of G determined by N is denoted by G/N. If X and Y are subsets of a group G, we shall write XY for the set

$$XY = \{xy : x \in X,\ y \in Y\}.$$

If one of them is a singleton, say $Y = \{y\}$, then we write Xy for XY. Similarly $xY = \{x\}Y$.

Theorem 6.2.2. (First homomorphism theorem). *Let* N *be a normal subgroup of a group* G *and let*

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

For $Na, Nb \in G/N$*, define*

$$(Na)\cdot(Nb) = Nab.$$

This defines a single-valued binary operation $\cdot$ on G/N and G/N is a group with respect to $\cdot$ such that the quotient map

$$q_N : a \mapsto Na; \quad \textit{is a homomorphism of } G \textit{ onto } G/N \textit{ with} \quad \ker q_N = N.$$

Moreover if $\phi : G \to H$ is any homomorphism, there is an injective homomorphism $\psi_\phi : G/\ker\phi \to H$ such that we have the following commutative diagram:

$$\begin{tikzcd} & H \\ G \arrow[ur, "\phi"] \arrow[r, "q_{\ker\phi}"'] & G/\ker\phi \arrow[u, "\psi_\phi"'] \end{tikzcd}$$

ψ_ϕ is an isomorphism [$q_{\ker\phi}$ is an isomorphism] if and only if ϕ is surjective [injective].

Proof. To show that $\cdot$ is a well-defined binary operation, let $Na, Nb \in G/N$. Now $Na = Na'$ if and only if $a' \in Na$; that is, $a' = na$ for some $n \in N$. Hence, if $a' \in Na$ and $b' \in Nb$, we have

$$\begin{aligned} a'b' &= (na)(n'b) && \text{for some } n, n' \in N; \\ &= n(an'a^{-1})ab \in Nab \end{aligned}$$

since $n(an'a^{-1}) \in N$ by Proposition 6.2.2. Hence $Nab = Na'b'$ and so $\cdot$ is single valued. It is trivial to verify that G/N is a group with respect to this composition having identity N and such that inverse of Na is Na^{-1}. Since G/N is a partition of G, the equation $aq_N = Na$ defines a mapping of G onto G/N. If $a, b \in G$, by the definition of $\cdot$, we have

$$(aq_N) \cdot (bq_N) = (Na) \cdot (Nb) = Nab = (ab)q_N$$

which shows that $q_N : G \to G/N$ is a homomorphism. Clearly, $aq_n = N$ if and only if $a \in N$ and so, $\ker q_N = N$. Suppose that $\phi : G \to H$ is a homomorphism and let $K = \ker\phi$. Define $\psi = \psi_\phi : G/K \to H$ by

$$(Ka)\psi = a\phi. \qquad \text{(eq:}\psi\text{)}$$

If $Na = Nb$, then $ab^{-1} = k' \in K$ and so $k'\phi = e'$. Hence $a\phi = b\phi$ which shows that ψ is well defined. For $Ka, Kb \in G/K$, we have

$$(Ka)\psi(Kb)\psi = (a\phi)(b\phi) = (ab)\phi = (Kab)\psi$$

and so, ψ is a homomorphism. Also $Ka \in \ker\psi$ if and only if

$$(Ka)\psi = a\phi = e' \implies a \in K \implies Ka = K.$$

Therefore, by proposition 6.2.3, ψ is injective. The definition of ψ clearly shows that ψ is surjective, and hence an isomorphism, if and only if ϕ is surjective. Now, if $\ker\phi = N$, $\ker q_N = \ker\phi = N$ and so, q_N is injective if and only if ϕ is injective. $q_{\ker\phi}$ is always surjective and so, q_N is an isomorphism if and only if ϕ is injective.

If a is an element of a group G it is easily seen that the mapping

$$\phi : \mathbb{Z} \to G; \quad n \mapsto a^n \tag{6.2.4}$$

is a homomorphism of the additive group $\mathbb{Z}$ of integers into G. Hence by Proposition 6.2.3

$$\operatorname{Im}\phi = \langle a \rangle = \{a^n : n \in \mathbb{Z}\} \quad \text{and} \quad \ker\phi = \{n \in \mathbb{Z} : a^n = 1\} \tag{6.2.5}$$

are subgroups of G and $\mathbb{Z}$ respectively. By Exercise 6.8, either $\ker\phi = 0$ (the trivial subgroup of $\mathbb{Z}$) or $\ker\phi = n\mathbb{Z}$ for some $n \in \mathbb{N}$. In the first case, ϕ is an isomorphism of $\mathbb{Z}$ onto $\langle a \rangle$ and so $\langle a \rangle$ is infinite. In the other case, by Theorem **??**, $\langle a \rangle$ is isomorphic to the quotient group $\mathbb{Z}/n\mathbb{Z}$ which is of order n (see Exercise 6.8). We have the following:

Corollary 6.2.1. Let a be an element of a group G. Then the mapping $\phi_a = \phi$ defined by Equation (**??**) is homomorphism of $\mathbb{Z}$ into G. ϕ_a is either an isomorphism of $\mathbb{Z}$ onto $\langle a \rangle$ or

$$\operatorname{Im}\phi_a = \langle a \rangle \simeq \mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}.$$

Consequently, for any $a \in G$, the subgroup $\langle a \rangle$ of G is either finite or countable.

We define, the *order* of an element a in the group G as the order of the subgroup $\langle a \rangle$. We denote the order of a by $o(a)$. It follows from the corollary above that the order of any element a in a group G is either finite or countable. Further, the definition of $\langle a \rangle$ shows that when a has finite order, the order of a is the smallest positive integer $n \geq 1$ such that $a^n = 1$.

Note that every group G has a unique element of order 1; viz, the identity of G. In some groups such as the additive group of real numbers, this may be the only element of finite order. On the other hand, the group $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ of all complex numbers of absolute value 1 contains infinitely many elements of finite order. In fact, the set

$$\Omega = \{\omega \in \mathbb{C} : \omega^n = 1 \quad \text{for some} \quad n \in \mathbb{N}\}$$

of all roots of unity is an infinite subgroup of S^1 in which every element is of finite order.

6.3. Products of Groups

There are several methods of generating new groups from given groups. The process of taking subgroups and quotient groups can yield new groups in this way. Construction of direct products of groups is another useful method by which new groups can be constructed from a given family of groups.

Let $\mathcal{X} = \{X_\lambda : \Lambda\}$ be a family of sets. Recall that, by definition, the Cartesian product $\prod_{\lambda\in\Lambda} X_\lambda$ of $\mathcal{X}$ is the set of all functions

$$x : \Lambda \to \cup_\Lambda \{X_\lambda\} \quad \text{such that} \quad (\lambda)x = x_\lambda \in X_\lambda.$$

We will refer to such functions as *choice functions* (briefly *c-functions*) for the family $\mathcal{X}$ or Λ-*tuples*. If x is a c-function, then the value x_λ of x at $\lambda \in \Lambda$ is called the component of x at λ. Notice that this is consistent with the usual definition of n-tuples (when Λ is the set $\{1, \ldots, n\}$). Moreover, the Cartesian product of the family $\mathcal{X}$ is non-empty if and only if every set in $\mathcal{X}$ is non-empty.

Let $\{G_\lambda : \lambda \in \Lambda\}$ be a family of groups. Let e_λ denote the identity of the group G_λ. Suppose that

$$G = \prod_{\lambda\in\Lambda} G_\lambda \tag{6.3.1}$$

denote the Cartesian product of sets $\{G_\lambda\}$. Define product of c-functions as follows. If $x, y \in G$, let

$$(xy)_\lambda = (x_\lambda)(y_\lambda) \quad \text{for all} \quad x, y \in G,\ \lambda \in \Lambda. \tag{6.3.2}$$

Then xy is clearly a c-function in G. So, this defines a binary operation on G. It is easy to see that G is a group with respect to this binary operation such that the c-function $e : \lambda \mapsto e_\lambda$ is the identity in G and the map $x^{-1} : \lambda \mapsto (x_\lambda)^{-1}$ is the inverse of the c-function $x \in G$. Further, the map

$$\pi_\lambda : x \mapsto x_\lambda \quad \lambda \in \Lambda \tag{6.3.3}$$

is a surjective homomorphism $\pi_\lambda : G \to G_\lambda$. For convenience of later reference we summarize the foregoing discussion as:

Proposition 6.3.1. *Let $\mathcal{G} = \{G_\lambda : \lambda \in \Lambda\}$ be a family of groups. Then the Cartesian product G of the family $\mathcal{G}$ (Equation* (**??**)*) is a group with respect to that binary operation in G defined by Equation* (**??**)*. Moreover, for each $\lambda \in \Lambda$, the map π_λ (Equation* (**??**)*) is a homomorphism of G onto G_λ.*

The group G is abelian if and only if every group G_λ is abelian.

Definition 6.3.1. Let $\mathcal{G} = \{G_\lambda : \lambda \in \Lambda\}$ be a family of groups. The group

$$G = \prod \mathcal{G} = \prod_{\lambda \in \Lambda} G_\lambda,$$

constructed in the foregoing proposition is called the *direct product* of the family $\mathcal{G}$ and for each $\lambda \in \Lambda$, the homomorphism $\pi_\lambda : G \to G_\lambda$ is called the *projection* of the product to G_λ. In particular, if Λ is finite, say $\Lambda = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, then we write

$$G = G_0 \times G_1 \times \cdots \times G_{n-1}$$

as usual.

The set $\{\pi_\lambda\}$ of projections characterizes the product group up to isomorphism in the following sense.

Proposition 6.3.2. *Let $\{G_\lambda : \Lambda\}$ be a family of groups. A group H is isomorphic to the group*

$$G = \prod_{\lambda \in \Lambda} G_\lambda$$

if and only if, for each $\lambda \in \Lambda$, there exists a homomorphism $\phi_\lambda : H \to G_\lambda$ with the following universal property: if K is a group and for each $\lambda \in \Lambda$, $\eta_\lambda : K \to G_\lambda$ is a homomorphism then there exists a unique homomorphism $\eta : K \to G$ such that the following diagram commutes for each $\lambda \in \Lambda$:

$$\begin{tikzcd} & G_\lambda \\ K \arrow[ur, "\eta_\lambda"] \arrow[r, "\eta"'] & H \arrow[u, "\phi_\lambda"'] \end{tikzcd} \tag{6.3.4}$$

In particular, the set $\{\pi_\lambda : \lambda \in \Lambda\}$ of projections satisfies this universal property and up to isomorphism, the group G is uniquely characterized by this property.

Proof. We first show that the set $\{\pi_\lambda\}$ satisfies the stated universal property. So, let $\eta_\lambda : K \to G_\alpha$ be a homomorphism for each $\lambda \in \Lambda$. For $k \in K$, let $k\eta$ be the function of Λ defined by

$$(k\eta)_\lambda = k\eta_\lambda \quad \text{for all} \quad \lambda \in \Lambda.$$

Then $k\eta$ is clearly a unique c-function and $\eta : k \mapsto k\eta$ is a well-defined function of K to G. Since each η_λ is a homomorphism, the definition of the binary operation in G and the above definition of $k\eta$ shows that η is a homomorphism. Since the component of $k\eta$ at $\lambda \in \Lambda$ is $k\eta_\lambda$ for all $\lambda \in \Lambda$, we have $(k\eta)\pi_\lambda = k\eta_\lambda$. Hence $\eta \circ \pi_\lambda = \eta_\lambda$ for all $\lambda \in \Lambda$ and so the diagram **??** commutes for all λ. To see that η is unique, assume that $\psi : H \to G$ also make Diagram **??** commute. Then for any $\lambda \in \Lambda$ and $k \in K$, we have

$$(k\psi)_\lambda = k\eta_\lambda = (k\eta)_\lambda.$$

Hence $k\psi$ and $k\eta$ have the same components at every $\lambda \in \Lambda$ and so, $\psi = \eta$.

The underlying set of product group G is, by definition, the Cartesian product of sets G_λ and the binary operation on G is defined *coordinate-wise* (see Proposition 6.3.1). As we shall see below, this construction appears in several contexts. Here it should be noted that we have not assumed that the groups G_λ are distinct for distinct indices. In fact an important particular case is obtained by taking G_λ to be same group H for all $\lambda \in \Lambda$. In this case, the cartesian product

$$\prod_{\lambda\in\Lambda} G_\lambda = \prod_{\lambda\in\Lambda} H = H^\Lambda$$

is the set of all functions $g : \Lambda \to H$. Thus the product group $G = H^\Lambda$ is the group of all functions on Λ with values in H and with composition defined pointwise: for $h, g \in G$,

$$(\lambda)hg = ((\lambda)h)((\lambda)g) \quad \text{for all} \quad \lambda \in \Lambda.$$

Notice that the right hand side above is the product in H.

We may also formulate this concept for special classes of groups. Thus, if $\mathfrak{C}$ is a class of group, the direct product of a family $\mathcal{G}$ in $\mathfrak{C}$ is a group $K \in \mathfrak{C}$ and a set of homomorphisms $\{\eta_\lambda : K \to G_\lambda\}$ such that, given any set $\{h_\lambda : H \to G_\lambda\}$ of homomorphisms of groups in $\mathfrak{C}$, there is a unique homomorphisms $h : H \to K$ such that $h_\lambda = h \circ \eta_\lambda$ for all λ. When direct products exist for all families of groups in $\mathfrak{C}$, we say that the class $\mathfrak{C}$ *has* direct products. By Proposition 6.3.2, the direct product defined earlier is the direct product in the class of all groups. Similarly, since direct product of abelian groups is abelian, the class of abelian groups has direct products.

More general definitions of products (the *semi-direct products* etc., see Exercise 6.18) are also possible and are needed in the study of structure of groups. The readers may refer to any good book on algebra (in particular, group theory) for a systematic account of these (see for example, Jacobson (1974)).

6.4. Direct Sum

Another useful construction of groups is the direct sum. As above, let $G = \prod_\Lambda G_\lambda$ be the direct product of the family of groups $\mathcal{G} = \{G_\lambda : \Lambda\}$. For each $\lambda \in \Lambda$, let e_λ denote the identity of the group G_λ. Suppose that

$$H = \{c \in G : \text{for some finite} \quad F \subseteq \Lambda, \quad c_\lambda = e_\lambda \quad \text{for all} \quad \lambda \in \Lambda - F.\} \tag{6.4.1}$$

It is easy to see from Proposition 6.3.1 (the definition the group structure on G) that H is a subgroup of G. In particular, for fixed $\lambda \in \Lambda$ and $a \in G_\lambda$, the c-function $\hat{a}$ such that

$$\hat{a}_\mu = \begin{cases} a & \text{if } \mu = \lambda; \\ e_\mu & \text{if } \mu \neq \lambda \end{cases}$$

is in H. Furthermore, the map $\iota_\lambda : a \mapsto \hat{a}$ is an injective homomorphism of G_λ into H. For each $\lambda \in \Lambda$, let

$$\hat{G}_\lambda = \operatorname{Im} \iota_\lambda, \qquad H_\lambda = \vee\{\hat{G}_\mu : \mu \neq \lambda\}. \tag{6.4.2}$$

Then it is clear that

$$H_\lambda = \{x \in H : x_\lambda = e_\lambda\}, \qquad H = \vee\{\hat{G}_\lambda : \lambda \in \Lambda\}.$$

It follows easily that every element in $\hat{G}_\lambda$ commutes with every element in H_λ. Using the definition of $\hat{G}_\lambda$ and the second equality above, it can be shown that every $h \in H$ can be uniquely written in the form

$$h = a_1 a_2 \ldots a_n \quad \text{with} \quad a_i \in \hat{G}_{\mu_i}$$

where the indices μ_i, $i = 1, 2, \ldots, n$ are distinct.

Definition 6.4.1. The group H constructed above is called the *direct sum* of the family $\mathcal{G}$ and is written as

$$H = \bigoplus_{\lambda \in \Lambda} G_\lambda.$$

In particular, if Λ is finite, say $\Lambda = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, then we write

$$H = G_0 \oplus \cdots \oplus G_{n-1}$$

as usual. The homomorphisms ι_λ with $\lambda \in \Lambda$ are called the *injections* of the direct product.

Observe that, we have constructed direct sum H as a subgroup of the corresponding direct product consisting of all c-functions that have only finitely many non-identity components. Hence if Λ is finite, it follows that $H = G$ and so, the direct sum coincide with the direct product: we have

$$G_1 \times G_2 \times \cdots \times G_n = G_1 \oplus G_2 \oplus \cdots \oplus G_n \tag{6.4.3}$$

if $\Lambda = \mathbb{Z}_n$.

As for direct products, we have a characterization of direct sums in terms of injections. We first prove the following.

Proposition 6.4.1. *Suppose that $\mathcal{G} = \{G_\lambda : \lambda \in \Lambda\}$ is a family of groups with direct sum H and, for each $\lambda \in \Lambda$, let $\kappa_\lambda : G_\lambda \to K$ be a homomorphism of G_λ to the group K. Write*

$$G_\lambda^k = \operatorname{Im} \kappa_\lambda \quad \textit{and} \quad K_\lambda = \vee\{G_\mu^\kappa : \mu \neq \lambda\}.$$

Then there is a unique homomorphism $\kappa : H \to K$ such that the following diagram commute

$$\begin{tikzcd} H \arrow[r, "\kappa"'] & K \\ G_\lambda \arrow[u, "\iota_\lambda"] \arrow[ur, "\kappa_\lambda"'] & \end{tikzcd} \tag{6.4.4}$$

for all $\lambda \in \Lambda$ if and only if

$$(a\kappa_\lambda)(b\kappa_\mu) = (b\kappa_\mu)(a\kappa_\lambda) \tag{6.4.5}$$

for all $a \in G_\lambda$ and $b \in G_\mu$ with $\lambda \neq \mu$. Furthermore, the homomorphism $\kappa : H \to K$ is surjective if and only if

$$K = \vee\{G_\lambda^\kappa : \lambda \in \Lambda\} \tag{6.4.6}$$

and injective if and only if for every $\lambda \in \Lambda$, κ_λ is injective and

$$G_\lambda^\kappa \cap K_\lambda = \{e_K\} \tag{6.4.7}$$

where e_K denotes the identity of K.

Proof. First assume that the set $\{\kappa_\lambda\}$ of homomorphisms from $\mathcal{G}$ to K satisfies the given conditions. Let $x \in H$. Then, by the definition, x has only finitely many non-identity components, say, $a_1, a_2, \ldots, a_n$ with $a_i \in G_{\lambda_i}$. Then

$$x = \hat{a}_1\hat{a}_2 \ldots \hat{a}_n.$$

Define

$$x\kappa = (a_1)\kappa_{\lambda_1}(a_2)\kappa_{\lambda_2}\dots(a_n)\kappa_{\lambda_n}.$$

Now if $x = y$, $x, y \in H$, then

$$x = \hat{a}_1\hat{a}_2\dots\hat{a}_n = \hat{b}_1\hat{b}_2\dots\hat{b}_m = y$$

where $a_i \in G_{\lambda_i}$, $i = 1, \dots n$ and $b_j \in G_{\mu_j}$, $j = 1, \dots, m$, then x and y are representations of the same c-function. Hence they must have the same components. Thus for each i, we must have $\lambda_1 = \mu_j$ and $a_i = b_j$ for some j. Therefore $x = y$ only if x and y have the same factors except for order in which they appear. In view of Equation (**??**), it follows that κ defined above is a single valued map of H to K. Clearly, $\kappa : H \to K$ is a homomorphisms. Since, for $\hat{a} \in \hat{G}_\lambda \subseteq H$, $\lambda \in \Lambda$, $(\hat{a})\kappa = a\kappa_\lambda$ by the definition above, the Diagram **??** commutes for all $\lambda \in \Lambda$. If the homomorphism $\kappa' : H \to K$ also make the diagram commute, then for $x = \hat{a}_1\dots\hat{a}_r \in H$,

$$\begin{aligned}
x\kappa' &= (\hat{a}_1)\kappa'\dots(\hat{a}_r)\kappa' \\
&= (a_1)\kappa_{\lambda_1}\dots(a_r)\kappa_{\lambda_r} && \text{by Equation (??)} \\
&= (\hat{a}_1)\kappa\dots(\hat{a}_r)\kappa && \text{again by Equation (??)} \\
&= x\kappa.
\end{aligned}$$

Hence $\kappa' = \kappa$ and this proves the uniqueness of κ.

Conversely, assume that homomorphism $\kappa : H \to K$ exists so that Diagram **??** commutes for all λ. Let $a \in G_\lambda$ and $b \in G_\mu$ where $\lambda \neq \mu$. Then

$$\begin{aligned}
(a\kappa_\alpha)(b\kappa_\mu) &= ((a\iota_\lambda)\kappa)((b\iota_\mu)\kappa) \\
&= ((\hat{a})\kappa)((\hat{b})\kappa) \\
&= ((\hat{a})(\hat{b})\kappa) \\
&= ((\hat{b})(\hat{a})\kappa) \\
&= (b\kappa_\mu)(a\kappa_\lambda).
\end{aligned}$$

Hence Equation (**??**) holds.

Assume that $\kappa : H \to K$ is surjective and let $u \in K$. By hypothesis, there is $x = \hat{a}_1\hat{a}_2\dots\hat{a}_r$ with $a_i \in G_{\lambda_i}$ such that

$$\begin{aligned}
u = (x)k &= (\hat{a}_1\hat{a}_2\dots\hat{a}_r)\kappa \\
&= (\hat{a}_1)\kappa(\hat{a}_2)\kappa\dots(\hat{a}_r)\kappa && \text{using Equation (??)} \\
&= (a_1)\kappa_{\lambda_1}(a_2)\kappa_{\lambda_2}\dots(a_r)\kappa_{\lambda_r}.
\end{aligned}$$

Hence $u \in \vee\{G_\lambda^\kappa : \lambda \in \Lambda\}$ and so, Equation (**??**) holds. Conversely suppose that Equation (**??**) is satisfied and let $h \in K$. So $h = (a_1)\kappa_{\lambda_1}(a_2)\kappa_{\lambda_2} \ldots (a_r)\kappa_{\lambda_r}$ for $a_i \in G_{\lambda_i}$. Then, as above, using Equation (**??**), we have have

$$\begin{aligned} u &= (a_1)\kappa_{\lambda_1}(a_2)\kappa_{\lambda_2} \ldots (a_r)\kappa_{\lambda_r} \\ &= (\hat{a}_1\hat{a}_2 \ldots \hat{a}_r)\kappa \\ &= (x)\kappa \end{aligned}$$

where $x \in H$. So κ is surjective.

Next suppose that $\kappa : H \to K$ is injective and let $u \in G_\lambda^\kappa \cap K_\lambda$. Then, for some $a \in G_\alpha$, $u = (a)\kappa_\alpha$ and for $b_i \in G_{\mu_i}$, $i = 1, 2, \ldots, r$, $u = (b_1)\kappa_{\mu_1} \ldots (b_r)\kappa_{\mu_r}$ where $\lambda \neq \mu_i$ for any i. Then

$$\begin{aligned} e_K &= (a^{-1})\kappa_\lambda(b_1)\kappa_{\mu_1} \ldots (b_r)\kappa_{\mu_r} \\ &= (\hat{a}^{-1}\hat{b}_1 \ldots \hat{b}_r)\kappa. \end{aligned}$$

Since κ is injective, we have

$$x = \hat{a}^{-1}\hat{b}_1 \ldots \hat{b}_r = e.$$

It follows that every component of the c-function x is identity and so, $a = e_\lambda$ and $b_i = e_{\mu_i}$ for all i. Therefore $u = e_K$ which implies that Equation (**??**) holds. Since ι_λ is injective, each κ_λ is injective by Equation (**??**). On the other hand, assume that each κ_λ is injective and that Equation (**??**) holds for each λ. Let $x \in H$ with $x\kappa = e_K$. Since $x \in H$, we can find $a_i \in G_{\mu_i}$, $i = 1, 2, \ldots, r$ such that

$$x = \hat{a}_1\hat{a}_2 \ldots \hat{a}_r.$$

Then an easy calculation using Equation (**??**) gives

$$(a_1)\kappa_{\lambda_1}(a_2)\kappa_{\lambda_2} \ldots (a_r)\kappa_{\lambda_r} = x\kappa = e_K.$$

By Equation (**??**), this gives

$$u = (a_i^{-1})\kappa_{\lambda_i} = (a_1)\kappa_{\lambda_1} \ldots (a_{i-1})\kappa_{\lambda_{i-1}}(a_{i+1})\kappa_{\lambda_{i+1}} \ldots (a_r)\kappa_{\lambda_r}.$$

Therefore, $u \in G_{\lambda_i}^\kappa \cap K_{\lambda_i}$ and so, by Equation (**??**), $(a_i)\kappa_{\lambda_i} = e_K$. Since κ_{λ_i} is injective, we have $a_i = e_{\lambda_i}$. Hence $\hat{a}_i = e$. Since this is true for all i, we conclude that $x = e$. Thus κ is injective.

The following characterization of direct sums are immediate from the proposition above.

Proposition 6.4.2. *Let $\mathcal{G} = \{G_\lambda : \lambda \in \Lambda\}$ be a family of groups. A group K is isomorphic to the direct sum of the family $\mathcal{G}$ if and only if for each $\lambda \in \Lambda$ there is an injective homomorphism $\phi_\lambda : G_\lambda \to K$ satisfying Equations* (**??**), (**??**) *and* (**??**).

In view of the foregoing result we may define the direct sum as a pair $(K, \{\kappa_\lambda\})$ consisting of a group K and injective homomorphisms $\kappa_\lambda : G_\lambda \to K$ satisfying Equations (**??**), (**??**) and (**??**). In particular, if we consider the family $\{\hat{G}_\lambda : \Lambda\}$, the inclusion homomorphisms $\jmath_\lambda : \hat{G}_\lambda \to H$ satisfy the conditions specified above. Here H is the direct sum of the given family (see Definition **??**) defined earlier. Hence H is also the direct sum of the family $\{\hat{G}_\lambda\}$ with respect to the inclusions of $\hat{G}_\lambda$ in H. We say that H is the *internal* direct sum of the family $\{\hat{G}_\lambda\}$. Thus every direct sum is isomorphic to an internal direct sum. In fact, identifying each $\hat{G}_\lambda$ with G_λ by ι_λ (which is an isomorphism of G_λ on to $\hat{G}_\lambda$), the direct sum H is identified as an internal direct sum.

Given any family of homomorphisms $\{h_\lambda : G_\lambda \to K\}$, the condition Equation (**??**) holds automatically if the group K is abelian. Therefore in this case, the homomorphism $\kappa : H \to K$ always exists:

Corollary 6.4.1. Let $\mathcal{G}$ be a family of groups (as in the statement of Proposition **??**) and for each $\lambda \in \Lambda$, let $\{\kappa_\lambda : G_\alpha \to K\}$ be a homomorphism to an abelian group K. Then there is a unique homomorphism $\kappa : H \to K$ such that the diagram Equation (**??**) commutes.

Remark 6.4.1 There is a construction dual to the construction of direct product of groups which is called the *coproduct* or *free product* of the family. The coproduct of a family $\{G_\lambda : \lambda \in \Lambda\}$ of groups consists of a group

$$K = \coprod_{\lambda \in \Lambda} G_\lambda \quad \text{together with a set} \quad j_\lambda : G_\lambda \to K \tag{6.4.8}$$

of homomorphisms, called *injections* of the coproduct, such that given any set of homomorphisms $g_\lambda : G_\lambda \to K'$ there is a unique homomorphism $g : K \to K'$ such that the following diagram commutes:

$$\begin{tikzcd} & G_\lambda \arrow[dl, "g_\lambda"'] \arrow[d, "j_\lambda"] \\ K' & K \arrow[l, "g"] \end{tikzcd} \tag{6.4.9}$$

for each $\lambda \in \Lambda$ (see Exercise 6.16 for a construction of coproducts). As for products, coproducts may also be represented as pairs of the form $(K, \{j_\lambda\})$ that determine coproducts uniquely up to isomorphism. Notice that, the diagram (**??**) above specifying the universal property of coproduct is obtained essentially by reversing the arrows of the diagram (**??**) (cf. Proposition 6.3.2). The coproduct is dual to product in this sense. Also, unlike products, coproducts defined above may not be commutative even when all groups G_λ are commutative. However, Corollary **??** shows that in the class of abelian groups direct sums are coproducts (see also Exercise 6.17). In general, coproducts and direct sums are different, the former is bigger than the latter in the sense that the direct sum is a quotient of coproducts. For this reason, we often call the coproducts of groups as *free products*.

6.5. Generators and Relations

Let X be a set. A *word* over X is a finite sequence

$$w = a_1 a_2 \dots a_n$$

of symbols in X. In this situation X is often referred to as an *alphabet* and elements of X as letters. The length of the word w is the positive integer $n \in \mathbb{N}$, which represents the number of letters in w. Notice that letters in w may repeat. We also admit a unique word e having no letters, called the empty word. The set of all words over the alphabet X, including empty word e, is denoted by $W(X)$. It is clear that concatenation is an associative binary operation on $W(X)$ with the empty word e as identity. Thus $W(X)$ is a monoid, called the *free monoid* generated by the set X.

Now suppose that X and X' are disjoint sets of the same cardinality. Fix a bijection $\iota : X \to X'$ (which exists by the definition of cardinal numbers). For each $x \in X$, let x^{-1} denote the element $x\iota \in X'$; similarly if $y \in X'$, y^{-1} denotes the unique element in X such that $(y^{-1})\iota = y$. Pairs of elements of the form (x, x^{-1}) or (y^{-1}, y) are said to be mutually inverse. For $w_1, w_2 \in W(X \cup X')$, we shall write

$$w_1 \Leftrightarrow w_2$$

if and only if either $w_1 = w_2$ or w_2 is obtained from w_1 by introducing or removing a pair of adjacent and mutually inverse pair of letters. This clearly defines a reflexive and symmetric relation on the set of all words over $X \cup X'$. Let $\sim$ denote the transitive closure of $\Leftrightarrow$:

$$\begin{aligned} w \sim w' \iff & \text{ there exists } w_i \in F_{X\cup X'},\ i = 1, 2, \dots, n \text{ such that} \\ & w = w_1 \Leftrightarrow w_2 \Leftrightarrow \cdots \Leftrightarrow w_n = w'. \end{aligned} \tag{6.5.1}$$

The relation $\sim$ defined by Equation (**??**) is clearly an equivalence relation on the set $W(X \cup X')$ of all words over $X \cup X'$. Let $[w]$ denote the $\sim$-class of $w \in W(X \cup X')$ and let

$$F_X = \{[w] : w \in W(X \cup X')\}.$$

Given any word $w \in W(X \cup X')$, removing all the adjacent and mutually inverse pair of letters from w, we obtain a word w^* for which no further reduction (removal of non-trivial adjacent, mutually inverse pair of letters) is possible. It can be shown that the word w^* is unique. Therefore each $\sim$-class $[w]$ contains a unique reduced word. If no ambiguity is likely, we may take $[w]$ to be the unique reduced word belonging to the $\sim$-class of w. Note that even if w_1 and w_2 are reduced words, the word w_1w_2 obtained by concatenation, may not be reduced. Clearly, empty word e is reduced so that $e = [e]$. Also, for any $w \in W(X \cup X')$, $[ww^{-1}] = [e]$.

We use notations and conventions established above in the following statement:

Theorem 6.5.1. *Let X be a set. For $w_1, w_2 \in W(X \cup X')$ define*

$$[w_1][w_2] = [w_1w_2].$$

This is a single-valued binary operation on $F_X = F$ such that F is a group with the following property: Given any map $f : X \to G$ of X into a group G, there is a unique homomorphism $\tilde{f} : F \to G$ making the following diagram commute:

$$\begin{tikzcd} & G \\ X \arrow[ur, "f"] \arrow[r, "j"'] & F \arrow[u, "\tilde{f}"'] \end{tikzcd} \qquad (\bullet)$$

Here $j = j_X : x \mapsto [x]$ is the map sending x to the $\sim$-class $[x]$ of the word containing the only letter x.

Proof. The discussion preceding the statement shows that $\sim$ is an equivalence relation. From Equation (**??**) it clear that

$$w_1 \sim v_1, \quad \text{and} \quad w_2 \sim v_2 \Longrightarrow w_1w_2 \sim v_1v_2.$$

Hence the binary operation on $F = F_X$ defined in the statement is single-valued. Also since concatenation is an associative binary operation on $W(X \cup X') = W$ with identity e (the empty word), the binary operation of F is associative and has identity

$[e]$. If $w = x_1x_2 \dots x_n$, let $w^{-1} = x_n^{-1} \dots x_2^{-1}x_1^{-1}$. Then we have

$$\begin{aligned} ww^{-1} &\Leftrightarrow x_1 \dots x_{n-1}x_{n-1}^{-1} \dots x_1^{-1} \\ &\Leftrightarrow \cdots \Leftrightarrow e. \end{aligned}$$

Hence $[w][w^{-1}] = [ww^{-1}] = [e]$. Similarly $[w^{-1}][w] = [e]$. Therefore $[w^{-1}]$ is the inverse of $[w]$ and this shows that F is a group. To prove that the diagram (•) commutes, let $f : X \to G$ be a map. For convenience, write a for xf, $x \in X$. First extend to $X \cup X'$ by setting $(x^{-1})f = (xf)^{-1}$. Since $X \cap X' = \emptyset$, f extended this way is a single-valued map of $X \cup X'$ to G. If $w = x_1 \dots x_n$ and $w' = y_1 \dots y_m$ are words in W, then easily seen that

$$(x_1)f \dots (x_n)f = (y_1)f \dots (y_m)f \quad \text{if} \quad w \sim w'.$$

Therefore,

$$[x_1 \dots x_n]\tilde{f} = (x_1)f \dots (x_n)f$$

is a single-valued map of F to G. It follows readily from the definition of $\tilde{f}$ that it is a homomorphism. Let $x \in X$. The definition of $j = j_X$ and $\tilde{f}$ gives

$$(x)j \circ \tilde{f} = [x]\tilde{f} = (x)f.$$

Since this holds for all $x \in X$, the given diagram commutes.

Definition 6.5.1. A *free group* on a set X is a pair (F, j) where F is a group and $j : X \to F$ is a map such that, given any map $f : X \to G$ from X to a group G, there is a unique homomorphism $\tilde{f} : F \to G$ such that

$$j \circ \tilde{f} = f$$

(that is, the diagram in the statement of the theorem above commutes).

Clearly, any two free groups on a set X are isomorphic. Also the theorem above shows that there is a free group F_X on every set X. Hence the group F_X may be taken as the unique (up to isomorphism) free group generated by X. As we have observed above, F_X can be identified as the set of all reduced words over $X \cup X'$ and hence a subset of $W = W(X \cup X')$. But notice that F_X is not a subgroup of W; that is, the binary operation in F_X defined in the theorem is not concatenation.

Another consequence of the theorem above is the following. Let G be any group. Then the identity map $1_G : G \to G$ is a map from the set G to the group G. Hence by Theorem **??** $q = \tilde{1}_G : F_G \to G$ is a homomorphism which is clearly surjective. Let $R_G = R = \ker q$. By Theorem **??**, G is isomorphic to the quotient group F_G/R. Thus:

Corollary 6.5.1. *Every group is isomorphic to a quotient group of a free group.*

Suppose that G is isomorphic to the quotient F_X/R where R is a normal subgroup in F_X. Then R is set of elements of F_X that are mapped by the quotient homomorphism $q_R : F_X \to F_X/R$ to identity. Now, as observed above, we may consider R as a set of reduced words over X. Hence the group G is uniquely determined by the set X and the set R of reduced words; this fact is indicated by writing

$$G = \langle X : R\rangle = \langle X : \{w = 1 | w \in R\}\rangle$$

which is called a *presentation* of G. The set X called a set of *generators* of G and the words in R are called *relations* in G. Also, a group G is free if and only if it has a presentation in which the set of relations contains only empty relation. Evidently, a group can have more than one presentation. If $\{w_\alpha : \alpha \in I\}$ is a set of words in R such that every word in R is a finite product of words w_α, then a presentation for G can also be expressed as

$$G = \langle X : \{w_\alpha = 1 | \alpha \in I\}\rangle.$$

In this case relations in R are said to be *consequences* of the relations w_α and consists of the subgroup generated by the set $\{w_\alpha : \alpha \in I\}$. When X is finite, G is called a *finitely generated* group and if all relations in R are consequences of a finite set of relations $w_1, w_2, \ldots, w_n$ then G is said to be *finitely presented*. If the group is both finitely generated with the set of generators $X = \{x_1, x_2, \ldots, x_n\}$ and finitely presented with relations w_i, $i = 1, 2, \ldots, r$ then a presentation of G is usually written as

$$G = \langle x_1, \ldots, x_n : w_1 = 1,\ w_2 = 1,\ \ldots,\ w_r = 1\rangle.$$

Note that, often, relations in a group may be presented more conveniently in the form $u_i = v_i$ where $u_i, v_i \in F_X$ if we can write w_i as $w_i = u_i(v_i)^{-1}$ (see Exercise 6.20).

Clearly every finite group is both finitely generated and finitely presented. A group generated by a single element is said to be *cyclic* (see Exercise 6.19).

6.6. Actions of Groups

In practice, groups that come up naturally in various contexts are groups of functions, matrices, etc. Therefore methods of representing groups as groups of functions, matrices, etc., are important. In general, a *representation* of a group G is a homomorphism of G into a group of some concrete type such as groups of matrices over fields, permutations on sets, operators on spaces, etc. Matrix representations and permutation representations are of particular importance in algebraic theory of groups. We begin with the definition of an auxillary concept of an *action* of a group on a set which is equivalent to representations. Though we are concerned with groups here, we define the concept for the more general class of semigroups and monoids. Notice that groups are monoids.

Definition 6.6.1. By an *right action* of a semigroup S on a set X we mean a function

$$F : X \times S \to X; \quad (x, g) \mapsto xg$$

satisfying the following:

$$(xg)h = x(gh) \quad \text{for all} \quad g, h \in S, \ x \in X. \tag{6.6.1}$$

When this holds, X is called a *right S-set* (with respect to the action F). A *left action* of S over X and a *left S-set* can be defined modifying the above definition in the obvious way. In addition, if S is a monoid (having identity 1), the action F of S on X is a *monoid action* if

$$x1 = x \quad \text{for all} \quad x \in X. \tag{6.6.2}$$

In particular, a right [left] *group action* by a group G on X is a monoid action by G on X (that is function F on $X \times G$ to X satisfying both Equation (**??**) and Equation (**??**)).

For brevity, by an action of a group or a semigroup S on X we shall mean a right action, unless otherwise indicated explicitly. Similarly, by a S-set we shall mean a right S-set.

Definition 6.6.2. Let X and Y be S-sets. A *S-map* $f : X \to Y$ is a function such that

$$f(xs) = f(x)s \quad \text{for all} \quad x \in X, \quad s \in S. \tag{6.6.3}$$

If $X \subseteq Y$, then X is said to be an S-subset of Y if the inclusion is an S-map. A bijective S-map $f : X \to Y$ is called an S-isomorphism.

If $f : X \to Y$ is a bijective S-map, then $f^{-1} : Y \to X$ is also a bijective S-map. Hence the usual property of isomorphisms that *inverse of an isomorphism is also an isomorphism* holds in the case of S-maps also.

Note that we have written S-maps of right S-sets as left operators. To be consistent with this we shall use the “right-left” composition law for S-maps of right

S-sets. Analogously, S-maps of left S-sets will be written as right operators and the "left-right" composition law will be used for these.

Let X be a S-set and $s \in S$. Then $\rho_s : x \mapsto xs$ is clearly a transformation of X. If $s, t \in S$,

$$\begin{aligned} x\rho_s\rho_t &= (xs)t = x(st) && \text{by Equation } (\textbf{??}) \\ &= x\rho_{st} && \text{for all } x \in X \end{aligned}$$

This gives that the mapping $s \mapsto \rho_s$ is a homomorphism of S to the semigroup T_X of all transformations of X (see Exercise 6.2). If $S = G$, a group, it can be seen, using Equation (**??**) and Equation (**??**) that the transformation $\rho_{s^{-1}}$ induced as above by the element $s^{-1} \in G$ is the inverse of ρ_s and so, ρ_s is a permutation of X. Hence we have the following in which the converse part is routine.

Proposition 6.6.1. *Let X be a right S-set. For $s \in S$, the map*

$$\rho : s \mapsto \rho_s \quad \text{where for each } x \in X \quad x\rho_s = xs$$

is a homomorphism of S into the semigroup T_X of transformations on X. If S is a group, ρ is a homomorphism of S into the symmetric group $S(X)$ of all permutations on X.

Conversely, if $\phi : S \to T_X$ is any homomorphism of the semigroup S into T_X, then the map

$$(x, s) \mapsto x\phi(s) \quad (x, s) \in X \times S$$

defines a right action of S on X such that the homomorphism ρ associated with this right S-set as in the first part coincides with ϕ. Moreover, if S is a group, the the action determined by ϕ is a group action if and only if ϕ is a permutation representation.

Remark 6.6.1. Let T°_X denote the semigroup of all transformations of X under "right-left" composition (the semigroup obtained from T_X by reversing the multiplication). Then the proposition above holds for left S-sets if we replace T_X by T°_X. Notice that a map $\phi : S \to T_X$ is a homomorphism into T°_X if and only if

$$(g\phi)(h\phi) = (hg)\phi \quad \text{for all} \quad g, h \in S$$

where the left-hand side represents composition in T_X. Maps with this property are called *anti-homomorphisms* (or an anti-representations) of S to T_X. Alternatively Proposition **??** can be formulated for left S-sets by replacing homomorphisms in the statement of the proposition by anti-homomorphisms. These remarks carry over verbatim to left group actions if we replace T_X by the symmetric group $S(X)$ and

T_X° with $S^\circ(X)$, the symmetric group on X under “right-left” composition. Note that if the semigroup (or group) under consideration is abelian, then there is no difference between left and right actions. Moreover, a left group action can always be identified canonically with a right action: if X is a left G-set, define a right action of G on X by setting $xg = g^{-1}x$ for all $x \in X$ and $g \in G$.

The Proposition above shows that with each action of a group G on a set X, there is a representation of G by permutations of X. Thus group actions or G-sets and permutation representations are equivalent. We say that a G-set is *faithful* if the associated representation is faithful (or one-to-one). The corresponding remarks are valid for semigroup actions and representations by transformations; in particular, an action by a semigroup S on the set X is faithful if the associated representation is one-to-one.

For the remainder of this section, we are concerned with group actions.

Definition 6.6.3. Suppose that X be a G-set. For $x \in X$, the subset

$$xG = \{xg : g \in G\} \tag{6.6.4}$$

of X is called the *orbit* of x under the action of G and

$$G_x = \{g \in G : xg = g\} \tag{6.6.5}$$

is called the *stabilizer* of x. G_x is a subgroup of G. A G-set X is said to be *transitive* if $X = xG$ for any $x \in X$.

If $f : X \to Y$ is a G-map then for any $x \in X$, it is easily seen that

$$f(xG) = f(x)G \quad \text{and} \quad G_x \subseteq G_{f(x)}.$$

Consequently any injective G map of transitive G-sets is an isomorphism. The following observations illustrate the definitions above. The verification is routine.

Proposition 6.6.2. *Let H be a subgroup of a group G. Then the set $X = H \wr G$ of all right cosets of H is a G-set under the natural action of G on X:*

$$(Hk)g = H(kg) \quad \textit{for all} \quad Hk \in H \wr G, \; g \in G.$$

Moreover, $H \wr G$ is a transitive G-set under the above action and the stabilizer group of Hk is

$$G_{Hk} = k^{-1}Hk.$$

Dually the set $G \wr H$ is a left G-set under the natural action of G on $G \wr H$.

We use these observations in

Proposition 6.6.3. *For a G-set X we have the following:*

A. *For each $x \in X$ the orbit xG is a G-subset of X and there is a G-isomorphism $\phi : G_x \wr G \to xG$.*

B. *The set of orbits forms a partition of X.*

Proof. It is clear from the definition that xG is a transitive G-subset of X. Define $\phi : G_x \wr G \to xG$ by

$$\phi(G_x k) = xk.$$

This is well-defined. For if $G_x k = G_x g$, then $kg^{-1} \in G_x$ and so, $xg = (xkg^{-1})g = xk$. Similar argument shows that ϕ is one to one. Obviously, ϕ is surjective. Now

$$\phi((G_x k)g) = \phi(G_x(kg)) = x(kg) = (xk)g = (\phi(G_x k))g.$$

Hence ϕ is a G-isomorphism. This proves A. To prove B, let $z \in xG \cap yG$. Then there is $g, h \in G$ such that $z = xg = yh$ Then $y = xgh^{-1} \in xG$ and so, $yG \subseteq xG$. Similarly $xG \subseteq yG$ and so, $xG = yG$. This proves that orbits determine a partition of X.

The statements A and B above give some elementary counting formulas that are very useful in the study of finite groups and finite G-actions.

Corollary 6.6.1. *Suppose that X is a G-set.*

If G is finite then

$$o(G) = o(G_x)|xG|$$

for all $x \in X$. Hence the number of elements in an orbit is a divisor of the order of G.

If X is finite

$$|X| = |(x_1)G| + |(x_2)G| + \cdots + |(x_k)G|$$

where $(x_i)G$, $i = 1, 2, \ldots, k$ denote distinct orbits of G in X.

Proof. It follows from A of Proposition **??** that $|G_x \wr G| = |xG|$. Hence the desired equality in item (1) holds by Equation (**??**). If X is finite, there are only finitely many distinct orbits in X. Since by Proposition **??** B orbits form a partition, the number of elements in X is the total of the number of elements in distinct orbits. This completes the proof.

We shall discuss large number of examples of G-sets later. In fact most examples of groups arise as G-set on suitable sets. Moreover, every group has a faithful (injective) representation by permutations on a suitable set:

Theorem 6.6.1. (Cayley's Theorem). *Every group G is isomorphic to a permutation group on a suitable set X.*

Proof. We show that every group G is isomorphic to a subgroup of $S(G)$ so that the theorem holds with $X = G$. Clearly the multiplication

$$(x, g) \mapsto xg$$

of $G \times G$ to G defines a right action of the group on itself. Let $\rho : g \mapsto \rho_g$ be the representation determined by this right action as in Proposition **??**. If $\rho_g = \rho_h$, then for all $x \in G$, $xg = xh$ and it follows directly from axioms for groups that $g = h$. Hence $\rho : G \to S(G)$ is injective.

Note that if G is a finite group, G is a finite set and so, $S(G)$ is the symmetric group S_n if $o(G) = n$. Since S_n is clearly a finite group, it follows from the above that every finite group has a representation by a group of finite permutations.

Cayley's theorem gives one permutation representation for every group; but the representation obtained in this way is neither unique nor the most efficient possible. For S_3, the group of all permutations of degree 3, has obvious representation by permutations of degree 3. But S_3 has 6 elements (see Exercise 6.10) and so, the representation given by Cayley's theorem is by permutations of degree 6.

Remark 6.6.2. It may be noted that the argument above can be extended to any semigroup S. In fact, the map $\rho_s : t \mapsto ts$ clearly belongs to T_S for every $s \in S$. Also, it follows as above that the map $s \to \rho_s$ is a homomorphism of S to T_S. In addition, if S is a monoid, then as above it can be shown that $\rho : S \to T_S$ is an injective homomorphism. But ρ may not be a permutation representation (that is ρ_s may not be a permutation for all $s \in S$) unless S is a group. The representation $\rho : S \to T_S$ is called the *right regular representation* of S. The representation constructed in the proof of Cayley's theorem is called *Cayley's* representation which is, in fact the right regular representation of the group.

Another important action of a group G on itself is the action by *conjugation*. If $g \in G$, any element of the form $a^{-1}ga$, $a \in G$ is called a *conjugate* of g. It is clear that the map

$$(a, g) \mapsto a^{-1}ga \tag{6.6.6}$$

is a right action of G on itself. The orbits of $g \in G$ under this action are called the *conjugacy* class of g in G. Some properties of this action are mentioned in Exercise 6.14.

Remark 6.6.3. Very often when we consider action of a group G on a set X, the set may carry additional structures. Thus in the two examples of the action of a group G on itself, the first example (Cayley's representation) does not take the group structure on G into consideration whereas the action by conjugation gives a representation by automorphisms of G. The later type are very important in many applications. Thus we may have an action of a group G on an abelian group A that admits the addition on A in the sense that for all $x, y \in A$ and $g \in G$, $(x + y)g = xg + yg$ which is equivalent to the fact that the corresponding representation is by automorphisms of A. In this case we say that A is a G module with respect to the action. Similarly, we may consider action of a group on vector spaces in which case the action must admit both addition and scalar multiplication or the representation associated with it must be representation by linear transformations. Similarly we can consider actions by rings, fields,etc. (See Definition **??**)

6.7. Rings and Fields

Here we give the definitions of the remaining algebraic objects needed for discussing vector spaces and related concepts.

Definition 6.7.1. Suppose that R is a set with two binary operations $+$, called *addition* and $\cdot$, called *multiplication*. Then the system $(R, +, \cdot)$ is called a *ring* (or that R is a ring with respect to $+$ and $\cdot$) if it satisfies the following axioms:

A: [Addition] Under addition $+ : (x, y) \mapsto x + y$, R is an additive (abelian) group (that is, satisfies axioms G1 - G4 of Definition **??**).

M: [Multiplication] Multiplication $\cdot : (x, y) \mapsto x \cdot y$ is an associative binary operation on R (cf. Equation (**??**)).

D: [Distributive laws]

$$x \cdot (y + z) = x \cdot y + x \cdot z \text{ for all } x, y, z \in R;$$
$$(x + y) \cdot z = x \cdot z + y \cdot z \text{ for all } x, y, z \in R.$$

The ring R is *commutative* if in addition to axioms **A**, **M** and **D** it satisfies:

C: [Commutative law] the multiplication in R is commutative (cf. Equation (**??**)).

Further R is called a *division ring* or a *skew-field* if

> **F: [Skew-field]** $R^* = R - \{0\}$ is a group under multiplication.

Finally a commutative division ring is called a *field*.

By the above, a ring R is a field if and only if R satisfies all the axioms, **A**, **M**, **D**, **C** and **F** of the definition above. In the following, we shall use the symbol $\Bbbk$ to denote fields. Also conventions regarding multiplicative and additive notations established in § **??** and § **??** will be followed for addition and multiplication in rings and fields. Thus the product of $x, y \in \Bbbk$ will be written as xy rather than $x \cdot y$. Note that any division ring, in particular, a field must contain at least two distinct elements. More generally, in a ring R for which multiplicative identity 1 exists and $1 \neq 0$ (for brevity, called *ring with identity*), an element $x \in R$ for which inverse x^{-1} exists, is called a *unit*. The collection of units in R is closed under multiplication and so, forms a subgroup U of R under multiplication called the *group of units* of R. (see Herstein (1975), Artin (1990), etc for details). In particular, in a division ring or a field R, axiom F implies that very non-zero element is a unit.

Given a ring (or a field) R, a subset S of R is a subring (or a subfield) if S itself is a ring (field) with respect to the induced operations on S. Note that this in particular implies that S is closed with respect to both addition and multiplication in R; that is, for all $x, y \in S$, the sum $x + y$ and the product xy in R belong to S. Also, in the case of subfield, multiplicative identity of S must be the same as that of R. A map $f : R \to R'$ of rings is called a *homomorphism* if

$$(x + y)f = xf + yf; \quad (xy)f = (xf)(yf) \quad \text{for all} \quad x, y \in R. \tag{6.7.1}$$

In addition, if R and R' have identities and if f maps the identity of R to identity of R', then f is said to preserve identity. A homomorphism of fields is an identity preserving homomorphism. It is an immediate consequence of the definition that any homomorphism $f : \Bbbk \to \Bbbk'$ of fields is injective.

Products, sums and other constructions considered for groups can be extended to rings also (see Herstein (1975), Artin (1990). The principal example of a ring is the set $\mathbb{Z}$ of integers under usual addition and multiplication. $\mathbb{Z}$ is clearly a commutative ring having identity. Similarly the set $\mathbb{Z}_n$ (see Exercise 6.12) is a ring with respect to addition and multiplication modulo n. Principal examples of fields are $\mathbb{R}$ the set of real numbers under usual addition and multiplication, the set $\mathbb{C}$ of complex numbers, the set $\mathbb{Q}$ of rational numbers.

Remark 6.7.1. We can define the action of a ring (or field) on an abelian group. First note that given any abelian group A the set $\mathrm{End}(A)$ of all endomorphisms of A is a ring (see Exercise 6.21). A right action of a ring R on an additive group A is a homomorphism of R into $\mathrm{End}(A)$. If $\phi : R \to \mathrm{End}(A)$ is any representation, we say that A is a right *R-module* with respect to ϕ. It can be seen from Exercise 6.21 that every ring is a right R module over itself (with respect to the right regular representation) and any abelian group A is a right $\mathrm{End}(A)$ module with respect to the identity homomorphism on $\mathrm{End}(A)$. The abelian group A is also a right (left) module over the ring $\mathbb{Z}$ of integers: the action of $\mathbb{Z}$ on A is defined for all $a \in A$ and $n \in \mathbb{Z}$ by

$$an = na = \begin{cases} a + \cdots + a & n \text{ terms if } n > 0; \\ 0 & \text{if } n = 0; \\ -(a(-n)) & \text{if } n < 0. \end{cases} \tag{6.7.2}$$

We say that the ring R acts on the left of the abelian group A if there is an anti-homomorphism of R into $\mathrm{End}(A)$ and A is a left R module if there is a left action of R on A.

Exercises 6.

6.1. Verify whether the following functions are binary operations. Find those that are associative and/or commutative.

The map $(m, n) \mapsto m + n$ of $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$ (where $\mathbb{N}$ denote the set of natural numbers).

The map $(m, n) \mapsto e^{mn}$ where $m, n \in \mathbb{N}$ and e denote the base of the natural logarithm.

The map $(m, n) \mapsto \mathrm{diff}(m, n)$ where $m, n \in \mathbb{N}$ and $\mathrm{diff}(m, n) = |m - n|$ denotes the difference between m and n.

The map $(m, n) \mapsto (m, n)$ where (m, n) denotes the greatest common divisor of $m, n \in \mathbb{N}$.

Let $\mathfrak{P}(X)$ denote the set of all subsets of a set X; the maps $(U, V) \mapsto U \cap V$, $(U, V) \mapsto U \cup V$, $U, V \in \mathfrak{P}(X)$.

Prove that multiplication of polynomials (with real coefficients) is a binary operation in the set $\mathbb{R}[x]$ of all polynomials with real coefficients.

Find also identities and zeros of the binary operations in the list above whenever they exist.

6.2. Prove that composition of functions has the following properties:

If f, g and h are functions such that the composites fg and gh exist, then $(fg)h$ and $f(gh)$ exist and they are equal.

If $f : X \to Y$, then $1_X \circ f = f = f \circ 1_Y$.

The function $f : X \to Y$ is injective (one-to-one) if and only if the following condition holds: For any $g, h : Z \to X$,

$$g \circ f = h \circ f \Longrightarrow g = h.$$

f is surjective (onto) if and only if for any $g, h : Y \to Z$,

$$f \circ g = f \circ h \Longrightarrow g = h.$$

Let f and g be composable functions. If f and g are injective [surjective], prove that fg is injective [surjective]. Conversely, if fg is injective [surjective], then show that f [g] is injective [surjective] while g [f] may not be injective [surjective].

The function $f : X \to Y$ is bijective (one-to-one and on-to) if and only if there is a function $g : Y \to X$ such that $f \circ g = 1_X$ and $g \circ f = 1_Y$. We denote the function g by f^{-1} and is called the *inverse* of f. When f^{-1} exists, f is said to be *invertible*.

In particular deduce that the set T_X of all transformations of X (that is, functions of X into itself), is a monoid under composition which is not commutative. Moreover, T_X has no zero.

6.3. Verify whether the following are groups.

$(\Bbbk, +)$ where $\Bbbk = \mathbb{C}, \ \mathbb{R}, \ \mathbb{Q}$ or $\mathbb{Z}$.

$(\Bbbk, \cdot)$ where $\Bbbk$ is as in 1 and $\cdot$ is the multiplication.

$(\Bbbk*, \cdot)$ where $\Bbbk^*$ is the set of nonzero numbers in $\Bbbk$ and $\cdot$ is the multiplication.

$(\mathbb{N}, +)$ and $(\mathbb{N}, \cdot)$.

$(\mathbb{R}^+, +)$ and $(\mathbb{R}^+, \cdot)$ where $\mathbb{R}^+$ denotes the set of all positive real numbers.

$(S^1, +)$ and $(S^1, \cdot)$ where $S^1 = \{z \in \mathbb{C} : |z| = 1\}$.

Find those additive groups in the list above which are also rings and/or fields.

6.4. Let X be a set. Prove that the set T_X of all maps of X into itself is not a group under composition. However, if $S(X)$ denotes the set of all permutations of X onto X, then $S(X)$ is a group with respect to composition which is not commutative if X contains more than two elements. Furthermore, let $f : X \to Y$ be a bijection of sets and $\alpha \in S(X)$. Then

$$(\alpha)f^{\#} = f^{-1} \circ \alpha \circ f \in S(Y)$$

and the map $f^{\#} : S(X) \to S(Y)$ is an isomorphism of groups.

6.5. Suppose that S_n is the group of all permutations of the set $X = \{1, 2, \ldots, n\}$ $(n \geq 2)$. For $i, j \in X$, let (ij) denote the map defined for all $k \in X$ by

$$k(ij) = \begin{cases} j & \text{if } k = i; \\ i & \text{if } k = j; \\ k & \text{if } k \neq i \text{ and } k \neq j. \end{cases}$$

Then $(ij) \in S_n$ and is called a *transposition*. Show that any $\alpha \in S_n$ can be expressed as a product of transpositions. α is called an *even* [*odd*] permutation if α can be written as the product of an even [odd] number of transpositions. Show further that any $\alpha \in S_n$ is either an even permutation or an odd permutation (but not both) and that the set $\boldsymbol{A}_n$ of all even permutations is a subgroup of index two in S_n. $\boldsymbol{A}_n$ is called the *alternating group* of degree n. Find $\boldsymbol{A}_2$ and $\boldsymbol{A}_3$.

6.6. Let $j_t \in X = \{1, \ldots, n\}$, $t = 1, 2, \ldots, r$. The *r-cycle* $(j_1, \ldots, j_r)$ is defined as the permutation $\alpha \in S_n$ such that for any $k \in X$,

$$k\alpha = \begin{cases} j_{t+1} & \text{if } k = j_t \quad \text{for } 1 \leq t < r; \\ j_1 & \text{if } k = j_r; \\ k & \text{if } k \neq j_t \quad \text{for any } t \text{ with } 1 \leq t \leq r. \end{cases}$$

Two cycles $(j_1, \ldots, j_r)$ and $(i_1, \ldots, i_s)$ are said to be disjoint if the sets $\{j_1, \ldots, j_r\}$ and $\{i_1, \ldots, i_s\}$ are disjoint. Show that every permutation can be factorized uniquely as a product of disjoint cycles. Show also that the set of all 3-cycles generates the alternating group $\boldsymbol{A}_n$.

6.7. Call a group G to be *simple* if it does not have a proper, non-trivial normal subgroup. Show that $\boldsymbol{A}_4$ is not simple and $\boldsymbol{A}_n$ is simple if $n \neq 4$.

6.8. Prove the following:

$\mathbb{R}^+$ is a subgroup of $\mathbb{R}^*$ under multiplication and that the map $Exp_a : x \mapsto a^x$ is an isomorphism of $(\mathbb{R}, +)$ onto $(\mathbb{R}^+, \cdot)$ for any $a \in \mathbb{R}^+ - \{1\}$. Find the inverse of Exp_a.

The additive group $\Bbbk$ has no non-trivial finite subgroup for $\Bbbk = \mathbb{C}, \mathbb{R}, \mathbb{Q}$ or $\mathbb{Z}$.

The only non-trivial finite subgroup of the multiplicative group $\mathbb{R}$ is $\{-1, 1\}$.

For every $n \in \mathbb{N}$, there is a subgroup of order n contained in the multiplicative group $\mathbb{C}^*$.

H is a subgroup of the additive group $\mathbb{Z}$ if and only if $H = n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ for some $n \in \mathbb{N}$.

6.9. Let $\boldsymbol{Sg}(G)$ denote the set of all subgroups of a group G. Prove the following:

Prove that $\boldsymbol{Sg}(G)$ is a partially ordered by inclusion with the smallest member $\{e\}$ (e is the identity of G) and the largest member G.

Let $\mathcal{H} \subseteq \boldsymbol{Sg}(G)$ and $\bigcap \mathcal{H} = H$. Then prove that $H = \wedge\mathcal{H}$ is the greatest lower bound of $\mathcal{H}$.

Prove that there is a subgroup $K = \vee\mathcal{H}$ with the property:

$H \subseteq K$ for all $H \in \mathcal{H}$; and

if $K' \in \boldsymbol{Sg}(G)$ with $H \subseteq K'$ for all $H \in \mathcal{H}$, then $K \subseteq K'$.

If $\boldsymbol{Ng}(G)$ denote the set of all normal subgroups of G, prove that $\boldsymbol{Ng}(G)$ is a partially ordered subset of $\boldsymbol{Sg}(G)$ containing the smallest and the largest ($\{e\}$ and G respectively). Further if $\mathcal{H} \subseteq \boldsymbol{Ng}(G)$, then $\vee\mathcal{H}, \wedge\mathcal{H} \in \boldsymbol{Ng}(G)$.

6.10. Show that elements of the group S_3 of all permutations (or bijections of the 3-element set $\{0, 1, 2\}$ can be represented as

$$S_3 = \{1, \rho, \rho^2, \sigma, \tau, \mu\}$$

where 1 denote the identity map on the set,

$$\rho = (012), \quad \sigma = (01), \quad \tau = (02), \quad \mu = (12).$$

Here we have written (012) for the cyclic permutation which sends $0 \to 1 \to 2 \to 0$ and the remaining are transpositions that interchange the symbols. Show that $H = \{1, \sigma\}$ is a subgroup of S_3 such that $H\rho = \{\rho, \tau\}$ and $\rho H = \{\rho, \mu\}$.

6.11. Let N be a normal subgroup of the group G and $Na, Nb \in G/N$. Prove that the set product $(Na)(Nb)$ is the coset Nab and that the product $(Na) \cdot (Nb)$ defined on G/N in Theorem **??** can be identified with the set product.

6.12. Let $n \in \mathbb{N}$ and for each $i \in \mathbb{N}$, let $[i] = i + n\mathbb{Z}$. Then show that $[i] = [j]$ if and only if $i - j$ is divisible by n and so, the set of distinct cosets of the subgroup $n\mathbb{Z}$ in $\mathbb{Z}$ are

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

With addition of cosets defined by $[i] + [j] = [i + j]$, show that $\mathbb{Z}_n$ becomes a group isomorphic to $\mathbb{Z}/n\mathbb{Z}$. $\mathbb{Z}_n$ is called the cyclic group of integers modulo n.

Furthermore, with multiplication defined by $[i][j] = [ij]$ (modulo n) show that $\mathbb{Z}_n$ becomes a finite commutative ring with identity and the map $q_n : i \mapsto [i]$ is a ring homomorphism of the ring $\mathbb{Z}$ of integers onto $\mathbb{Z}_n$. Verify that $\mathbb{Z}_n$ is a field if and only if n is prime.

6.13. Prove Proposition 6.3.1.

6.14. Prove that Equation (**??**) defines a right action of the group G on itself. Prove the following:

The conjugacy class C_z of $z \in G$ contains exactly one element z if and only if z commutes with every element in G.

$Z(G) = \{z \in G : C_z = \{z\}\}$ is a normal subgroup of G. $Z(G)$ is called the *centre* of G.

For each $x \in G$, let $N(x) = \{y : xy = yx\}$, show that $N(x)$ is a subgroup of G and that there is a bijection of $G \wr N(x)$ onto C_x. In particular, if G is finite, then $|C_x|$ divides $o(G)$.

If G is a finite group, prove that the following *Class Equation* holds:

$$o(G) = o(Z(G)) + \sum_{\alpha} C_\alpha$$

where $\{C_\alpha\}$ denotes the set of all nontrivial conjugacy classes of G.

6.15. A *commutator* in a group G is an element which can be written in the form $aba^{-1}b^{-1}$ for $a, b \in G$. The group G' generated by the set of all commutators is called the *commutator subgroup* of G. Prove the following:

G' is the set of all finite products of commutators in G.

G' is a normal subgroup of G.

The quotient group $\boldsymbol{Ab}(G) = G/G'$ is abelian.

If $\phi : G \to H$ is any homomorphism of G to an abelian group H, then there exists a unique homomorphism $\bar{\phi}$ of $\boldsymbol{Ab}(G)$ to H such that

$$\phi = q \circ \bar{\phi}$$

where $q : G \to \boldsymbol{Ab}(G)$ is the quotient homomorphism.

Verify that, if $G = S_3$, then the commutator subgroup of G is isomorphic to $\mathbb{Z}_3$, the cyclic group of order 3 and that $\boldsymbol{Ab}(S_3) = \mathbb{Z}_2$.

6.16. Let $\mathcal{G} = \{G_\lambda : \lambda \in \Lambda\}$ be a family of groups. A word over $X = \cup_{\lambda\in\Lambda} G_\lambda$ is a finite sequence of elements in X. We indicate a word $w = a_1 a_2 \ldots a_n$ by juxtaposition of its alphabets $a_i \in X$ and the set of all words over X by F_X. We define an *elementary reduction* among words as follows: let $w, w' \in F_X$. Then w' is obtained from w by an elementary reduction if

w' is obtained from w by replacing two adjacent alphabets a_{i-1}, a_i in w belonging to the same group G_λ by their product $a_{i-1}a_i = c$ in G_λ; or

w' is obtained from w by deleting an alphabet $a_i \in G_\lambda$ which is the identity of G_λ.

We shall write

$$w \leftrightarrow w'$$

if either $w = w'$ or one of them is obtained from the other by an elementary reduction. Clearly $\leftrightarrow$ defines a reflexive and symmetric relation and so, its transitive closure is an equivalence relation which we denote by $\sim$. For $w \in F_X$, let $[w]$ denote the $\sim$-class of w. Then show that

$$K = F_X/\sim = \{[w] : w \in F_X\}$$

is a group with respect to the binary operation defined by

$$[w_1][w_2] = [w_1 w_2], \quad w_1, w_2 \in F_X.$$

For each $a \in G_\lambda$, $\lambda \in \Lambda$, there is a unique word in F_X whose only alphabet is a. We denote this word also by a. Then the map $j_\lambda : a \mapsto [a]$ is clearly an injective homomorphism of the group G_λ into K. Prove that

$$(K, \{j_\lambda\}) = \coprod_{\lambda\in\Lambda} G_\lambda$$

is the coproduct of the given family of groups with respect to the set of injections $\{j_\lambda\}$ defined above. Show that the coproduct is not abelian even if all groups G_λ are abelian.

6.17. Let $\mathcal{H} = \{H_\alpha : \alpha \in \Omega\}$ be a family of abelian groups and let

$$G = \coprod_{\alpha\in\Omega} H_\alpha \quad \text{and} \quad H = \bigoplus_{\alpha\in\Omega} H_\alpha.$$

Show that

$$H = G/G' = \boldsymbol{A}b(G)$$

where G' (as in Exercise 6.15) denotes the commutator subgroup of G.

6.18. Let G and H be groups and let $\mu : G \to \operatorname{aut} H;\ g \mapsto \mu_g$ be a homomorphism. For convenience, for each $g \in G$ and $h \in H$, we write h^g for $h\mu_g$. Let K denote the set $G \times H$ with binary operation defined by

$$(g, h)(g', h') = (gg', h^{g'} h').$$

The binary operation is associative since one easily computes using the homomorphism property of μ that

$$((g_1, h_1)(g_2, h_2))(g_3, h_3) = ((g_1g_2)g_3, h_1^{g_1g_2} h_2^{g_3} h_3)$$
$$(g_1, h_1)((g_2, h_2)(g_3, h_3)) = (g_1(g_2g_3), h_1^{g_1g_2} h_2^{g_3} h_3).$$

Also if e_G and e_H denote identities of G and H respectively, show that (e_G, e_H) is the identity in K and that (g^{-1}, k) is the inverse of $(g, h) \in K$ if

$$k = (h^{-1})^{g^{-1}}.$$

Deduce that K is a group such that the maps

$$p : (g, h) \mapsto g \quad \text{and} \quad j : g \mapsto (g, e_H)$$

are homomorphisms of K onto G and G into K respectively such that

$$j \circ p = 1_G.$$

We call $K = G \times_\mu H$, the *semidirect product* of G and H with respect to μ or a semidirect product of these groups. In some context, a semidirect product is also referred to as a *split extension* of G by H. If we choose μ as the trivial homomorphisms of G to $\operatorname{aut} H$ (that is, if $\mu_g = 1_H$ for all $g \in G$), then the semidirect product reduces to the direct product of G and H.

6.19. Prove that a group G is cyclic if and only if G is isomorphic to $\mathbb{Z}$ or isomorphic to $\mathbb{Z}_n$ for some $n \in \mathbb{N}^*$. Show also that $\mathbb{Z}$ is a free cyclic group and any cyclic group G which is not free has a presentation $G = \langle x : x^n = 1 \rangle$ for some $n \in \mathbb{N}^*$.

6.20. Show that the symmetric group S_3 of all permutations of a 3-element set $\{1, 2, 3\}$ has a presentation with two generators and three relations:

$$S_3 = \langle x, y : x^3 = y^2 = 1, \quad yx = x^2 y \rangle.$$

Prove also that the group having the following presentation

$$D_n = \langle x, y : x^n = y^2 = 1, \quad xyx = y \rangle$$

is a finite group of order $2n$ and that

$$D_n = \{x^i y^j : 0 \leq i < n; \quad 0 \leq j < 2\}.$$

Hence show that $D_3 = S_3$. Is this true for any $n > 3$?

6.21. An *endomorphism* of a group G is a homomorphism of G to itself. Let $\mathrm{End}(A)$ denote the set of all endomorphisms of an additive group A. For $h, g \in \mathrm{End}(A)$, let $h + g$ denote the map defined by:

$$a(h + g) = ah + ag \quad \text{for all} \quad a \in A.$$

Show that $h + g \in \mathrm{End}(A)$ and that $\mathrm{End}(A)$ additive group with respect to $+$. Moreover, show that $\mathrm{End}(A)$ is a ring with addition defined above and composition as multiplication.

Suppose that R is a ring and let $\mathrm{End}(R)_+$ denote the endomorphism ring of the additive group $(R, +)$ of R. Show that $\rho_s : t \mapsto ts$ is an endomorphism of $(R, +)$ and the right regular representation $\rho : R \to \mathrm{End}(R)_+$ is a homomorphism of rings.

References

Artin, M. (1990). *Algebra*, Prentice Hall, Engelwood Cliffs, N.J., U.S.A. Printed in India by special arrangement with Prentice Hall; Forth Printing: (December 1998).

Halmos, P.R. (1958). *Finite Dimentional Vector Spaces*, Van Nostrand, Princeton, New Jersey, 2^{nd} edition.

Herstein, I.N. (1975). *Topics in Algebra*, Wiley Eastern, New Delhi, second edition, November (1998), First published in 1964 by John Wiley and Sons, Fifth Wiley Eastern Reprint.

Kenneth Hoffman and Ray Kunze. (1971). *Linear Algebra*, Prentice Hall, Engelwood Cliffs, New Jersey. U.S.A.

Jacobson, N. (1984). *Basic Algebra, Volume 2,* W.H. Freeman, San Fransisco, 1984. Published in India by Hindustan Publishing Corporation, New Delhi, in 1984.