CHAPTER II

PRELIMINARIES

In this chapter we shall collect some definitions and results from topology and group theory which will be a basic requirement for our investigation. The materials of this chapter were extracted from references [2], [3], [4], [5]. We shall assume that the reader is familiar with common terms used in the set theory.

2.1 Algebraic Concepts

By a <u>group</u> we mean an ordered pair (G,o), where G is a non - empty set and o is a binany operation on G satisfying the following conditions :

(i) For all x, y, z of G, $xo(yoz) = (xoy)oz$

(ii) There exists an element e of G such that $eox = xoe = x$ for each x in G.

(iii) For each x in G, there is an element x^{-1} in G such that $xox^{-1} = e = x^{-1}ox$.

For convenience, we shall denote the group (G,o) simply by G. It can be shown that the element e in (ii) is unique, it is known as the <u>identity</u> of G. For each x in G, the element x^{-1} in (iii) is also unique. It is known as the <u>inverse</u> of x .

A group G is abelian or commutative, if and only if xoy = yox for all elements x, y of G. The number of elements in a group G shall be called the order of G and denoted by $|G|$. G is called finite or infinite as its order is finite or infinite. For any element x in G, the order of x is the least positive integer m such that $x^m = e$. If no such integer exists we say that x is of infinite order. If G is a group in which every element is of order 2, G is said to be a boolean group, otherwise, it is said to be a non-boolean group. A boolean group G of order 4 is also known as the Klein four group. It can be shown that any boolean group G is also abelian. If for each x in G there exists y in G such that x = yoy, G is said to be a 2-divisible group. A group H is a subgroup of G if and only if $H \subset G$ and the group operation of H is the restriction of that of G. It can be shown that any non-empty set H forms a subgroups of (G,o) if and only if $xoy^{-1} \in H$ for any x, y in H. If H is a subgroup of a group G and x, y are elements of G such that $xy^{-1} \in H$, we say that x is right congruent to y modulo H and denoted by $x \widetilde{HR}\, y$. If $x^{-1}y \in H$, we say that x is left congruent to y modulo H and denoted by $x \widetilde{HL}\, y$. If $\widetilde{HR}$ and $\widetilde{HL}$ are coincide we shall denote them by $\widetilde{H}$. It can be shown that left (right) congruence modulo H is an equivalence relation on G. The equivalence class of $x \in G$ under left(right) congruence modulo H is the set $xH = \{xh : h \in H\}$ $(Hx = \{hx : h \in H\})$, it is called a left(right) coset of H in G. It follows that $G = \bigcup xH = \bigcup Hx$ where the union is taken over all pairwise disjoint cosets. The number of distinct left(right) cosets of H in G is called the index of H in G and denoted by $[G:H]$. If H is a subgroup of G such that left and right congruence modulo H coincide, then H is said to be a normal subgroup of G. In an abelian group, each subgroup is normal. If H is a normal subgroup of a group G, then $G/\tilde{H}$ is a group of order $[G:H]$ under the binary operation given by $(xH)(yH) = xyH$, this group is called the quotient group of G by $\tilde{H}$, and will be denoted by G/H.

A mapping h on a group (G,o) into a group $(G,*)$ is said to be a homomorphism provided

$$h(xoy) = h(x) * h(y), \quad \text{for all } x,y \text{ in } G.$$

If h is bijective, h is called an isomorphism.

By a field we mean a triple $(F, +, \cdot)$, where $+, \cdot$ are two binary operations on F, known as addition and multiplication respectively, such that the followings hold :

(i) F forms a commutative group under addition.

(ii) $F^* = F - \{0\}$, where 0 is the additive identity forms a commutative group under multiplication.

(iii) For any $a,b,c \in F$, we have

$$a(b+c) = ab + ac .$$

For convenience, we shall denote a field $(F, +, .)$ simply by F. $(F, +)$ and $(F^*, .)$ will be refered to as the additive group and the multiplicative group of F, respectively. If there is a least positive integer n such that $na = 0$ for all $a \in F$, then F is said to have characteristic n. If no such n exists F is said to have characteristic zero. If K is any non - empty subset of a field $(F,+,.)$ such that K form a field under restriction of $+,.$ to $K \times K$, we say that $(K,+,.)$ is a subfield of $(F,+,.)$. If K is a subfield of F, we say that F is an extension field of K.

A function φ of a field F into a field K is a homomorphism provided that for all $a,b \in F$:

$$\varphi(a+b) = \varphi(a) + \varphi(b) \text{ and } \varphi(ab) = \varphi(a)\varphi(b) .$$

If φ is bijective, φ is called an isomorphism. If φ is an isomorphism of F into itself, φ is called an automorphism. If F is a field in which $a^2 \neq -1$ for any $a \in F$, let

$$C(F) = \{(a,b) : a \text{ and } b \text{ are elements of } F\}.$$

Define addition and multiplication on C(F) as follows :

$$(a, b) + (c, d) = (a + c, b + d) ,$$

and

$$(a, b)(c, d) = (ac - bd, ad + bc) .$$

It can be shown that $C(F)$ under the above addition and multiplication forms a field. This field contains $\bar{F} = \{(a,0) : a \in F\}$ as a subfield isomorphic to F. Hence we may veiw F as a subfield of $C(F)$. Observe that if we denote the element $(a,0)$ of F by a and denote $(0,1)$ by i, then each element (a,b) of $C(F)$ can be expressed as

$$\begin{aligned}(a, b) &= (a,0) + (b, 0)(0,1) \\ &= a + bi .\end{aligned}$$

Note that from the definition of i, we have $i^2 = (-1, 0) = -1$. It can be shown that the mapping $\varphi : C(F) \longrightarrow C(F)$ given by

$$\varphi(a+bi) = a - bi ,$$

is the unique automorphism of $C(F)$ fixing all elements of $\bar{F}$ and taking i into $-i$. Since $\bar{F}$ is isomorphic to F, hence we may veiw φ as the automorphism of $C(F)$ fixing all elements of F and taking i into $-i$. Let

$\Delta(F) = \{a + bi \in C(F) : (a + bi)\varphi(a + bi) = 1\}$.

It can be shown that $\Delta(F)$ forms a multiplicative subgroup of $C(F)^*$. To each field F, we **shall** associate a multiplicative group $M(F)$ as follows : if F contains an element i such that $i^2 = -1$, we let $M(F) = F^*$; if F contains no element i such that $i^2 = -1$, we let $M(F) = \Delta(F)$.

Lemma 2.1.1 Let G be a group, F be a field of characteristic different from 2 such that $a^2 \neq -1$ for any a in F. Let h be a homomorphism from G into $C(F)^*$. Then for each x in G,
$\frac{h(x) + h(x^{-1})}{2}$ and $\frac{h(x) - h(x^{-1})}{2i}$ belong to F if and only if h(x) belongs to $\triangle(F)$.

Proof Let φ be the automorphism of C(F) fixing all elements of F and taking i into -i .

Assume that $h : G \longrightarrow C(F)^*$ is a homomorphism such that $\frac{h(x) + h(x^{-1})}{2}$ and $\frac{h(x) - h(x^{-1})}{2i}$ belong to F .

Therefore

$$\frac{h(x) + h(x^{-1})}{2} = \varphi\left(\frac{h(x) + h(x^{-1})}{2}\right),$$

$$= \frac{\varphi(h(x)) + \varphi(h(x^{-1}))}{2},$$

thus ,

$$h(x) + h(x^{-1}) = \varphi(h(x)) + \varphi(h(x^{-1})) . \tag{2.1.1.1}$$

Also ,

$$\frac{h(x) - h(x^{-1})}{2i} = \varphi\left(\frac{h(x) - h(x^{-1})}{2i}\right),$$

$$= \frac{\varphi(h(x)) - \varphi(h(x^{-1}))}{-2i},$$

thus

$$(2.1.1.2) \qquad h(x) - h(x^{-1}) = \varphi(h(x^{-1})) - \varphi(h(x)).$$

It follows from (2.1.1.1) and (2.1.1.2) that

$$2h(x) = 2\,\varphi(h(x^{-1})) .$$

Hence $\quad h(x) \cdot \varphi(h(x)) = 1 .$

Therefore $\quad h(x)$ belongs to $\Delta(F)$.

Conversely, assume that h is a homomorphism from G into $\Delta(F)$.

Hence $h(x) \cdot \varphi(h(x)) = 1$ for all x in G . It follows that

$$\varphi(h(x)) = h(x)^{-1} = h(x^{-1}) .$$

Let $h(x) = a + bi$ where $a, b \in F$. Therefore,

$$\frac{h(x) + h(x^{-1})}{2} = \frac{h(x) + \varphi(h(x))}{2}$$

$$= \frac{(a + bi) + (a - bi)}{2}$$

$$= a ,$$

and

$$\frac{h(x) - h(x^{-1})}{2i} = \frac{h(x) - \varphi(h(x))}{2i}$$

$$= \frac{(a + bi) - (a - bi)}{2i}$$

$$= b .$$

Hence $\frac{h(x) + h(x^{-1})}{2}$ and $\frac{h(x) - h(x^{-1})}{2i}$ belong to F .

Let (F, +, .) be a field and (V, +) be a commutative group with a rule of multiplication which assigns to any $a \in F$, $u \in V$, a product $au \in V$. Then V is called a vector space ever F if the following axioms hold :

1) For any $a \in F$ and any $u, v \in V$, $a(u+v) = au + av$.

2) For any $a, b \in F$ and any $u \in V$, $(a+b)u = au + bu$.

3) For any $a, b \in F$ and any $u \in V$, $a(bu) = (ab)u$.

4) For $v \in V$, $1v = v$ where 1 is the multiplicative identily of F.

The elements of F and V will be refered to as scalars and vectors, respectively. If V is a vector space over the field F and $\{x_i\}$ $(1 \leq i \leq n)$ is a finite subset of V, then for $a_i \in F$, $1 \leq i \leq n$, $\sum_{i=1}^{n} a_i x_i$ is called a linear combination of the x_i . The vectors $x_1, \ldots, x_n \in V$ are said to be linearly dependent over F, or simply dependent, if there exist scalars $a_1, \ldots, a_n \in F$, not all of them zero, such that $\sum_{i=1}^{n} a_i x_i = 0$. An arbitrany set A of vectors is said to be a linearly dependent set if some finite subset of A is linearly dependent. Otherwise, the set A is called linearly independent or simply independent. If $\mathcal{B}$

is a linearly independent subset of V such that for every $v \in V$, v can be written as a linear combination of vectors in $\mathcal{B}$, we say that $\mathcal{B}$ is a basis of V. It can be shown that every vector in V has a unique representation as a linear combination of elements of any basis $\mathcal{B}$.

Observe that the set $\mathbb{R}$ of real numbers can be considered as a vector space over the field $\mathbb{Q}$ of rational numbers. It can be shown that $\mathbb{R}$ has a basis over $\mathbb{Q}$. Such a basis is known as a Hamel basis. A proof of the existence of such a basis is given in [6].

2.2 Topological Concepts

Let X be a set and $\mathfrak{J}$ be a collection of subsets of X. The collection $\mathfrak{J}$ is called a topology on X provided $\mathfrak{J}$ satisfies the following conditions :

a) X and $\emptyset$ are elements of $\mathfrak{J}$.

b) The intersection of any two members of $\mathfrak{J}$ is in $\mathfrak{J}$.

c) The arbitrary union of members of $\mathfrak{J}$ is in $\mathfrak{J}$.

If $\mathfrak{J}$ is a topology on a set X, then $(X, \mathfrak{J})$ is said to be a topological space. Occasionally, we shall denote any topological space $(X, \mathfrak{J})$ simply by X. The members of $\mathfrak{J}$ are called $\mathfrak{J}$ - open sets of X, or simply open sets of X. If a topogical space X has the property that for any x, y in X there exist open sets O_1, O_2 such that $x \in O_1$, $y \in O_2$ and

$x \notin O_2$, $y \notin O_1$, we say that X is a T_1 - space. For any topological space $(X, \mathfrak{J})$, it can be shown that if Y is any subset of X, then the family $\mathfrak{J}_y = \{T \cap y : T \in \mathfrak{J}\}$ is a topology on Y; it is called the <u>relative topology</u> of Y and the topological space $(Y, \mathfrak{J}_y)$ is called a <u>subspace</u> of $(X, \mathfrak{J})$

A subcollection $\mathcal{B}$ of a topology $\mathfrak{J}$ is said to be a base of $\mathfrak{J}$ provided the following condition hold : for each $T \in \mathfrak{J}$ and $x \in T$, there exists $B \in \mathcal{B}$ such that $x \in B \subset T$, or equivalently, each T in $\mathfrak{J}$ is a union of members of $\mathcal{B}$. It can be shown that if a family $\mathcal{B}$ of subsets of a set X has the properties ;

(i) the union of sets in $\mathcal{B}$ is in X,

(ii) for each $B_1, B_2 \in \mathcal{B}$, $B_1 \cap B_2$ is the union of members of $\mathcal{B}$, then $\mathcal{B}$ is a base for some topology for X. This topology consists of all sets that can be written as unions of sets in $\mathcal{B}$. Observe that the family of all open intervals form a base for a topology on the set $\mathbb{R}$ of real numbers. This topology is known as the <u>usual topology</u> on $\mathbb{R}$.

A subfamily $\mathcal{S}$ of $\mathfrak{J}$ is a <u>subbase</u> of the topology $\mathfrak{J}$ on X if and only if the set of all finite intersections of members of $\mathcal{S}$ form a base for $\mathfrak{J}$.

Let $\{X_\alpha : \alpha \in A\}$ be a family of sets. $X = \prod_{\alpha \in A} X_\alpha$ denotes the set of all mappings $x: A \longrightarrow \bigcup_{\alpha \in A} X_\alpha$ such that

$x(\alpha) \in X_\alpha$ for each $\alpha \in A$. X is called the Cartesian product or product of X_α's. For each $x \in X$ and each $\alpha \in A$, $x(\alpha)$ is called the α-th coordinate of x. We shall denote $x(\alpha)$ by x_α. The mapping $P_\alpha : X \longrightarrow X_\alpha$ defined by $P_\alpha(x) = x_\alpha$, is called the α - th projection. It can be seen that P_α is a mapping from X onto X_α. If $\{ X_\alpha : \alpha \in A \}$ is a family of topological spaces, then the family of sets of the form $P_\alpha^{-1}(T_\alpha)$, where T_α is a $\mathfrak{T}_\alpha$ - open set, forms a subbase of a topology $\mathfrak{T}$ for the product $\prod_{\alpha \in A} X_\alpha$. This topology is known as the product topology. The topological space $(\prod_{\alpha \in A} X_\alpha , \mathfrak{T})$ will be called the product space of $\{ X_\alpha : \alpha \in A \}$.

Let X and Y be two topological spaces. A mapping f of X into Y is said to be continuous if for each open set V in Y, $f^{-1}[V] = \{ x \in X : f(x) \in V \}$ is an open set of X. If for each open set U in X, $f(U) = \{ f(x) : x \in U \}$ is an open set of Y, f is said to be open.

Let X be a topological space, R be an equivalence relation on X and $Y = X/R$ be the quotient set of X with respect to the relation R. The mapping $\varphi : X \longrightarrow Y$ defined by $\varphi(x) = \bar{x}$, where $\bar{x}$ denotes the equivalence class of x, will be called the canonical mapping. It can be shown that the family $\mathfrak{T}_\varphi = \{ V \subset Y : \varphi^{-1}(V) \text{ is open} \}$ is a topology on Y ;

it is called the quotient topology and $(Y, \mathfrak{T}_\varphi)$ is called the quotient space of X by R .

2.3 Topological Groups

A triple $(G, o, \mathfrak{T})$ is a topological group if and only if (G, o) is a group, $(G, \mathfrak{T})$ is a topological space and the function whose value at a member (x, y) of $G \times G$ is xoy^{-1} is continuous relative to the product topology for $G \times G$. We sometimes say "G is a topological group" .

The followings are examples of topological groups :

(a) The set $\mathbb{R}$ of real numbers with addition as the group operation and the usual topology form a topological group.

(b) The set $\mathbb{Z}$ of integers with addition as the group operation and the relative topology of the usual topology of $\mathbb{R}$ form a topological group.

(c) The set $\mathbb{R}^*$ of nonzero real numbers with multiplication as the group operation and the relative topology of the usual topology of $\mathbb{R}$ form a topological group .

(d) The set $\mathbb{R}^+$ of positive real numbers with multiplication as the group operation and the relative topology of the usual topology of $\mathbb{R}$ form a topological group.

(e) The set $\mathbb{R}^n$ of all real n-tuples with an addition as the coordinate addition and the usual topology of $\mathbb{R}$ form a topological group.

(f) A **complex** number can be considered as an ordered pair of real numbers. Hence the usual topology on $\mathbb{C}$, the set of complex numbers, shall mean the usual topology on $\mathbb{R}^2$. The set $\mathbb{C}$ of complex numbers with addition as a group operation and the usual topology on $\mathbb{C}$ form a topological group

(g) The set $\mathbb{C}^*$ of nonzero complex numbers with complex multiplication as a group operation and the relative topology of the usual topology of $\mathbb{C}$ form a topological group.

(h) The unit circle $\triangle = \{ z \in \mathbb{C} : |z| = 1 \}$ with complex multiplication as the group operation and the relative topology of the usual topology of $\mathbb{C}$ form a topological group .

If H is a subgroup of G, H endowed with the relative topology is a topological group ; it is called a topological subgroup or simply a subgroup of G . If H is a normal subgroups of G, then $G/_H$, the quotient group with respect to the equivalence relation $\tilde{H}$, and the quotient topology form a topological group ; it is called the quotient group of G by $\tilde{H}$. It can be shown that H is open if and only if each coset of H is open.

If φ is the canonical mapping of G onto $G/_H$, it can be shown that φ is an open continuous homomorphism of G onto $G/_H$. The following is a fact about continuous homomorphism. We state this fact for later refference, and it can be seen in [1].

Theorem 2.3.1 Every continuous homomorphism of $\mathbb{R}$ into $\mathbb{R}/\mathbb{Z}$ is of the form $x \longmapsto \varphi(ax)$ where $a \in \mathbb{R}$ and $\varphi : \mathbb{R} \longrightarrow \mathbb{R}/\mathbb{Z}$ is the canonical mapping .

2.4 Topological Fields.

A topological field is a quadruple $(F, +, \cdot, \mathfrak{J})$ such that $(F, +, \cdot)$ is a field, $(F, +, \mathfrak{J})$ and $(F^*, \cdot, \mathfrak{J}_{F^*})$ are topological groups where $\mathfrak{J}_{F^*}$ is the topology induced by $\mathfrak{J}$ on F^*. We sometimes say "F is a topological field ". If F is a topological field in which $a^2 + 1 \neq 0$ for all $a \in F$, then C(F) endowed with the product topology is a topological field. It can be shown that the multiplicative subgroup $\triangle(F)$ with the relative topology form a topological group.

2.5 Topological Vector Spaces.

A topological vector space is the vector space V over the field F of real or complex numbers and a topology $\mathfrak{J}$ on V such that the function $f : V \times V \longrightarrow V$ and $g : F \times V \longrightarrow V$ defined by $f(x, y) = x+y$ and $g(\lambda, x) = \lambda x$, are continuous, where the topology on F is the usual topology. The topology $\mathfrak{J}$ is said to be a vector topology.