1.A Appendix to Chapter 1

1.A.1 The Algebraic Structures of Groups, Fields and Rings

Definition:
The nonempty set *G* with a binary operation, that is, to each pair of elements $a, b \in G$ there is assigned an element $ab \in G$, is called a **group** if the following axioms hold:

1. *associative law*: $(ab)c = a(bc)$ for any $a, b, c \in G$
2. *identity element*: there exists an element $e \in G$, called the identity element, such that $ae = ea = a$
3. *inverse*: for each $a \in G$, there exists an element $a^{-1} \in G$, called the inverse of *a*, such that $aa^{-1} = a^{-1}a = e$

<u>Examples</u>:

(a) An example of a group is the set of integers under addition. In this case the binary operation is denoted by +, as in $a + b$; one has (1) addition is associative, $(a+b)+c$ equals $a+(b+c)$, (2) the identity element is denoted by 0, $a + 0 = 0 + a = a$, (3) the inverse of *a* is denoted by *a*, called the *negative* of *a*, and $a + (-a) = (-a) + a = 0$

Definition:
An **abelian group** is one for which the commutative law holds, that is, if $ab = ba$ for every $a, b \in G$.

<u>Examples</u>:

(a) The above group, the set of integers under addition, is commutative, $a + b = b + a$, and so is an abelian group.

Definition:
A mapping *f* of a group *G* to another group G', $f : G \to G'$, is called a **homomorphism** if $f(ab) = f(a) f(b)$ for every $a, b \in G$; if *f* is bijective (one-one and onto), then it is called an **isomorphism** and *G* and G' re said to be **isomorphic**

Definition:
If $f : G \to G'$ is a homomorphism, then the **kernel** of *f* is the set of elements of *G* which map into the identity element of G', $k = \{a \in G \mid f(a) = e'\}$

<u>Examples</u>

(a) Let *G* be the group of non-zero complex numbers under multiplication, and let G' be the non-zero real numbers under multiplication. The mapping $f : G \to G'$ defined by $f(z) = |z|$ is a homomorphism, because

$$f(z_1 z_2) = |z_1 z_2| = |z_1||z_2| = f(z_1) f(z_2)$$

The kernel of *f* is the set of elements which map into 1, that is, the complex numbers on the unit circle

Definition:
The non-empty set A with the two binary operations of addition (denoted by +) and multiplication (denoted by juxtaposition) is called a **ring** if the following are satisfied:

1. *associative law for addition*: for any $a, b, c \in A$, $(a+b)+c = a+(b+c)$
2. *zero element* (additive identity): there exists an element $0 \in A$, called the zero element, such that $a + 0 = 0 + a = a$ for every $a \in A$
3. *negative* (additive inverse): for each $a \in A$ there exists an element $-a \in A$, called the negative of a, such that $a + (-a) = (-a) + a = 0$
4. *commutative law for addition*: for any $a, b \in A$, $a + b = b + a$
5. *associative law for multiplication*: for any $a, b, c \in A$, $(ab)c = a(bc)$
6. *distributive law of multiplication over addition* (both left and right distributive): for any $a, b, c \in A$, (i) $a(b+c) = ab + ac$, (ii) $(b+c)a = ba + ca$

Remarks:

(i) the axioms 1-4 may be summarized by saying that A is an abelian group under addition

(ii) the operation of **subtraction** in a ring is defined through $a - b \equiv a + (-b)$

(iii) using these axioms, it can be shown that $a0 = 0a = 0$, $a(-b) = (-a)b = -ab$, $(-a)(-b) = ab$ for all $a, b \in A$

Definition:
A **commutative ring** is a ring with the additional property:

7. *commutative law for multiplication*: for any $a, b \in A$, $ab = ba$

Definition:
A **ring with a unit element** is a ring with the additional property:

8. *unit element* (multiplicative identity): there exists a nonzero element $1 \in A$ such that $a1 = 1a = a$ for every $a \in A$

Definition:
A commutative ring with a unit element is an **integral domain** if it has no zero divisors, that is, if $ab = 0$, then $a = 0$ or $b = 0$

Examples:

(a) the set of integers Z is an integral domain

Definition:
A commutative ring with a unit element is a **field** if it has the additional property:

9. *multiplicative inverse*: there exists an element $a^{-1} \in A$ such that $aa^{-1} = a^{-1}a = 1$

Remarks:

(i) note that the number 0 has no multiplicative inverse. When constructing the real numbers R, 0 is a special element which is not allowed have a multiplicative inverse. For this reason, division by 0 in R is indeterminate

Examples:

(a) The set of real numbers R with the usual operations of addition and multiplication forms a field

(b) The set of ordered pairs of real numbers with addition and multiplication defined by

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

is also a field - this is just the set of complex numbers C

1.A.2 The Linear (Vector) Space

Definition:

Let F be a given field whose elements are called *scalars*. Let V be a non-empty set with rules of addition and scalar multiplication, that is there is a *sum* $a+b$ for any $a, b \in V$ and a *product* αa for any $a \in V$, $\alpha \in F$. Then V is called a **linear space** over F if the following eight axioms hold:

1. *associative law for addition*: for any $a, b, c \in V$, one has $(a+b)+c = a+(b+c)$
2. *zero element*: there exists an element $0 \in V$, called the zero element, or origin, such that $a+0=0+a=a$ for every $a \in V$
3. *negative*: for each $a \in V$ there exists an element $-a \in V$, called the negative of *a*, such that $a+(-a)=(-a)+a=0$
4. *commutative law for addition*: for any $a, b \in V$, we have $a+b=b+a$
5. *distributive law, over addition of elements of V*: for any $a, b \in V$ and scalar $\alpha \in F$, $\alpha(a+b)=\alpha a+\alpha b$
6. *distributive law, over addition of scalars*: for any $a \in V$ and scalars $\alpha, \beta \in F$, $(\alpha+\beta)a=\alpha a+\beta a$
7. *associative law for multiplication*: for any $a \in V$ and scalars $\alpha, \beta \in F$, $\alpha(\beta a)=(\alpha\beta)a$
8. *unit multiplication*: for the unit scalar $1 \in F$, $1a=a$ for any $a \in V$.