CHAPTER I

PRELIMINARIES

The purpose of this chapter is to summarize the necessary background materials of abstract algebra needed as a basic reference for the remaining ones. However, for the most part definitions and theorems are stated without proofs which can be found in references [6] , [7] , [8], [9], [10] ,[11] .

IDEALS

Definition 1-1 A nonempty subset I of a ring R is said to be a (two-sided) ideal of R if

i) $a,b \in I$ imply $a - b \in I$, and

ii) for every $a \in I$ and $r \in R$ both ar and ra are in I.

Theorem 1-1 Let $\{I_i\}$ be an arbitrary collection of ideals of a ring R, where i ranges over some index set. Then $\bigcap I_i$ is also an ideal of R. (For proof see [6]).

Definition 1-2 The ideal generated by a nonempty subset S of a ring R is the ideal which is the intersection of all ideals of R containing S and is denoted by (S), that is,

$$(S) = \bigcap \{I \mid S \subseteq I \text{ ; } I \text{ is an ideal of } R\} .$$

This definition is well-defined, since the entiring ring R itself is an ideal containing any subset of R; thus the set (S) exists and satisfies $S \subseteq (S)$, and by virtue of theorem 1-1 (S) forms an ideal. It is noteworthy that whenever I is any ideal of R with $S \subseteq I$, then necessarily $(S) \subseteq I$. For this reason, one often speaks of (S) as being the smallest ideal of R containing S.

<u>Theorem 1-2</u> Let R be a commutative ring with identity 1 and S be a nonempty subset of R, then the ideal of R generated by S is the set of all elements of the form

$$\sum_{i=1}^{n} r_i x_i$$

for $r_i \in R$, $x_i \in S$ and $n \geq 1$.

<u>Proof</u> For convenience, set

$$\overline{S} = \{ \sum_{i=1}^{n} r_i x_i \mid r_i \in R,\ x_i \in S \} .$$

What we must prove is $(S) = \overline{S}$. Let $x \in S$, hence $x \in (S)$, and since (S) is an ideal, $rx \in (S)$ for any $r \in R$, and thus $\sum_{i=1}^{n} r_i x_i \in (S)$. So we can conclude that $\overline{S} \subseteq (S)$. On the other hand, $S \subseteq \overline{S}$ since if $x \in S$, then $x = 1.x \in \overline{S}$. It remains to prove that $\overline{S}$ is an ideal so that $\overline{S}$ is an ideal containing S, and using the fact that (S) is the smallest ideal containing S, we have $(S) \subseteq \overline{S}$ implying that $(S) = \overline{S}$. To prove that $\overline{S}$ is an ideal, let $a, b \in \overline{S}$, then a and b are of the form

$a = \sum_{i=1}^{n} a_i x_i$, $b = \sum_{i=1}^{m} b_i y_i$, for $a_i, b_i \in R$, $x_i, y_i \in S$.

Hence

$$a - b = \sum_{i=1}^{n} a_i x_i - \sum_{i=1}^{m} b_i y_i .$$

That is, a - b is of the form $\sum_{i=1}^{k} r_i z_i$ where $r_i \in R$, $z_i \in S$, and thus $a - b \in \overline{S}$. For any $r \in R$,

$$ra = \sum_{i=1}^{n} ra_i x_i = \sum_{i=1}^{n} s_i x_i$$

where $s_i = ra_i \in R$, so $ra \in \overline{S}$ implying that $\overline{S}$ is an ideal. This completes the proof.

Remark If S consists of a finite number of elements, say $a_1, a_2, \ldots, a_n$, then the ideal which they generate is customarily denoted by $(a_1, a_2, \ldots, a_n)$. Such an ideal is said to be finitely generated with the given elements $a_1, a_2, \ldots, a_n$ as its generators. That is,

$$(a_1, a_2, \ldots, a_n) = \{r_1 a_1 + r_2 a_2 + \ldots + r_n a_n \mid r_i \in R, 1 \leq i \leq k\}.$$

Definition 1-3 An ideal I of the ring R is a prime ideal if for all a,b in R, $ab \in I$ implies that $a \in I$ or $b \in I$.

Definition 1-4 An ideal P in a ring R is called perfect if P contains an element of R whenever it contains some power of that element : $a^t \in P$ implies $a \in P$.

Theorem 1-3 Let

$$I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

be an ascending chain of ideals of a ring R. Then $\bigcup_{i=1}^{\infty} I_i$ is also an ideal of R. Furthermore, if it is an ascending chain of prime ideals, then $\bigcup_{i=1}^{\infty} I_i$ is a prime ideal in R.

<u>Proof</u> Let $I = \bigcup_{i=1}^{\infty} I_i$ and $a,b \in I$. Then $a \in I_i$ and $b \in I_j$ for some i and j. Now one of the ideals I_i and I_j contains the other, and so we may choose $\ell = \max\{i,j\}$ so that a and b belong to I_ℓ. Then $a - b$ belongs to I_ℓ, and so to I. Let $a \in I$ and $r \in R$. Then $a \in I_s$ for some s. Since I_s is an ideal, ra and ar belong to I_s and hence belong to I. Therefore I is an ideal. If each I_n is a prime ideal, we shall prove that I is also a prime ideal. Let $ab \in I$, then $ab \in I_k$ for some k. Since I_k is a prime ideal, $a \in I_k$ or $b \in I_k$. Thus $a \in I$ or $b \in I$. Therefore I is a prime ideal.

Polynomial Rings

<u>Definition 1-5</u> Let R be a ring. By the <u>polynomial ring over R</u> in one indeterminate X, written as $R[X]$, we mean the set of all elements of the form

$$f(X) = a_o + a_1 X + \dots + a_n X^n ,$$

where n can be any nonnegative integer and where the coefficients a_o, a_1, ..., a_n are all in R. Such elements are called <u>polynomials over R.</u>

If $a_n \neq 0$, we call a_n the <u>leading coefficient</u> of f(x), and the integer n is called the <u>degree</u> of the polynomial.

If $a \in R$ we can define

$$f(a) = \sum_{n=o}^{k} a_n a^n$$

and if $f(a) = 0$, we call the element a <u>a root</u> or a <u>zero</u> of the polynomial f(X).

<u>Definition 1-6</u> If $f(X) = a_o + a_1X + \dots a_mX^m$ and $g(X) = b_o + b_1X + \dots b_nX^n$ are both in $R[X]$ then

i) $f(X) + g(X) = c_o + c_1X + \dots c_tX^t$

where for each i, $c_i = a_i + b_i$

ii) $f(X)g(X) = c_o + c_1X + \dots + c_kX_k$

where $c_t = a_tb_o + a_{t-1}b_1 + a_{t-2}b_2 + \dots a_ob_t$.

<u>Definition 1-7</u> Let R be a ring with identity 1, a polynomial whose leading coefficient is 1 is said to be a <u>monic polynomial</u>.

<u>Theorem 1-4</u> (Division Algorithm)

Let F be a field and f(x), g(x) $\neq 0$ polynomials in $F[X]$. Then there exist unique polynomials t(X) and r(X) in $F[X]$ such that

$$f(X) = t(X)g(X) + r(X)$$

where either r(X) = 0 or deg r(X) < deg g(X).

(For proof see [7])

<u>Theorem 1-5</u> Let R be an integral domain and $R[X]$ the polynomial ring over R. Let f(X) and g(X) be two polynomials in $R[X]$ of respectively degrees m and n, let k = max (m - n + 1,0) and b_n be the leading coefficient of g(X). Then there exist unique polynomials g(X) and r(X) such that

$$b_n^k f(X) = q(X)\ g(X) + r(X)$$

where r(X) is either of degree less than n or is zero.

<u>Proof</u> If m < n, there is nothing to prove since we take k = o, q(X) = o, r(X) = f(X) and we certainly have that

$$f(X) = 0.g(X) + f(X).$$

Consider the case $m \geq n$, let $d = m - n \geq 0$, We can write $f(X) = a_o + a_1X + \dots a_mX^m$ and $g(X) = b_o + b_1X + \dots + b_nX^n$ where a_m, $b_n \neq 0$. The existence proof is by induction on d, if $d = 0$, we have

$$b_nf(X) = a_ng(X) + (a_{n-1}b_n - a_nb_{n-1})X^{n-1} + (a_{n-2}b_n - a_nb_{n-2})X^{n-2} + \dots + a_ob_n - a_nb_o .$$

So we have proven the theorem if $d = 0$, therefore we can assume that the theorem holds for all polynomials $\ell(X)$ such that $\deg \ell(X) - \deg g(X) < d$ $(d \geq 1)$. Consider

$$b_nf(X) = a_mX^{m-n}g(X) + r_1(X)$$

where $r_1(X) = (b_na_{m-1} - b_{n-1}a_m)X^{m-1} + \dots (b_na_{m-n} - b_ca_m)X^{m-n} + \dots + b_na_o$.

Thus $b_nf(X) - a_mX^{m-n}g(X)$ has degree at most $m-1$, we might as well assume that it has degree $m-1$, if not, the argument is the same. By the induction hypothesis there exist polynomials $q_1(X)$, $r_2(X)$ such that

$$b_n^{(m-1)-n+1}(b_nf(X) - a_mX^{m-n}g(X) = q_1(X)g(X) + r_2(X),$$

where $\deg r_2(X) < n$ or $r_2(X) = 0$. We need now only take

$$q(X) = a_mb_n^{m-n}.X^{m-n} + q_1(X), \quad r(X) = r_2(X).$$

As regards uniqueness, we suppose that $b_n^k\ f(X)$ has an other form $b_n^k\ f(X) = h(X)g(X) + p(X)$. Then

$$(h(X) - q(X))g(X) = p(X) - r(X).$$

If $h(X) - q(X) \neq 0$, then $(h(X) - q(X))g(X)$ has degree at least n, whereas deg $(p(X) - r(X)) < n$. Hence $h(X) - q(X) = 0$, $p(X) - r(X) = 0$. This completes the proof of the theorem.

Definition 1-8 Let R be a commutative ring with identity. If $f(X) = a_o + a_1X + \ldots + a_nX^n \in R[X]$, then the derivative of f(X), written as f'(X), is defined to be

$$f'(X) = a_1 + 2a_2X + \ldots + na_nX^{n-1}.$$

Theorem 1-6 If $f(X), g(X) \in R[X]$ and $r \in R$, then

i) $(f(X) + g(X))' = f'(X) + g'(X)$

ii) $(r\, f(X))' = r\, f'(X)$

iii) $(f(X)g(X))' = f'(X)g(X) + f(X)g'(X)$

(For proof see [10])

Definition 1.9 Let R be an integral domain. A polynomial p(X) in R[X] is said to be irreducible over R if whenever $p(X) = a(X)b(X)$ with a(X), $b(X) \in R[X]$ then either a(X) or b(X) has degree 0 (i.e., is a constant).

Theorem 1-7 (Unique Factorization in F[X])

If F is a field, then each polynomial $f(X) \in F[X]$ of positive degree is the product of a non-zero element of F and irreducible monic polynomials of F[X] . Apart from the order of the factors, this factorization is unique. (see [6])

Polynomials in several indeterminates.

Definition 1-10 Let R be a ring. A polynomial ring over R in n indeterminates $X_1, X_2, \ldots, X_n$, denoted by $R[X_1, X_2, \ldots, X_n]$, is the set of all elements of the form of a finite sum:

$$\sum a_{i_1 \cdots i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \quad ,$$

where the i_j are non-negative integers and $a_{i_1 \ldots i_n} \in R$. Each $a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$ is called a monomial.

Definition 1-11 A polynomial in the n ideterminates $X_1, \ldots, X_n$ is called a symmetric polynomial if it is invariant under all permutations of the indices $1, 2, \ldots, n$.

Example $X_1^2 + X_2^2 + X_3^2 - X_1X_2 - X_1X_3 - X_2X_3$ is a symmetric polynomial in 3 indeterminates X_1, X_2 and X_3.

Definition 1-12 The elementary symmetric polynomials are defined as follows:

$$s_1(X_1, \ldots, X_n) = \sum_{i=1}^{n} X_i = X_1 + X_2 + \ldots + X_n$$

$$s_2(X_1, \ldots, X_n) = \sum_{i<j}^{n} X_iX_j = X_1X_2 + \ldots + X_1X_n + X_2X_3 + \ldots + X_2X_n + \ldots + X_{n-1}X_n$$

$$s_3(X_1, \ldots, X_n) = \sum_{i<j<k} X_iX_jX_k$$

.

.

.

$$s_n(X_1, \ldots, X_n) = X_1X_2 \ldots X_n .$$

From now on F will denote a field.

Theorem 1-8 If $f(X) = a_o + a_1X + \ldots + a_nX^n \in F[X]$ has the n zeroes $X_1, X_2, \ldots, X_n$ in F, then

$$s_j(X_1,\ldots, X_n) = (-1)^j \frac{a_{n-j}}{a_n}, \quad j = 1,2,\ldots, n.$$

(For proof see [11])

Theorem 1-9 Every symmetric polynomial in $X_1, X_2,\ldots, X_n$ over F can be expressed as a polynomial in the elementary symmetric polynomials over F. (For proof see [11])

Theorem 1-10 Let $f(X) \in F[X]$ of degree n with roots $X_1,X_2,\ldots, X_n$. If $g(y_1,y_2,\ldots,y_n)$ is a symmetric polynomial in $y_1,y_2,\ldots,y_n$ over F, then $g(X_1,X_2,\ldots, X_n)$ is an element of F.

Proof Since $X_1,X_2,\ldots, X_n$ are the roots of f(X), by theorem 1-8 the elementary symmetric polynomials $s_j(X_1,\ldots,X_n) = (-1)^j \frac{a_{n-j}}{a_n}$, $j = 1,2, \ldots, n$. Then $s_j(X_1,\ldots, X_n) \in F$. Now $g(y_1,y_2,\ldots,y_n)$ is a symmetric polynomial over F, it then follows from theorem 1-9 that $g(y_1,\ldots,y_n)$ can be written as a polynomial over F in indeterminates $s_1(y_1,\ldots,y_n)$, $s_2(y_1,\ldots,y_n),\ldots, s_n(y_1,\ldots, y_n)$. This implies that $g(X_1,\ldots, X_n)$ is a polynomial over F in $s_1(X_1,\ldots, X_n)$, $s_2(X_1,\ldots, X_n)$, $\ldots$, $s_n(X_1,\ldots, X_n)$ which are in F. Hence $g(X_1, X_2,\ldots, X_n) \in F$.

Fields and Extension Fields

Definition 1-13 Let F be a field and 1 its multiplicative identity. F is said to be of characteristic $p > o$ if p is the least positive integer for which $p.1 = o$ and F is said to be of characteristic 0 if there is no positive integer p for which $p.1 = o$ except $p = o$.

Definition 1-14 A field which does not contain any proper subfields is called a prime field.

Theorem 1-11 Any prime field of characteristic zero is isomorphic to the field of rational numbers. (For proof see [8])

Definition 1-15 Let F be a field; a field K is said to be an extension of F if F is a subfield of K. We call F a ground field.

From now on F will denote a ground field and K an extension of F.

Let $a_1, a_2, \ldots, a_n$ be fixed elements in K. Let $f(X_1, X_2, \ldots, X_n)$ and $g(X_1, X_2, \ldots, X_n)$ be two polynomials in $F[X_1, X_2, \ldots, X_n]$ such that $g(a_1, a_2, \ldots, a_n) \neq 0$, then the quotient $\dfrac{f(a_1, \ldots, a_n)}{g(a_1, \ldots, a_n)}$ belongs to K (since K is a field) and the set of all such quotients is a field, denoted by $F(a_1, a_2, \ldots, a_n)$. We call $F(a_1, a_2, \ldots, a_n)$ the subfield of K which is obtained by adjunction of the elements $a_1, a_2, \ldots, a_n$ to F.

Definition 1-16 If K is finite dimensional as a vector space over F, we say that K is a finite extension of F. If K is infinite dimensional as a vector space over F, we say that K is an infinite extension of F.

Definition 1-17 An element $a \in K$ is said to be algebraic over F if there exists a polynomial f(X) in $F[X]$ such that $f(a) = 0$. Otherwise, a is transcendental over F.

Definition 1-18 Let a be an element of K which is algebraic over F. The monic irreducible polynomial in $F[X]$ of which a is a root will be called the minimal polynomial of a in $F[X]$, or over F.

Theorem 1-12 If a is algebraic over F, then there exists a unique minimal polynomial of a in $F[X]$ and the field F(a) coincides with $F[a]$. Moreover, if the minimal polynomial of a over F is of degree n, then any element of F(a) has a unique expression of the form

$$c_o a^{n-1} + c_1 a^{n-2} + \ldots + c_{n-1} \text{ , } c_i \in F$$

(For proof see [8]).

Definition 1-19 Two elements a and b of one and the same extension field K of F are conjugate over F if they are algebraic over F and have the same minimal polynomial over F.

Definition 1-20 The extension field K of F is simple extension of F if K = F(a) for some a in K.

Theorem 1-13 If f(X) is a non-constant irreducible polynomial in F[X] , then there exists a simple extension F(a) such that a is a root of f(X) . (For proof see [8]).

Definition 1-21 The extension K of F is called an algebraic extension of F if every element in K is algebraic over F. Extensions which are not algebraic are called transcendental extensions.

Theorem 1-14 Any finite extension of a field of characteristic zero is a simple extension (See [7]).

Definition 1-22 If F is a subfield of K, then K is said to be an algebraic closure of F if

i) K is an algebraic extension of F and

ii) K possesses no proper algebraic extensions (that is, if every algebraic extension of F coincides with F).

Theorem 1-15 If F is a field, then there exists an algebraic closure of F, and any two algebraic closures of F are isomorphic (For proof see [8]).