CHAPTER I

PRELIMINARIES

In this thesis, we assume a basic knowledge of group theory. However, this chapter contains review of some important notations we will be using. Proofs will not be given, and can be found in [6], [8].

1.1 Definition. Let G be a finite group and let $a \in G$. Then the order of a, denoted by $O(a)$, is defined to be the least positive integer m such that $a^m = 1$, where 1 is the identity of G.

1.2 Definition. A polynomial in X over a field K, denoted by $f(X)$, is defined to be

$$f(X) = \sum_{i=0}^{n} a_i X^i ,$$

where the coefficients a_i, not all of them zero, belong to K, while the indeterminate, $X \notin K$, is considered here commutative with every element $a \in K$.

1.3 Notation. $K[X]$ denotes the set of all polynomials in X over K.

1.4 Definition. A non-zero element $f(X) \in K[X]$ is said to have degree n, denoted by deg. f = n, if n is the largest positive integer such that X^n has a non-zero coefficient, which itself is called the leading coefficient of $f(X)$.

1.5 Definition. Let K be a field. Let $f(X) \in K[X]$. Then

(i) $f(X)$ is said to be a monic polynomial in X if its leading coefficient is 1.

(ii) $f(X)$ is said to be an irreducible polynomial if $f(X)$ cannot be written as a product of two polynomials with positive degree.

(iii) If $f(X), g(X) \in K[X]$, we say that $f(X)$ divides $g(X)$ or $g(X)$ is a multiple of $f(X)$, written $f(X) \mid g(X)$, if there exists $h(X) \in K[X]$ such that $g(X) = f(X) \cdot h(X)$.

1.6 Definition. Let K be a field. If K is a subfield of a field F, then we say that F is a field extension of K.

1.7 Definition. Let K be a field and let $f(X)$ be a polynomial in $K[X]$ of degree $n > 0$. Let F be an extension field of K. Then we say that $f(X)$ splits into linear factors in F in case

$$f(X) = c\,(X - a_1) \dots (X - a_n),$$

where $a_i \in F$, $i = 1, \dots, n$.

1.8 Definition. Let K be a field. Let $f(X)$ be a polynomial in $K[X]$ of degree $n > 0$. Let F be an extension field of K such that F contains all n roots $\{a_1, \dots, a_n\}$ of $f(X)$. Then the field $K(a_1, \dots, a_n)$ is called the splitting field of $f(X)$ over K.

1.9 Theorem. Any two splitting fields of the same polynomial over a given field K are isomorphic.

1.10 Definition. Let K be a subfield of a field F. Then $\{v_1, \ldots, v_n\} \subseteq F$ is said to be linearly independent over K if and only if for all scalars c_i in K,

$$c_1v_1 + \ldots + c_nv_n = 0 \quad \text{implies} \quad c_1 = \ldots = c_n = 0.$$

Otherwise, $\{v_1, \ldots, v_n\} \subseteq F$ is said to be linearly dependent over K.

1.11 Definition. Let F be a field extension of a subfield K. Then the degree of F over K, denoted by $[F : K]$, is defined to be the maximal number of linearly independent elements of F over K. That is,

(i) $[F : K] = +\infty$, if for any $n \in \mathbb{Z}^+$ (set of all positive integers), there exists n linearly independent elements of F over K.

(ii) $[F : K] = n < +\infty$, if there exists n linearly independent elements of F over K and if any set of more than n elements in F is linearly dependent over K.

1.12 Definition. Let F be a field extension of a field K and $a \in F$. Then a is an algebraic element over K if it is a root of some polynomial over K.

1.13 Definition. Let F be an extension field of a field K. Let a be an algebraic element over K and f(X) be the monic polynomial of least degree for which a is a root. Then f(X) is called the minimal polynomial of a over K and the degree of f(X) is called the (algebraic) degree of a over K.

1.14 Definition. Let F be a field. Then the characteristic of F, denoted by ch.F, is defined as follows :

(i) if $ne \neq 0$ for all $n \in \mathbb{Z}^+$, where e is the identity of F, then ch.F = 0 ;

(ii) if $ne = 0$ for some $n \in \mathbb{Z}^+$, then ch.F is the smallest integer $d \in \mathbb{Z}^+$ such that $de = 0$.

1.15 Definition. If $f(X) = a_0X^n + a_1X^{n-1} + \ldots + a_{n-1}X + a_n \in K[X]$, then the derivative of f(X), written as $f'(X)$, is defined to be

$$f'(X) = na_0X^{n-1} + (n-1)a_1X^{n-2} + \ldots + a_{n-1} \in K[X].$$

1.16 Definition. Let K be a field and let $f(X) \in K[X]$. Then the element $a \in K$ is a root of f(X) of multiplicity m if $(X-a)^m \mid f(X)$ whereas $(X-a)^{m+1} \nmid f(X)$.

1.17 Theorem. Let F be a field and let $f(X) \in F[X]$. If f(X) is irreducible over F, then $F[X]/(f(X))$ is a field.

1.18 Theorem. Let F be a field. Let μ be a root of an irreducible polynomial $f(X) \in F[X]$. Then $F(\mu)$ is a field isomorphic to $F[X] / (f(X))$.