CHAPTER II

PRELIMINALIES

In this chapter we will give some definitions and theorems which will be basic tools for our investigation. The materials of this chapter are drawn from references [4], [5], [6], [7] and [8].

Algebra

A ring $(R, +, \cdot)$ consists of a nonempty set R together with two binary operations + and o called addition and multiplication respectively such that the following conditions are satisfied.

1) $a + b = b + a$

2) $(a + b) + c = a + (b + c)$

3) There exists an element 0 in R such that
$a + 0 = a$ for every a in R

4) for each $a \in R$ there exists an element $-a \in R$
such that $a + (-a) = 0$

5) $(a.b).c = a.(b.c)$ and

6) $a.(b + c) = a.b + a.c$ and
$(b + c).a = b.a + c.a$

where $a, b, c \in R$

A ring R is said to be division ring provided that the set $R - \{0\}$ is a group under . . If $R - \{0\}$ forms a commutative group then R is called a field. A field which does not posses any proper subfield is called a prime field. It can be shown that each field F contains a unique prime subfield. An element $a \neq 0$ of a ring R is called a zero divisor of R if there exists some $b \neq 0$ in R such that $a.b = 0$. A commutative ring R with identity is said to be an integral domain if R has no zero divisors. If there exists a positive integer n such that $na = 0$ for all $a \in$ a ring R, then the smallest positive integer with this property is called the characteristic of the ring R. If no such positive integer exists (that is $n = 0$ is the only integer for which $na = 0$ for all a in R) then R is said to be of characteristic zero.

The following remarks can be easily proven.

Remark 2.1. If R is a division ring then R has no zero divisors.

Remark 2.2. If R is a ring with identity having no zero divisors then the characteristic of R is either 0 or a prime number.

Remark 2.3. If R is division ring then the characteristic of R is either a prime number or 0.

Remark 2.4. Every finite subring of a division ring is a division ring.

A subring I of the ring R is said to be a two - sided ideal of R if $r \in R$ and $a \in I$ imply both $ra \in I$ and $ar \in I$. From now on we shall call a two - sided ideal an ideal. The ideal I is said to be a prime ideal if for all a, b in R, $a.b \in I$ implies that $a \in I$ or $b \in I$. And the ideal I is said to be a maximal ideal provided that $I \neq R$ and whenever J is an ideal of R with $I \subset J \subseteq R$ then $J = R$.

Again, the following remarks can be proved easily

Remark 2.5. If R is a ring with identity and R has no non-trival ideals then R is division ring.

Remark 2.6. A commutative ring R with identity is an integral domain if and only if the zero ideal $\{0\}$ is a prime ideal of R.

Remark 2.7. Let R be a ring with identity and M a maximal ideal of R then R/M has no non - trival ideals.

The following theorem is used several times later on. So we shall give the proof.

Theorem 2.8. An integral domain with more than one element and only a finite number of ideals is a field.

proof. Let $s \neq 0 \in$ integral domain S, and t an arbitrary element of S. We shall show that there exist an element x of S such that $sx = t$. For each positive integer i,

Let $S_i = \{ ys^i \mid y \in S \}$

Then S_i is an ideal of S, since $a \in S_i$, $b \in S$

$$a \cdot b = ys^i b = yb\, s^i = y' s^i .$$

Since S has only a finite number of different ideals, for certain positive integer m, n we must have

$$S_m = S_n \qquad \text{with } m < n .$$

Hence in particular, $t\, s^m$ being an element of S_m is also in S_n, that is there exists an element z of S such that

$$t\, s^m = z\, s^n$$

$$t\, s^m - z\, s^m = 0$$

$$s^m (t - z s^{n-m}) = 0$$

Since $s^m \neq 0$ as $s \neq 0$ and S is integral domain, therefore

$$t - z\, s^{n-m} = 0$$

$$t = z\, s^{n-m}$$

If $n - m = 1$ we get $x = z$.

While if $n - m > 1$ we set $x = z\, s^{n-m-1}$. Hence in either case, there exists an element x of S such that $sx = t$ and therefore S is a field.

Definition 2.9. Let $\{R_i\}_{i \in \mathcal{J}}$ be a family of rings. The complete direct sum of the rings R_i, denoted by $\sum_{i \in \mathcal{J}} \oplus R_i$, consists of functions a defined on $\mathcal{J}$ such that for each element $i \in \mathcal{J}$ a (i) lies in R_i.

$$\sum_{i \in \mathcal{J}} \oplus R_i = \left\{ a \mid a : \mathcal{J} \to \bigcup_{i \in \mathcal{J}} R_i, \ a(i) \in R_i \right\}$$

Addition and multiplication may be introduced in the set $\sum_{i \in \mathcal{J}} \oplus R_i$ by means of the corresponding operations in the individual components i.e.

$$(a + b)(i) = a(i) + b(i)$$

$$ab(i) = a(i)\, b(i) \quad \text{for all } i \in \mathcal{J}$$

It follows that the resulting set with the above operations comprises a ring, the zero element of $\sum_{i \in \mathcal{J}} \oplus R_i$ is the function $0 : \mathcal{J} \to \bigcup_{i \in \mathcal{J}} R_i$ defined by taking $0(i) = 0 \in R_i$ for $i \in \mathcal{J}$; similarly, the nagative $-a$ of a function $a \in \sum_{i \in \mathcal{J}} \oplus R_i$ is given by the rule $(-a)(i) = -a(i)$.

Definition 2.10. If $F \subset F'$ is a subfield then F' is called an extension field of F. An element $r \in F'$ is said to be algebraic over F if there exist element $a_0, a_1, a_2, \ldots a_r$ in F, not all zero, such that $a_0 r^n + a_1 r^{n-1} + \ldots + a_n = 0$.

F' is said to be a splitting field for $f(x)$ over F provided that $f(x)$ can be factored completely into linear factors in $F[x]$.

The theorems on extension fields, stated in the following can be found in reference [5].

Theorem 2.11. (Simple Algebraic Field Extension)

If $r \in F' \supseteq F$ is algebraic over F, then there exists a unique monic irreducible polynomial $f(x) \in F[x]$ such that $f(r) = 0$. Furthermore, if $g(x)$ is a polynomial in $F[x]$ for which $g(r) = 0$, then $f(x) \mid g(x)$.

Theorem 2.12. Let F' be an extension field of F and $r \in F'$ be algebraic over F of degree n. Then the elements $1, r, \ldots r^{n-1}$ form a basis of the vector space F' over F.

Theorem 2.13. If F is a finite field, then F has exactly p^n elements for some prime number p and $n \in \mathbb{Z}_+$. Moreover, every element of F is the root of the polynomial $f(x) = x^{p^n} - x \in F[x]$.

Theorem 2.14. The multiplicative group of a finite field is cyclic

Theory of Numbers

Let a, b be two integers not both 0, if c is the greatest integer that divides a and b , we call c the greatest common divisor of a and b . It is usually denoted by the symbol (a, b). If (a,b) = 1 we say that the two numbers are relatively prime. If m is some positive integer, the number of integers in the sequence 1, 2, ... m - 1, m which are relatively prime to m will be denoted by $\phi(m)$, and it is known as Euler ' s ϕ - function. When m = p a prime then , $\phi(p) = p-1$

Theorem 2.16. (Euler's Theorem)

For any integer a that is relatively prime to m one has the congruence $a^{\phi(m)} \equiv 1 \mod(m)$

proof. See reference [6].

Theorem 2.17. (Dirichlet)

If a > 0 and b are integers such that (a, b) = 1, then there are infinitely many primes of the form a n + b , where n is a positive integer.

proof . See reference [6].

Set Theory

Definition 2.18. A choice function on a set of nonempty sets $\mathcal{A}$ is a function $\theta : \mathcal{A} \to \bigcup \mathcal{A}$ such that for each $A \in \mathcal{A}$ $\theta(A) \in A$.

Axiom of choice : Every family of nonempty sets has a choice function.

Definition 2.19. A partial ordering defined on a set X is a relation r on X satisfying

1) Reflexive law : $a \, r \, a \quad \forall a \in X$

2) Antisymmetric law : $a \, r \, b$ and $b \, r \, a \Rightarrow a = b$ $\forall a, b \in X$

3) Transitive law : $a \, r \, b$ and $b \, r \, c \Rightarrow a \, r \, c$ $\forall a, b, c \in X$

(X, r) is called a partially ordered set. A partial ordered set is said to be well - ordered if every nonempty subset of it has a smallest element.

Well - ordering Theorem : Every set can be well ordered.

proof. See reference [8].

Definition 2.20. If A is a well - ordered set and if $a \in A$. The initial segment of X determined by a is the set I_a, defined as follows

$$I_a = \left\{ x \in A \;\middle|\; x < a \right\}$$

If $x < y$ and if there is no element between x and y , we say that x is an immediate predecessor of y , or y is an immediate sucessor of x.

Definition 2.21, Let A be a set and suppose that A can be well - ordered in such a way that $\forall x \in A \quad x = I_x$. Then A is called an ordinal number .

Definition 2.22. Let α and β be ordinal numbers we say that $\alpha \leq \beta$ if and only if $\alpha \subseteq \beta$.

Definition 2.23. Let β be a non - zero ordinal number, if β has no immediate predecessor. That is, if β is not equal to $\alpha \cup \{\alpha\}$ for any ordinal α , then β is called a limit ordinal. Otherwise β is called a non limit ordinal.

Remark. 1. $\emptyset$ is an ordinal, $\emptyset \cup \{\emptyset\}$ is an ordinal, and $\{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$ is an ordinal. It is customary to denote $\emptyset$ by 0 , $\{\emptyset\}$ by 1, $\{\emptyset, \{\emptyset\}\}$ by 2 and so on . We shall define ω to be a set of all finite ordinals. It can be shown that ω is a limit ordinal.

2. Let $(A, \leq)$ and $(B, \leq)$ be disjoint well - ordered sets let $C = A \cup B$ and $\leq$ be defined on C as follows : for $x, y \in C$, $x \leq y$ if and only if

i) $x \in A$ and $y \in A$ and $x \leq y$ in A or

ii) $x \in B$ and $y \in B$ and $x \leq y$ in B or

iii) $x \in A$ and $y \in B$

Then $(C, \leq)$ is a well - ordered set .

Definition 2.24. Let α and β be ordinal numbers, and let A and B be disjoint well - ordered sets such that α is ordinal of A and β is ordinal of B . We will define $\alpha + \beta$ to be the ordinal number of the well - ordered set $(A \cup B , \leq)$.

By using this definition , it can be seen that

$\alpha + 1 = \alpha \cup \{\alpha\}$

Transfinite Induction for Ordinals

Let $P(\gamma)$ be a statement for each ordinal γ . Suppose that for each ordinal α we have $[\, P(\beta) , \forall \beta < \alpha \,] \Rightarrow P(\alpha)$. Then $P(\gamma)$ is true for all ordinal γ .

Definition 2.25. Let X be a set. The cardinal of X , denoted by $\overline{\overline{X}}$ is the smallest ordinal S with $S \approx X$ ($\approx$ means equipotent i.e $\exists$ 1 - 1 onto map between the two sets)

The following are facts about cardinals. The proof of these facts can be found in reference [8].

Theorem 2.26. $\overline{\overline{X}} < \overline{\overline{P(X)}}$ (P(X) = power set of X) for every set X .

Theorem 2.27. Each infinite cardinal number is a limit ordinal.

proof. Let α be an infinite cardinal number. Since α is a cardinal, α is also an ordinal. Suppose that α is not a limit ordinal. Hence there exists an ordinal β such that $\beta + 1 = \alpha$. We will show that β is equipotent with $\beta + 1$

Since $\beta + 1$ is infinite, β is also infinite.

Define $f : \beta + 1 \rightarrow \beta$ by

$$f(\beta) = 0$$

$$f(n) = n + 1 \qquad \text{for } n \in \omega$$

$$f(x) = x \qquad x \in \beta - \omega$$

Then β is equipotent with $\beta + 1$, i.e. β equipotent with α, then α is not a cardinal, contrary to our hypothesis, where α is a limit ordinal.