CHAPTER II

PRELIMINARIES

In this chapter we shall collect some definitions and results from semigroup theory and field theory which will be necassary for our invertigation. The meterials of this chapter are taken from [1] and [2]. We shall assume that the reader is familiar with common terms used in set theory.

By a <u>semigroup</u> we mean an ordered pair $(S, \circ)$ where S is a nonempty set and $\circ$ is a binary operation on S satisfying the associative law, this is, for all a,b,c in S,

$$a \circ (b \circ c) = (a \circ b) \circ c.$$

For convenience, we shall denote the semigroup $(S, \circ)$ simply by S and we shall denote $a \circ b$ simply by ab. An element e of a semigroup S is a <u>left [right] indentity</u> of S if ea = a [ae = a] for all a in S. An element e of a semigroup S is an <u>identity</u> (two-sided indentity) of S if e is both a left and a right identity of S. If a semigroup S has an identity then it is unique and it is usually denoted by 1. An element z of a semigroup S is a <u>left [right] zero</u> of S if za = z [az = z] for all a in S. If an element z of a semigroup S is both a left and a right zero of S, then it is called a <u>zero</u> of S. If a semigroup S has a zero, then it is unique and it is usually denoted by o. An element e of a semigroup S is an <u>idenpotent</u> if $e^2 = e$. For any semigroup S, we denote the set of all its idenpotents by E(S), this is $E(S) = \{e \in S / e^2 = e\}$. If a, b are an elements of a semigroup S we say that b is an <u>inverse</u> of a if a = aba and b = bab. An element a may have more than one inverse.

A semigroup S is commutative if ab = ba for all a, b in S. A semigroup S is an inverse semigroup iff each element a of S has a unique inverse which is denoted by a^{-1}. If S is an inverse semigroup and E(S) contains 1 alone, then S is a group. In a semigroup S, if we have that a = aba then it is easy to verify that ab, ba belong to E(S). Thus for all a in an inverse semigroup S, aa^{-1} and $a^{-1}a$ belong to E(S). If S is a semigroup with zero 0 such that

$$ab = \begin{cases} a & \text{if } a = b, \\ 0 & \text{otherwise,} \end{cases}$$

then S is called a Kronecker semigroup and it is easy to see that E(S) = S.

A nonempty subset T of a semigroup S is a subsemigroup of S if it is closed under the operation of S, i.e. if a,b $\in$ T, then ab $\in$ T. The order of a semigroup S is the number of its elements if S is finite, otherwise S is of infinite order. Let A be a subset of a semigroup S, we write AS for $\{as \mid a \in A \text{ and } s \in S\}$ and SA for $\{sa \mid s \in S \text{ and } a \in A\}$. A nonempty subset A of a semigroup S is a left ideal of S if SA $\subseteq$ A. A right ideal is defined dually. A nonempty subset A of a semigroup S is an ideal (two-sided ideal) of S if it is both a left and a right ideal of S. Evidently every ideal (whether one-sided or two-sided) is a subsemigroup, but not every subsemigroup is an ideal. An ideal of an inverse semigroup is an inverse semigroup. An ideal A of a semigroup S is called completely prime ideal if ab $\in$ A implies a $\in$ A or b $\in$ A. A subsemigroup T of a semigroup S is a filter of S if for any a, b in S, ab belongs to T implies both a and b belong to T.

A filter of an inverse semigroup is an inverse subsemigroup. It is known that a nonempty subset T of S is a filter if and only if $S \setminus T$ is either an empty set or a completely prime ideal of S.

A relation ρ on a semigroup S is said to be a congruence on S if it is an equivalence relation on S such that for any a,b,x,y in S if $a\rho b$ and $x\rho y$ then $ax\rho by$. For any congruence ρ on a semigroup S, the ρ-class containing an element a will be denoted by $a\rho$. If ρ is a congruence of a semigroup S, then $S/\rho = \{a\rho \mid a \in S\}$ forms a semigroup under the binary operation given by $(a\rho)(b\rho) = ab\rho$, this semigroup is called the quatient semigroup of S relative to ρ. Let $\mathcal{S}$ be a class of semigroups. We say that a congruence ρ on a semigroup S is an $\mathcal{S}$-congruence on S if S/ρ is in $\mathcal{S}$. In this thesis $\mathcal{K}, \mathcal{K}_n, \mathcal{G}, \mathcal{G}_n, \mathcal{G}_{n,m}$ denote the class of all Kronecker semigroups, the class of all Kronecker semigroups of order n, the class of all groups, the class of all groups of order n and $\mathcal{G}_{n,m} = \mathcal{G}_n \cup \mathcal{G}_m$ respectively.

A mapping h from a semigroup $(S, \circ)$ into a semigroup $(S', *)$ is said to be a homomorphism provided that for all a,b in S,

$$h(a \circ b) = h(a) * h(b).$$

It is easy to verify that if h is a homomorphism from S into S' then h(S) is a subsemigroup of S' and $h(E(S)) \subseteq E(h(S))$. Let ρ be a congruence on a semigroup S. Then the mapping $\rho^{\#}$ from S into S/ρ defined by

$$\rho^{\#}(a) = a\rho$$

for all a in S, is called the natural homomorphism.

We state the following theorems without proofs. Their proofs can be found in the references indicated or in the Appendex.

Theorem 2.1. ([2] , Proposition 1.4, pp 131-132) Let S be an inverse semigroup. Then the following hold:

(2.1.1) $(a^{-1})^{-1} = a$ for all a in S.

(2.1.2) $e^{-1} = e$ for all e in E(S).

(2.1.3) $(ab)^{-1} = b^{-1}a^{-1}$ for all a,b in S.

Theorem 2.2. ([2] , Proposition 3.1, pp 139-140) If S is an inverse semigroup, then the relation

$$\sigma = \{(a,b) \in S \times S \ / \ ae = be \text{ for some } e \text{ in } E(S)\}$$

is the minimum group congruence on S.

Proofs of the following theorems are given in the Appendex.

Theorem 2.3. Let A be an ideal of an inverse semigroup S and B an ideal of A, then B is an ideal of S.

Theorem 2.4. Let S be a semigroup and A and B completely prime ideals of S such that $A \subseteq B \subseteq S$, then $B \setminus A$ is either an empty set or a completely prime ideal of $S \setminus A$.

Theorem 2.5. For a subset A of a semigroup S, A is a filter of S iff $S \setminus A$ is either a completely prime ideal of S or an empty set.

Theorem 2.6. Let $(S, \circ)$ and $(S', \circ')$ be disjoint semigroups. Then $S \cup S'$ with the binary operation * defined by

$$a * b = a \circ b \quad \text{if } a,b \in S$$

$$a * b = a \circ' b \qquad \text{if } a,b \in S'$$

$$a * b = b * a = a \text{ if } a \in S \text{ and } b \in S'$$

is a semigroup. The semigroup $S \cup S'$ in Theorem 2.6 will be called the semigroup S' with S adjoined as zeroes.

A field is trible (F, +, ∘), where +, ∘ are two binary operations on F, known as addition and multiplication respectively, such that the following hold:

(i) F forms a commutative group under addition.

(ii) $F^* = F \setminus \{o\}$, where o is the additive indentity, 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 $(F^*, \circ)$ will be referred to as the additive group and the multiplicative group of F, respectively. If there is a least positive integer n such that na = o 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 nonempty subset of a field (F, +, ∘) such that K forms a field under restiction of +, ∘ to KxK, 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 h of a field F into a field F' is a homomorphism provided that for all a,b in F,

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

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

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

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

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

and

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

It can be shown that C(F) under the above addition and multiplication forms a field. This field contains $\bar{F} = \{(a,o) / a \varepsilon F\}$ 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,o) of $\bar{F}$ by a and denote (o,1) by i, then each element (a,b) of C(F) can be expressed as

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

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

$$\psi(a+bi) = a - bi$$

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

$$\Delta(F) = \{a+bi \ \varepsilon \ C(F) / (a+bi)\psi(a+bi) = 1\}.$$

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) =

$\Delta(F)$. A proof of the following lemma is given in the Appendex.

Lemma 2.7. Let S be an inverse semigroup, F a field of characteristic different from 2 such that $a^2 \neq -1$ for any a in F. Let h be a homomorphism from S into $C(F)^*$. Then for each x in S, $\frac{h(x)-h(x^{-1})}{2i}$ and $\frac{h(x)+h(x^{-1})}{2}$ belong to F if and only if h(x) belongs to $\Delta(F)$.