CHAPTER I

PRELIMINARIES

In this chapter we shall give some notations, definitions and theorems used in this thesis. Our notations are

$\mathbb{Z}$ is the set of all integers,

$\mathbb{Z}^+$ is the set of all positive integers,

$\mathbb{Q}^+$ is the set of all positive rational numbers,

$\mathbb{R}^+$ is the set of all positive real numbers,

$\mathbb{Z}_n$, $n \in \mathbb{Z}^+$, is the set of congruence classes modulo n in $\mathbb{Z}$,

$\mathbb{Z}_0^+ = \mathbb{Z}^+ \cup \{0\}$.

Definition 1.1. A triple $(S,+,\cdot)$ is said to be a right seminear-ring iff S is a set and + and $\cdot$ are binary operations on S such that

(a) $(S,+)$ is a semigroup,

(b) $(S,\cdot)$ is a semigroup,

(c) $\forall\, x, y, z \in S$ $(x+y)z = xz+yz$. (right distributive law)

A left seminear-ring is similarly defined. If $(S,+,\cdot)$ is both a left and a right seminear-ring, then it is a semiring.

Throughout this thesis we shall only study right seminear-ring All definitions and theorems stated for right seminear-rings have a dual statement and proof for left seminear-rings. So from now on the word "seminear-ring" will mean a right seminear-ring. The reason that we choose right seminear-rings is that seminear-rings of maps (the most important examples) are all right distributive (see Example 1.4)

Example 1.2. $\mathbb{Z}$, $\mathbb{Z}^+$ and $\mathbb{Z}_0^+$ with the usual addition and multiplication are seminear-rings.

Example 1.3. Let S be a nonempty set. Define + and . on S by $x + y = y$ and $x.y = x$ for all $x, y \in S$. Then $(S,+,.)$ is a seminear-ring.

Example 1.4. Let $(S,+)$ be a semigroup (not necessarily commutative). Let $M(S) = \{f: S \to S \mid f \text{ is a map}\}$. Define + and . on $M(S)$ by $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(g(x))$ for all $x \in S$. Then $(M(S),+,.)$ is a seminear-ring which is not left distributive if $\|S\| > 1$.

Definition 1.5. A seminear-ring $(N,+,.)$ is said to be a near-ring iff $(N,+)$ is a group. We shall always denote the identity of $(N,+)$ by 0 and the additive inverse of $x \in N$ by $-x$.

Example 1.6. Let $(N,+)$ be a group (not necessarily commutative) with identity 0. Then the following sets with + and . defined in Example 1.4 are near-rings:

(1) $M(N) = \{f: N \to N \mid f \text{ is a map}\}$.

(2) $M_0(N) = \{f: N \to N \mid f(0) = 0\}$.

(3) $M_c(N) = \{f: N \to N \mid f \text{ is constant}\}$.

Lemma 1.7. Let N be a near-ring. Then $0.x = 0$ for all $x \in N$. Also, $(-x).y = -(x.y)$ for all $x, y \in N$.

Proof. Let N be a near-ring. Let $x \in N$. Then

$0.x = (0 + 0).x = 0.x + 0.x$, so $0.x = 0$ since a group has only one idempotent. Let $x, y \in N$. Then $x.y + (-x).y = (x + (-x)).y = 0.y = 0$, so $(-x).y = -(x.y)$.

#

Remark. In a near-ring N it is possible that $x.0 \neq 0$ and $x.(-y) \neq -(x.y)$. See Example 1.6.

Definition 1.8. A near-ring $(N,+,.)$ is said to be a near-field iff $(N \setminus \{0\},.)$ is a group.

Example 1.9. Let $M_c(\mathbb{Z}_2) = \{ f: \mathbb{Z}_2 \to \mathbb{Z}_2 \mid f \text{ is constant}\}$. Thus $M_c(\mathbb{Z}_2) = \{f_0, f_1\}$ where $f_0(x) = \bar{0}$ and $f_1(x) = \bar{1}$ for all $x \in \mathbb{Z}_2$. Let $+$ and $.$ be defined as in Example 1.4. Clearly, $(M_c(\mathbb{Z}_2),+)$ is a group, $(M_c(\mathbb{Z}_2),.)$ is a semigroup, $(M_c(\mathbb{Z}_2) \setminus \{f_0\},.)$ is a group and the right distributive law holds in $M_c(\mathbb{Z}_2)$, Therefore $(M_c(\mathbb{Z}_2),+,.)$ is a near-field.

Proposition 1.10. Let N be a near-field. If $\|N\| > 2$, then $x.0 = 0.x = 0$ for all $x \in N$.

Proof. Let N be a near-field and $\|N\| > 2$. Suppose there exists x in N such that $x.0 \neq 0$. Since $(N \setminus \{0\},.)$ is a group, there is a y in N such that $(x.0).y = y(x.0) = 1$, the identity of $(N \setminus \{0\},.)$. By Lemma 1.7, $0.y = 0$. Thus $x.0 = x.(0.y) = (x.0).y = 1$, so $x.0 = 1$. Let $z \in N \setminus \{0, 1\}$. Then $z = 1.z = (x.0).z = x.(0.z) = x.0 = 1$, so $z = 1$, a contradiction. Therefore $x.0 = 0$ for all $x \in N$. By Lemma 1.7, $x.0 = 0.x = 0$ for all $x \in N$.

#

Remark. From this proposition we see that if a near-field N is not isomorphic to $M_c(\mathbb{Z}_2)$ then $x.0 = 0.x = 0$ for all $x \in N$.

Definition 1.11. Let G be a group and G_1, G_2 subgroups of G. Then G is said to be a Zappa-Szép product of G_1 and G_2 iff $G = G_1G_2$ and $G_1 \cap G_2 = \{1\}$ where 1 is the identity of G. If G is a Zappa-Szép product of G_1 and G_2 we shall denote this by $G = G_1 * G_2$.

Example 1.12. (1) Let G be a group with $G = G_1 \times G_2$ for some subgroups G_1, G_2 of G. Then $G = G_1 * G_2$. Note that in this case $G_1, G_2 \trianglelefteq G$.

(2) Let S_3 be the symmetric group on three elements. Thus $S_3 = \{(1), (12), (13), (23), (123), (132)\}$. Let $A = \{(1), (12)\}$ and $A_3 = \{(1), (123), (132)\}$. Then A and A_3 are subgroups of S_3. Since $(13) = (132)(12) \in A_3A$ and $(23) = (123)(12) \in A_3A$, $S_3 = A_3A$. Therefore $S_3 = A_3 * A$. Since $(13)(12)(13) = (23) \notin A$, $A \ntrianglelefteq S_3$. Thus $S_3 \neq A_3 \times A$. Hence we have an example of a Zappa-Szép product which is not a direct product.

Lemma 1.13. Let $(G, \cdot)$ be a group such that $G = G_1 * G_2$ for some subgroups G_1, G_2 of G. Then

(1) $G = G_2 * G_1$.

(2) For all $g \in G$ there exist unique $g_1, \bar{g}_1 \in G_1$, $g_2, \bar{g}_2 \in G_2$ such that $g = g_1g_2 = \bar{g}_2\bar{g}_1$.

(3) For all $g_1 \in G_1$, $g_2 \in G_2$ there exist unique $\bar{x} \in G_1$, $\bar{y} \in G_2$ such that $\bar{x}g_2 = \bar{y}g_1$.

Proof. (1) We must show that $G = G_2G_1$. To show this, let $g \in G$. Since $G = G_1G_2$, $g^{-1} = g_1g_2$ for some $g_1 \in G_1$, $g_2 \in G_2$. Thus $g = g_2^{-1}g_1^{-1}$ which is in G_2G_1. Hence $G = G_2G_1$. Therefore $G = G_2 * G_1$.

(2) Let $g \in G$. Since $G = G_1 * G_2 = G_2 * G_1$, there are $g_1, \bar{g}_1 \in G_1$, $g_2, \bar{g}_2 \in G_2$ such that $g = g_1g_2 = \bar{g}_2\bar{g}_1$. Suppose $h_1, \bar{h}_1 \in G_1$, $h_2, \bar{h}_2 \in G_2$ are such that $g = h_1h_2 = \bar{h}_2\bar{h}_1$. Thus $g_1g_2 = h_1h_2$ and $\bar{g}_2\bar{g}_1 = \bar{h}_2\bar{h}_1$. So $h_1^{-1}g_1 = h_2g_2^{-1} \in G_1 \cap G_2 = \{1\}$ and $\bar{g}_1\bar{h}_1^{-1} = \bar{g}_2^{-1}\bar{h}_2 \in G_1 \cap G_2 = \{1\}$. Therefore $h_1 = g_1$, $\bar{h}_1 = \bar{g}_1$, $h_2 = g_2$ and $\bar{h}_2 = \bar{g}_2$.

(3) Let $g_1 \in G_1$ and $g_2 \in G_2$. Since $G = G_2 * G_1$, there are unique $x_1 \in G_1$, $x_2 \in G_2$ such that $g_1 g_2^{-1} = x_2 x_1$. Thus $x_2^{-1} g_1 = x_1 g_2$. Suppose $y_1 \in G_1$, $y_2 \in G_2$ are such that $y_2 g_1 = y_1 g_2$. Thus $g_1 g_2^{-1} = y_2^{-1} y_1$, so $y_1 = x_1$ and $y_2 = x_2^{-1}$. Put $\bar{x} = x_1$ and $\bar{y} = x_2^{-1}$.#

Definition 1.14. Let S be a semigroup. S is said to be a band iff $x^2 = x$ for all $x \in S$. S is said to be a rectangular band iff $xyx = x$ for all $x, y \in S$.

Theorem 1.15. Every finite semigroup has an idempotent.

Proof. Let S be a finite semigroup. Let $a \in S$. Thus there are $m, n \in \mathbb{Z}^+$ such that $m < n$ and $a^m = a^n$. Let

$$k = \min \{ n \in \mathbb{Z}^+ \mid a^m = a^n \text{ for some } m, n \in \mathbb{Z}^+ \text{ such that } m < n \}.$$

Thus there is $r \in \mathbb{Z}^+$ such that $r < k$ and $a^r = a^k$. By the property of k, $a, a^2, \ldots, a^{k-1}$ must be distinct. Therefore there exists a unique $r \in \{1, 2, \ldots, k-1\}$ such that $a^r = a^k$. Let $m = k-r$. Thus $a^{m+r} = a^{(k-r)+r} = a^k = a^r$, so $a^r = a^{m+r} = a^m a^r = a^m a^{m+r} = a^{2m+r}$. By multiplying $a^{m+r} = a^r$ successively by a^m, we obtain $a^r = a^{lm+r}$ for all $l \in \{0, 1, 2, \ldots\}$.

Let $n \in \mathbb{Z}^+$.

Case $n \leq r$. Then $a^n \in \{a, a^2, \ldots, a^r, a^{r+1}, \ldots, a^{r+m-1}\}$.

Case $n > r$. Thus there are $l, i \in \mathbb{Z}_0^+$ such that $n-r = lm+i$, $0 \leq i < m$. Then $a^n = a^r a^{n-r} = a^r a^{lm+i} = a^{lm+r+i} = a^{r+i} \in \{a, a^2, \ldots, a^r, \ldots, a^{r+m-1}\}$. Hence $\langle a \rangle = \{a, a^2, \ldots, a^r, a^{r+1}, \ldots, a^{r+m-1}\}$ and the order of a is $k-1 = m+r-1$.

Let $K_a = \{a^r, a^{r+1}, \ldots, a^{r+m-1}\}$. Claim that K_a is a cyclic subgroup of order m. To show that K_a is a subsemigroup of S, let $i, j \in \{0, 1, \ldots, m-1\}$. Thus there exist $p, q \in \mathbb{Z}_0^+$ such that

$r+i+j = pm+q,\ 0 \leqslant q < m.$ Then

$a^{r+i}a^{r+j} = a^{r+(r+i+j)} = a^{r+(pm+q)} = a^{(r+pm)+q} = a^{r+q} \in K_a.$

Define $f: K_a \to (\mathbb{Z}_m,+)$ by $f(a^n) = \bar{n}$. Clearly, f is a homomorphism. To show f is one-to-one, let $n, n' \in \{r, r+1, \ldots, r+m-1\}$ be such that $\bar{n} = \bar{n'}$. Assume $n \geqslant n'$. Then $n-n' = xm$ for some $x \in \mathbb{Z}_0^+$. Thus $a^n = a^{n'+xm} = a^{(n'-r)+(xm+r)} = a^{(n'-r)+r} = a^{n'}$. Hence f is one-to-one. Because f is one-to-one and $\|K_a\| = \|\mathbb{Z}_m\| = m$, f is onto. Thus $K_a \cong (\mathbb{Z}_m,+)$ Since $(\mathbb{Z}_m,+)$ is a cyclic group of order m, K_a is a cyclic group of order m. Observe that there exists a unique $n \in \{r, r+1, \ldots, r+m-1\}$ which is a multiple of m and a^n becomes the identity of K_a and a^{n+1} is a group generator of K_a.

From this we have that some power of every element of S is an idempotent.#

Lemma 1.16. A semigroup which has a left identity and has the property that every element has a left inverse is a group.

Proof. Let S be a semigroup with a left identity e and suppose that every element of S has a left inverse. Claim that $ab = e$ iff $ba = e$ for all $a, b \in S$. To prove this, let $a, b \in S$ be such that $ab = e$. Then $(ba)(ba) = b(ab)a = b(ea) = ba$. Let x be a left inverse of ba. Thus $ba = e(ba) = (xba)(ba) = x(baba) = xba = e$. Thus we have the claim. Since for all $a \in S$ there exists $b \in S$ such that $ba = e$, by the claim $ab = e$. Thus every element of S has a right inverse. Finally, let $a \in S$. Then

$$\begin{aligned} ae &= a(ba) \text{ for some } b \in S \\ &= (ab)a \\ &= ea = a. \end{aligned}$$

Hence e is a right identity of S. Therefore S is a group.#

<u>Definition 1.17</u>. Let S be a semigroup. S is said to be <u>right cancellative</u> iff for all x, y, $z \in S$ $yx = zx$ implies $y = z$. <u>Left cancellativity</u> is similarly defined. A semigroup is <u>cancellative</u> iff it is both left and right cancellative.

<u>Theorem 1.18</u>. Every finite cancellative semigroup is a group.

<u>Proof</u>. Let $G = \{a_1, a_2, \ldots, a_n\}$ be a cancellative semigroup of order n. Pick any a in G. Since $aa_i = aa_j$ implies $a_i = a_j$, the elements $aa_1, aa_2, \ldots, aa_n$ are all distinct. Thus

$$\{aa_1, aa_2, \ldots, aa_n\} = \{a_1, a_2, \ldots, a_n\}.$$

Similarly, we can show that

$$\{a_1a, a_2a, \ldots, a_na\} = \{a_1, a_2, \ldots, a_n\}.$$

Then for all $i \in \{1, 2, \ldots, n\}$ there is an $a_j \in G$ such that $aa_j = a_i$ and there exists an $e \in G$ such that $ea = a$. Hence $ea_i = e(aa_j) = (ea)a_j = aa_j = a_i$ for all $i \in \{1, 2, \ldots, n\}$, so e is a left identity of G. Further, for all $a \in G$ there exists an $a_k \in G$ such that $a_ka = e$. This implies that each element of G has a left inverse. By Lemma 1.16, G is a group.

#