CHAPTER I

PRELIMINARIES

In this thesis we use the following notations

$\mathbb{Z}$ = the set of all integers

$\mathbb{Q}$ = the set of all rational numbers

$\mathbb{R}$ = the set of all real numbers

For $p \in \mathbb{Z}$, $p>0$ $\mathbb{Z}_p$ is the integers modulo p

If $A = \mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$ then $A^+ = \{x \in A \mid x > 0\}$ and $A_a = A \cup \{a\}$

Similarly $A_a^+ = A^+ \cup \{a\}$.

If A and B are sets then $A \subset B$ means that A is a proper subset of B. $A \subseteq B$ signifies set inclusion.

Semirings, Semifields and Division Semirings. A semiring is an ordered triple (S, +, .) such that (S, +) and (S, .) are semi-groups and where for all $x,y,z \in S$ $x(y + z) = xy + xz$ and $(y + z)x = yx + zx$. A semiring (S, +, .) is said to be commutative iff for all $x,y \in S$, $x + y = y + x$ and $xy = yx$. If S is a semiring and for some $a \in S$ $ax = xa = x$ for all $x \in S$, then a is said to be a multiplicative identity for S and is denoted by 1. If $a \in S$ and $ax = a = xa$ for all $x \in S$ then a is said to be a multiplicative zero for S.

Let S be a commutative semiring and $a \in S$. Then $\langle a \rangle = \{sa \mid s \in S\}$

Let S be a semiring and $A \subseteq S$. Then $S + A = \{s + a \mid s \in S, a \in A\}$. Similarly $A + S = \{a + s \mid a \in A, s \in S\}$. If $A = \{x\}$ for some $x \in S$ Then we may write $A + S = x + S$ and $S + A = S + x$. AS is defined to be {as | a ∈ A, s ∈ S} and similarly $SA = \{sa \mid s \in S \text{ and } a \in A\}$

Let S be a commutative semiring with 1. Then S is said to be a <u>semifield</u> iff S has a multiplicative zero a, and $S \setminus \{a\}$ is a group with respect to multiplication.

<u>1.1.1 Theorem</u> : Let S be semifield with a multiplicative zero a, Then either $a + x = x$ for all $x \in S$ or $a + x = a$ for all $x \in S$. These two possibilities are called <u>0-semifields</u> and ∞-semifields respectively. (page 326 ref. 1)

For example any field is a semifield. $\mathbb{Q}^+_\infty$ and $\mathbb{R}^+_\infty$ with the usual addition and multiplication are semifields.

Let (S, +, .) be a commutative semiring with 1 such that (S, .) is a group. Then S is said to be a <u>division semiring</u> . For example $\mathbb{Q}^+$ with the usual addition and multiplication is a division semiring.

<u>1.1.2 Theorem.</u> If S is a division semiring then the order of S (denoted by ||S||) is 1 or is infinite (page 332 reference 1).

If (S, .) is a semigroup and $\sim$ is an equivalence relation on S then $\sim$ is said to be a <u>congruence</u> on S iff for all $x, y, a \in S$, $x \sim y \Rightarrow xa \sim ya$ and $ax \sim ay$. Let (S. +, .) be a semiring and $\sim$ an equivalence relation on S. Then $\sim$ is a congruence on (S, +, .) iff $\sim$ is a congruence on (S. +) and (S, .).

Example. $(\mathbb{Z}^+, +, .)$ with the usual addition is a commutative semiring with 1. Define an equivalence relation on S by saying that $x \sim y$ iff either 2 divides x and 2 divides y or 2 doesn't divide x and 2 doesn't divide y. Then $\sim$ is a congruence on $(\mathbb{Z}^+, +, .)$

Let S be any set. Then $\Delta = \{(x,x) \mid x \in S\}$ is always an equivalence relation. In fact if (S, +, .) is a semiring then Δ is a congruence relation on S. Similarly, S × S, the universal congruence, is always a congruence on S.

If S is a semiring then S is said to be congruence-free iff the only congruences on S are Δ and the universal congruence. Thus Z^+ by the example above is not congrunce free $\mathbb{Q}^+$ and $\mathbb{R}^+$ are congruence free. (page 127 and 128 ref. 2) A semigroup S is said to be congruence-free iff the only congruences on S are Δ and S × S.

Quotient Semifields and Quotient Division Semifields. Let S be a semiring and a ∈ S. Then a is said to be multiplicatively cancellative (or MC) iff either ax = ay or xa = ya implies x = y for all x,y ∈ S. Similarly a is said to be additively cancellative (AC) iff either a + x = a + y or x + a = y + a implies x = y for all x,y ∈ S is said to be MC iff every a ∈ S is MC except for the multiplicative zero (if it exists). S is said to be AC iff all elements in S are AC.

Let S be a MC commutative semiring of order > 1 which has a multiplicative zero a. Then we define the quotient semifield of S (denoted by QS) as follows. Define a relation on (S×S\{a}) by saying that $(x,y) \sim (z,b)$ iff xb = zy. Since S is MC this relation is an equivalence relation. Let $[(x,y)]$ denote the equivalence class of (x,y) (sometimes we use the notation $\frac{x}{y}$ for $[(x,y)]$). For $\alpha, \beta \in S \times S \setminus \{a\}/\sim$ choose $(x,y) \in \alpha$ and $(z,b) \in \beta$ and define $\alpha + \beta = [xb + yz, yb]$. To show that this is well defined suppose $(x_1,y_1) \in \alpha$ and $(z_1,b_1) \in \beta$. Then $[x_1b_1 + y_1z_1, y_1b_1] = [(xb + yz, yb)]$ since $x_1y = y_1x$ and $z_1b = b_1z$ so $(x_1b_1 + y_1z_1)yb = (xb + yz)y_1b_1$ (because $(x_1b_1+y_1z_1)yb = x_1b_1yb + y_1z_1yb = (x_1y)b_1b + (z_1b)\, y_1y = (y_1x)(b_1b) + (b_1z)(y_1y) = y_1b_1\,(xb + yz)$). Define $\alpha\beta = [(x,y)] \cdot [(z,b)] = [(zx, yb)]$

Again $[(zx,yb)] = [(z_1x_1,y_1b_1)]$ since $zxy_1b_1 = (y_1x)(zb_1) = x_1y\,z_1b = (x_1z_1)(yb)$, so multiplication is well defined. $S \times S \setminus \{a\}/\sim$ has a multiplicative identity $[(x,x)]$.

If α is not a multiplicative zero in $S \times S \setminus \{a\}/\sim$. (i.e. $\alpha = [(x,y)]$ where $x \neq a$). Then $\alpha^{-1} = [(y,x)]$. Thus $S \times S \setminus \{a\}/\sim$ which we denote by QS is a semifield. In fact QS is the smallest semifield (up to isomorphism) which contains S. (page 337 ref. 1)

If S is an MC semiring without a multiplicative zero we define $QS = S \times S/\sim$ where $\sim$, addition and multiplication are defined as above. Then QS is a division semiring and is called the quotient <u>division semiring</u> of S. Again QS is the smallest division semiring (up to isomorphism) which contains S. (page 338, ref.1)

Let S be an AC commutative semiring. Then the <u>difference ring</u> of S, denoted by DS, is $S \times S/\sim$ where we say that $(x,y) \sim (a,b)$ iff $x + b = y + a$. (Sometimes we denote $[(x, y)]$ as $x - y$). Since S is AC, $\sim$ is transitive and thus is an equivalence relation on $S \times S$. For $\alpha = [(x,y)]$ and $\beta = [(a,b)] \in DS$ we define $\alpha\beta = [(xa + by, ay + bx)]$ and $\alpha + \beta$ is $[(x + a, b + y)]$. By an argument similar to the one used for QS, addition and multiplication are well defined in DS. Since for any $x \in S$, $[(x,x)]$ is an additive identity in DS and the additive inverse of $[(x,y)]$ is $[(y,x)]$. Thus DS is a ring. In fact DS is the smallest ring (up to isomorphism) which contains S. (page 338 ref.1)

Thus using the definitions above $QZ^+ = Q^+$ and $DZ^+ = Z$.

<u>Partial orders on Rings</u>

A partial order on a ring R is said to be compatible iff :

1) $x \geq y$ implies $a + x \geq a + y$ for all $a,x,y \in R$.

2) $x \geq 0$ and $y \geq 0$ imply $xy \geq 0$ for all $x,y \in R$.

Let $\geq$ be a compatible partial order an a ring R . Then for $x,y \in R$, x is said to be <u>incomparably smaller</u> than y (written $x << y$) iff $n.x \leq y$ for all $n \in \mathbb{Z}\setminus\{0\}$. (Note : if $n \in Z^+$ $n.x$ = x added to itself n times. If $n \in \mathbb{Z}$, $n < 0$ then $n.x = -((-n).x)$.) R is said to be <u>Archimedean</u> with respect to $\geq$ iff no nonzero element in R is incomparably smaller than any other element in R . Thus $\mathbb{Z}$ is Archimedean. Let R and S be rings with $\geq$ and $\geq_1$ compatible partial orders on R and S respectively. Let $\phi : R \to S$ be a ring homomorphism. Then ϕ is said to be <u>isotonic</u> iff $x \geq y$ in R implies $\phi(x) \geq_1 \phi(y)$ in S.

<u>1.1.3 Theorem</u> : Let R be a ring which is Archimedean with respect to a compatible total order $\geq$. Then there exists on isotonic monomorphism $\phi : R \to \mathbb{R}$ (where $\mathbb{R}$ has the usual order).

Proof : See Theorem 3. page 398 in reference III.

<u>Two Easy Theorems</u>.

A <u>group with zero</u> is a semigroup (G,.) such that G has a multiplicative zero a (i.e. $a.x = a = x.a$ for all $x \in G$) and such that $(G\setminus\{a\}, \cdot)$ is a group.

<u>1.1.4 Theorem</u>. Let (S,.) be a commutative congruence-free semigroup with a multiplicative identity 1 with order greater than 1. Then S is a group and $S \cong \mathbb{Z}_p$ for some prime $p \in \mathbb{Z}^+$ or S is a group with zero and $||S|| = 2$.

Proof : $S \supset \{1\}$ since $||S|| > 1$ so we can choose $x \neq 1 \in S$. For $a, b \in S$ say that $a \sim b$ iff $a, b \in \langle x \rangle$ or $a = b$ ($\langle x \rangle = \{ ax \mid a \in S \}$) . Clearly $\sim$ is an equivalence relation on S. Suppose $a \sim b$ and $a \neq b$. Then there exist $s_1, s_2 \in S$ such that $s_1x = a$ and $s_2x = b$. For all $s \in S$, $s(s_1x) \in \langle x \rangle$ and $s(s_2x) \in \langle x \rangle$. Thus $sa, sb \in \langle x \rangle$ so $sa \sim sb$. Therefore $\sim$ is a congruence on S. Since S is congruence-free $\langle x \rangle = \{x\}$ or $\langle x \rangle = S$. If $\langle x \rangle = S$ then $1 \in \langle x \rangle$ so $x^{-1} \in S$. Suppose that $\langle x \rangle = \{x\}$. Then $ax = x$ for all $a \in S$. Thus x is a zero of S. Clearly this can happen for at most one $x \in S$. Thus S is a group or a group with zero.

To finish the proof suppose that S is a group. Since S is congruence free S can have no proper subgroups other than $\{1\}$ since each subgroup of S determines a congruence on S. (i.e. if H is a subgroup of S then $\sim$ defined by $x \sim y$ iff $xy^{-1} \in H$ is a congruence on S). Thus $S \cong \mathbb{Z}_p$ for some prime p. If S is a group with zero then let a be the multiplicative zero in S. Then $(S \setminus \{a\} \times S \setminus \{a\}) \cup \{(a,a)\}$ is a congruence. Thus since S is congruence free $||S \setminus \{a\}|| = 1$.

A similar result applies to rings.

<u>1.1.5 Theorem.</u> Let R be a congruence-free commutative ring with 1. Then R is a field.

Proof : Choose $x \neq 0 \in R$. Say that for $a, b \in R$ $a \sim b$ iff $a - b \in \langle x \rangle$. $\sim$ is clearly a congruence relation on R. Thus $\sim = R \times R$ or $\sim = \Delta$. $(x + x) - x \in \langle x \rangle$ so $\sim \neq \Delta$. Thus $\sim = R \times R$ and thus for all $a, b \in R$, $a - b \in \langle x \rangle$. In particular $1 = 1 - 0 \in \langle x \rangle$. Thus $x^{-1} \in R$.

Thus R is a field. (Note : The converse to this theorem is true and is proved in Chapter IV

Additional Notation and Terminology

Let (S,+,.) be a semiring. Then $a \in S$ is said to be an additive zero iff $a + x = x + a = a$ for all $x \in S$. If for all $x, y \in S$, $x + y = a$ then S is said to have the trivial structure. If for all $x,y \in S$, $x + y = a$ if $x \neq y$ and $x + y = x$ if $x = y$ then S is said to have the almost trivial structure.

Let use make one more convention. Occassionally we use "$\forall$" to denote "for all".