CHAPTER III

SEMIFIELDS

<u>Definition 3.1.</u> A nonempty set K is said to be a <u>semifield</u> if there are two binary operations, + (addition) and $\cdot$ (multiplication) defined on it such that :

(i) $(K, \cdot)$ is an abelian group with zero;

(ii) $(K, +)$ is a commutative semigroup;

(iii) $x(y + z) = xy + xz \quad \forall x, y, z \in K.$

We will denote the multiplicative identity and multiplicative zero of a semifield by 1 and 0 respectively.

It is clear that any field is a semifield.

<u>Example 3.2.</u> Let $(G, \cdot)$ be an abelian group with zero (0). Then we can define a binary operation + on G so that G is a semifield, by defining $x + y = 0 \;\; \forall x, y \in G$. We call this semifield <u>the trivial semifield</u>.

<u>Example 3.3.</u> Let $(G, \cdot)$ be an abelian group with zero. We can define a binary operation + on G so that G is a non-trivial semifield by defining $x + y = 0$ if $x \neq y$ and $x + x = x \;\; \forall x, y \in G$.

<u>Proof</u> : We need to show that $(G, +)$ satisfies the associative law and $(G, +, \cdot)$ satisfies distributive law.

Let $x, y, z \in G$.

<u>Case $x = y = z$.</u> Then $(x + x) + x = x + x = x$ and $x + (x + x) = x + x = x$;

$$x(x + x) = x^2 \text{ and } xx + xx = x^2.$$

<u>Case $x = y \neq z$.</u> Then $(x + x) + z = x + z = 0$ and $x + (x + z) = x + 0 = 0$;

$$x(x + z) = x0 = 0 \text{ and } xx + xz = 0.$$

<u>Case $x = z \neq y$.</u> Then $(x + y) + x = 0 + x = 0$ and $x + (y + x) = x + 0 = 0$;

$$x(y + x) = x0 = 0 \text{ and } xy + xx = 0.$$

<u>Case $x \neq y = z$.</u> Then $(x + y) + y = 0 + y = 0$ and $x + (y + y) = x + y = 0$;

$$x(y + y) = xy \text{ and } xy + xy = xy.$$

<u>Case $x \neq y \neq z$.</u> Then $(x + y) + z = 0 + z = 0$ and $x + (y + z) = x + 0 = 0$;

$$x(y + z) = x0 = 0 \text{ and } xy + xz = 0.$$

Therefore G is a non-trivial semifield. We call this the <u>almost trivial semifield</u>.

<u>Example 3.4.</u> Let D be a P.R.D. Let 0 be a symbol not representing any element of D. Then $D \cup \{0\}$ is clearly a semifield by extending the operations of D to $D \cup \{0\}$ by $x0 = 0x = 0$ and $x + 0 = 0 + x = x$ $\forall x \in D \cup \{0\}$.

<u>Example 3.5.</u> There is another way extending the operation of D to $D \cup \{0\}$ where D is a P.R.D. and $0 \notin D$ so that $D \cup \{0\}$ is a semifield. Just define $x0 = 0x = 0$ and $x + 0 = 0 + x = 0$ $\forall x \in D \cup \{0\}$.

<u>Example 3.6.</u> $\mathbb{Q}^+ \cup \{0\}$ and $\mathbb{R}^+ \cup \{0\}$ with the usual addition and multiplication are semifields.

Remark 3.7. (i) Since $\mathbb{Q}^+$ with the usual addition and multiplication is a P.R.D., follows from Example 3.5, we have $\mathbb{Q}^+ \cup \{0\}$ by extending $+$ and $\cdot$ by $x + 0 = 0 + x = 0$ and $x0 = 0x = 0$ $\forall x \in \mathbb{Q}^+ \cup \{0\}$, is a semifield having 0 as its additive zero.

(ii) $\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, c \in \mathbb{Q}^+ \cup \{0\}, b \in \mathbb{Q}\right\}$ satisfies all the axioms of a semifield except that $\cdot$ is not commutative.

(iii) If K is a semifield then $K \times K$ is not a semifield since $(0, 1)(1, 0) = (0, 0)$.

Definition 3.8. Let K be a semifield. Then define $A = \{x \in K \mid x + y = 0 \ \forall y \in K\}$ and $B_0 = \{x \in K \mid x + 0 = 0\}$.

Follow from previous examples we have that :

(1) $A = K$ and $B_0 = K$ if K is as in Example 3.2 ;

(2) $A = \{0\}$ and $B_0 = K$ if K is as in Example 3.3 ;

(3) $A = \phi$ and $B_0 = \{0\}$ if K is as in Example 3.4 ;

(4) $A = \{0\}$ and $B_0 = K$ if K is as in Example 3.5 ;

If K is a field, then we have $A = \phi$ and $B_0 = \{0\}$.

Theorem 3.9. Let K be a semifield. Then the following hold :

(1) $0 + 0 = 0$

(2) Either $A = \phi$ or $A = \{0\}$ or $A = K$;

(3) Either $B_0 = \{0\}$ or $B_0 = K$.

Proof : (1) Suppose $0 + 0 = x$. Since $0(0 + 0) = 0x$, $0 + 0 = 0$.

(2) Suppose $A \neq \phi$. To show either $A = \{0\}$ or $A = K$, we first assume that $A \neq \{0\}$, so $\exists\, x \in A$ such that $x \neq 0$. Let $y \in K - \{0\}$. Since $x + z = 0$ $\forall z \in K$, $yx^{-1}(x + z) = 0$ $\forall z \in K$. Hence $y + yx^{-1}z = 0$ $\forall z \in K$.

Since $\{yx^{-1}z \mid z \in K\} = K$, $y + w = 0 \ \forall w \in K$. Thus $y \in A$. From (1), $0 + 0 = 0$. If $\exists\, u \in K - \{0\}$ such that $0 + u = w$ for some $w \in K - \{0\}$, then $u \notin A$, a contradiction. Hence $\forall u \in K - \{0\}$, $0 + u = 0$. Therefore $A = K$.

(3) From (1), we have that $0 \in B_0$, so $B_0 \neq \phi$. Assume that $B_0 \neq \{0\}$. Let $x \in B_0 - \{0\}$. Let $y \in K$. Since $x + 0 = 0$, $1 + 0 = 0$. Hence $y + 0 = y1 + y0 = y(1 + 0) = y0 = 0$ and so we have $y \in B_0$. Therefore $B_0 = K$. #

Theorem 3.10. If K is a semifield then either 0 is the additive identity or 0 is the additive zero.

Proof : From Theorem 3.9 (3), we have that either $B_0 = \{0\}$ or $B_0 = K$.
Case $B_0 = K$. Then $\forall x \in K$, $0 + x = 0$ and so 0 is the additive zero.
Case $B_0 = \{0\}$. Then $0 + x \neq 0 \ \forall x \in K - \{0\}$. Let $x \in K - \{0\}$. Hence $\exists\, y \in K - \{0\}$ such that $0 + x = y$ and so $0 + xy^{-1} = 1$. Since $0 + 1 = z$ for some $z \in K - \{0\}$, $0 + 0 + xy^{-1} = 0 + 1 = z$. Hence $0 + xy^{-1} = z$, so $z = 1$ and we get that $0 + 1 = 1$.

Let $y \in K$. Then we have $y(0 + 1) = y$ and so $0 + y = y$. Therefore 0 is the additive identity. #

Theorem 3.10 indicates that there are two types of semifields when considering the multiplicative zero. We call a semifield with 0 as its additive identity a semifield of zero type and a semifield with 0 as its additive zero a semifield of infinity type. The reason for this terminology is as follows :

If 0 is the additive identity, then $x + 0 = x \ \forall x$. Hence 0 behaves like zero in $\mathbb{Q}^+ \cup \{0\}$ with the usual addition and multiplication, so we call it of zero type.

If 0 is the additive zero, then 0 behaves like ∞ in $\mathbb{Q}^+ \cup \{\infty\}$, i.e. $x\infty = \infty$ and $x + \infty = \infty$ $\forall x \in \mathbb{Q}^+ \cup \{\infty\}$, so we call it of infinity type.

Therefore we have $\mathbb{Q}^+ \cup \{0\}$ with the usual addition and multiplication is a semifield of zero type and $\mathbb{Q}^+ \cup \{0\}$ as in Remark 3.7 (i) is a semifield of infinity type.

<u>Proposition 3.11</u>. Let K be a semifield of zero type. If $\exists a_0 \in K - \{0\}$ such that $\forall x, y \in K$ $(x + a_0 = y + a_0 \Rightarrow x = y)$, then $\forall a \in K$ we get that $\forall x, y \in K$ $(x + a = y + a \Rightarrow x = y)$.

<u>Proof</u> : Let $a \in K$. Let $x, y \in K$ be such that $x + a = y + a$. If $a = 0$, then we have $x = y$. So we may assume that $a \neq 0$. Then $a_0a^{-1}(x + a) = a_0a^{-1}(y + a)$. Hence $a_0a^{-1}x + a_0 = a_0a^{-1}y + a_0$. Therefore $a_0a^{-1}x = a_0a^{-1}y$ and so $x = y$. #

<u>Proposition 3.12</u>. Let K be a semifield of zero type. If $\exists x \in K - \{0\}$ such that x has an additive inverse, then every element in K has an additive inverse and K is a field.

<u>Proof</u> : Let $y \in K$. We want to show that y has an additive inverse. If $y = 0$, then we are done because $0 + 0 = 0$. We assume that $y \neq 0$. Let z be an additive inverse of x. Hence $x + z = 0$, so $yx^{-1}(x + z) = 0$. Thus $y + yx^{-1}z = 0$ and $yx^{-1}z$ is an additive inverse of y. #

<u>Theorem 3.13</u>. A finite semifield of zero type of order > 2 is a field.

<u>Proof</u> : Let K be a finite semifield of zero type such that K has order > 2.

<u>Case 1</u>. If $\exists\ x \in K - \{0\}$ such that x has an additive inverse then by Proposition 3.12, every element in K has an additive inverse and so K is a field.

<u>Case 2</u>. Assume that every element in $K - \{0\}$ has no additive inverse. Let $x, y \in K - \{0\}$. Then $x + y \neq 0$, so $x + y \in K - \{0\}$. Hence $(K - \{0\}, +)$ is a commutative semigroup and so $K - \{0\}$ is a finite P.R.D. of order > 1 which contradicts Theorem 2.5. Therefore this case cannot occur. #

<u>Remark 3.14</u>. (i) Theorem 3.13 is not true when K is an infinite semifield since $\mathbb{Q}^+ \cup \{0\}$ of zero type is not a field.

(ii) Theorem 3.13 is not true when K is a semifield of zero type of order 2. For example, let $K = \{0, 1\}$ and let + and $\cdot$ be the following:

$\cdot$	0	1
0	0	0
1	0	1

+	0	1
0	0	1
1	1	1

Then we have that :

$0 + (0 + 1) = 0 + 1 = 1$ and $(0 + 0) + 1 = 0 + 1 = 1$;

$0 + (1 + 0) = 0 + 1 = 1$ and $(0 + 1) + 0 = 1 + 0 = 1$;

$0 + (1 + 1) = 0 + 1 = 1$ and $(0 + 1) + 1 = 1 + 1 = 1$;

$1 + (0 + 0) = 1 + 0 = 1$ and $(1 + 0) + 0 = 1 + 0 = 1$;

$1 + (0 + 1) = 1 + 1 = 1$ and $(1 + 0) + 1 = 1 + 1 = 1$;

$1 + (1 + 0) = 1 + 1 = 1$ and $(1 + 1) + 0 = 1 + 0 = 1$;

$$0(0 + 1) = 01 = 0 \quad \text{and} \quad 00 + 01 = 0 + 0 = 0 \ ;$$
$$0(1 + 0) = 01 = 0 \quad \text{and} \quad 01 + 00 = 0 + 0 = 0 \ ;$$
$$0(1 + 1) = 01 = 0 \quad \text{and} \quad 01 + 01 = 0 + 0 = 0 \ ;$$
$$1(0 + 0) = 10 = 0 \quad \text{and} \quad 10 + 10 = 0 + 0 = 0 \ ;$$
$$1(0 + 1) = 1^2 = 1 \quad \text{and} \quad 10 + 11 = 0 + 1 = 1 \ ;$$
$$1(1 + 0) = 1^2 = 1 \quad \text{and} \quad 11 + 10 = 1 + 0 = 1 \ ;$$
$$1(1 + 1) = 1^2 = 1 \quad \text{and} \quad 11 + 11 = 1 + 1 = 1 \ .$$

Therefore $(K, +)$ is a commutative semigroup, $(K, \cdot)$ is an abelian group with zero and distributive law holds in K, so K is a semifield of zero type but it is not a field.

Corollary 3.15. Any proper extension semifield of semifield in Remark 3.14 (ii) is infinite.

Proof : Suppose $\exists$ K a finite proper extension semifield of semifield in Remark 3.14 (ii). Then K has order > 2. Since $0 + 1 = 1$, by Theorem 3.10 K is of zero type. By Theorem 3.13 K is a field. Since $0 + 1 = 1 + 1$ but $1 \neq 0$, K is not additively cancellative which is a contradiction. #

As a consequence of Remark 3.14 (ii), we see that a semifield of order 2 is an interesting special case of semifields. We wish to study more about semifields of this order and to do this we first find all the possible commutative semigroup operations on $\{0, 1\}$ that make

$\cdot$	0	1
0	0	0
1	0	1

into a semifield.

Since $0 + 0 = 0$, there are four possible commutative binary operations $+$ on $\{0, 1\}$ such that $\{0, 1\}$ is a semifield :

+	0	1
0	0	1
1	1	0

Table 1.

+	0	1
0	0	0
1	0	0

Table 2.

+	0	1
0	0	1
1	1	1

Table 3.

+	0	1
0	0	0
1	0	1

Table 4.

Note that Table 1 makes $\{0, 1\}$ into a field, Table 2 makes $\{0, 1\}$ into the trivial semifield and Table 4 makes $\{0, 1\}$ into the almost trivial semifield. And we have that the only finite semifield of zero type which is not a field is the semifield of table 3.

Table 3 shows that it is possible that a semifield has an additive zero which is not 0.

<u>Proposition 3.16</u>. If K is a semifield of order > 2 such that K has the additive zero e then $e = 0$.

<u>Proof</u> : Suppose $e \neq 0$. Then $x + e = e \quad \forall\, x \in K$, so $e^{-1}x + 1 = 1$ $\forall\, x \in K$. Since $\{e^{-1}x\}_{x \in K} = K$, 1 is also an additive zero. Hence $e = 1$. Let $x \in K - \{0, 1\}$. Then $x + 1 = 1$, so $1 + x^{-1} = x^{-1}$. Since $x^{-1} + 1 = 1$, $x^{-1} = 1$. Thus $x = 1$, a contradiction. #

Table 4 shows that it is possible that a semifield has an additive identity which is not 0.

<u>Proposition 3.17</u>. If K is a semifield of order > 2 such that K has an additive identity e then $e = 0$.

Proof : Suppose $e \neq 0$. Then $x + e = x \ \forall x \in K$, so $e^{-1}x + 1 = e^{-1}x$ $\forall x \in K$. Since $\{e^{-1}x\}_{x \in K} = K$, we see that 1 is also an additive identity and so $1 = e$. Let $x \in K - \{0, 1\}$. Then $x + 1 = x$, so $1 + x^{-1} = 1$. Since $x^{-1} + 1 = x^{-1}$, $x^{-1} = 1$. Thus $x = 1$, a contradiction. #

Table 4 also shows that + and • are equal.

Proposition 3.18. If K is a semifield such that + and • are equal then K has order 2.

Proof : Suppose K has order > 2. Let $x \in K - \{0, 1\}$. Since $x(1 + 1) = x + x$, $x(1^2) = x^2$. Hence $x = x^2$ and x is an idenpotent in $(K, \circ)$. We have that 0 and 1 are the only idenpotents in $(K, \circ)$ since $(K, \cdot)$ is a group with zero, so $x \neq x^2$ which is a contradiction. #

In Chapter II we proved a theorem concerning the smallest sub-P.R.D. of a given P.R.D. Since the intersection of subsemifields of a semifield is a subsemifield, we have that the smallest subsemifield of a semifield exists and is the intersection of all of its subsemifields which will be called the prime semifield. In this chapter we shall also determine the prime semifield of a semifield up to isomorphism. Before studying this we first prove some theorems concerning semirings.

Definition 3.19. If S is a semiring with multiplicative zero (0) and satisfies property that $\forall x, y, z \in S$ $(xy = xz \Rightarrow x = 0 \vee y = z)$, then we say that S is 0-multiplicatively cancellative.

Example 3.20. $\mathbb{N} \cup \{0\}$ with the usual addition and multiplication is an example of a semiring with 0 as multiplicative zero having 0-multiplicative cancellation.

Theorem 3.21. If S is a semiring with multiplicative zero (0), then S can be embedded into a semifield iff S is 0-multiplicatively cancellative.

Proof : Assume that S is 0-multiplicatively cancellative.

Case 1. If $S = \{0\}$, then we can embed S into any semifield K by a homomorphism $\phi : S \longrightarrow K$ defined by $\phi(0) = 0$.

Case 2. Assume that $S \neq \{0\}$. Define a relation $\sim$ on $S \times (S - \{0\})$ by $(x, y) \sim (x', y') \Leftrightarrow xy' = x'y \quad \forall (x, y), (x', y') \in S \times (S - \{0\})$. Clearly $\sim$ is reflexive and symmetric. Let $(a, b), (c, d), (e, f) \in S \times (S - \{0\})$ be such that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad = cb$ and $cf = ed$, so $adf = cbf$ and $cfb = edb$. Hence $adf = edb$. Since $d \neq 0$, $af = eb$. Therefore $(a, b) \sim (e, f)$, so $\sim$ is transitive and hence $\sim$ is an equivalence relation.

Let $\alpha, \beta \in \underline{S \times (S - \{0\})}_{\sim}$. Define + and $\cdot$ on $\underline{S \times (S - \{0\})}_{\sim}$ in the following way : Choose $(a, b) \in \alpha$ and $(c, d) \in \beta$, and let $\alpha + \beta = [(ad + bc, bd)]$ and $\alpha\beta = [(ac, bd)]$. Since $b \neq 0$ and $d \neq 0$, and S is 0-multiplicatively cancellative, $bd \neq 0$ and so $\alpha + \beta$, $\alpha\beta \in \underline{S \times (S - \{0\})}_{\sim}$. As in the proof of Theorem 2.11, we have that + and $\cdot$ are well-defined.

Claim that $(\underline{S \times (S - \{0\})}_{\sim}, +, \cdot)$ is a semifield.

Let $a \in S - \{0\}$ and let $\alpha \in \underline{S \times (S - \{0\})}_{\sim}$. Choose $(c, d) \in \alpha$, then $[(a, a)]\alpha = [(ac, ad)] = [(c, d)] = \alpha$ and $[(0, a)]\alpha = [(0, ad)] = [(0, a)]$, so $[(a, a)]$ is the multiplicative identity and

$[(0, a)]$ is the multiplicative zero, $\forall\, a \in S - \{0\}$. Let $\mathfrak{p} \in \underset{\sim}{\underline{S \times (S - \{0\})}} - \{[(0, a)] \mid a \in S - \{0\}\}$. Choose $(c, d) \in \mathfrak{p}$, then $[(d, c)]$ is the multiplicative inverse of $\mathfrak{p}$. Clearly the associative law, commutative law and distributive law all hold in $\underset{\sim}{\underline{S \times (S - \{0\})}}$, so we have that $\underset{\sim}{\underline{S \times (S - \{0\})}}$ is a semifield.

Fix $a \in S - \{0\}$. Define $\theta : S \longrightarrow \underset{\sim}{\underline{S \times (S - \{0\})}}$ by $\theta(s) = [(sa, a)]$ $\forall\, s \in S$. Let $s_1, s_2 \in S$. Then $\theta(s_1 + s_2) = [((s_1 + s_2)a, a)] = [(s_1a + s_2a, a)][(a, a)] = [(s_1a^2 + s_2a^2, a^2)] = [(s_1a, a)] + [(s_2a, a)] = \theta(s_1) + \theta(s_2)$ and $\theta(s_1s_2) = [(s_1s_2a, a)] = [(s_1s_2a^2, a^2)] = [(s_1a, a)][(s_2a, a)] = \theta(s_1)\theta(s_2)$. Let $s_1, s_2 \in S$ be such that $\theta(s_1) = \theta(s_2)$. Then $[(s_1a, a)] = [(s_2a, a)]$ and so $s_1a^2 = s_2a^2$. Since $a \neq 0$, $s_1 = s_2$. Hence θ is a monomorphism, so we can embed S into a semifield.

Conversly, assume that S can be embedded into a semifield K. Let $x, y, z \in S$ be such that $xy = xz$. If $x = 0$, then we are done. Suppose that $x \neq 0$, then $x^{-1}xy = x^{-1}xz$. Hence $y = z$. #

<u>Remark 3.22.</u> If S has a multiplicative identity 1, then $\exists$ a canonical monomorphism from S into $\underset{\sim}{\underline{S \times (S - \{0\})}}$ defined by $\theta(s) = [(s, 1)]$ $\forall s \in S$.

<u>Proposition 3.23.</u> If S is a semiring with multiplicative zero (0) having 0-multiplicative cancellation of order > 1, then $\underset{\sim}{\underline{S \times (S - \{0\})}}$ is the smallest semifield containing S up to isomorphism.

<u>Proof</u> : Let K be a semifield containing S.
Define $\theta : \underset{\sim}{\underline{K \times (K - \{0\})}} \longrightarrow K$ in the following way : Let $\alpha \in \underset{\sim}{\underline{K \times (K - \{0\})}}$. Choose $(a, b) \in \alpha$ and let $\theta(\alpha) = ab^{-1}$. As we

already showed in the proof of Proposition 2.13, we have that θ is well-defined and θ is an isomorphism.

Define $\phi : \underset{\sim}{\underline{S \times (S - \{0\})}} \longrightarrow \underset{\sim}{\underline{K \times (K - \{0\})}}$ in the following way : Let $\alpha \in \underset{\sim}{\underline{S \times (S - \{0\})}}$. Choose $(a, b) \in \alpha$ and let $\phi(\alpha) = [(a, b)]'$ where $[(a, b)]'$ is the equivalence class of (a, b) in $K \times (K - \{0\})$. Clearly ϕ is a monomorphism. Hence $\underset{\sim}{\underline{S \times (S - \{0\})}}$ is isomorphic to a subsemifield of $\underset{\sim}{\underline{K \times (K - \{0\})}}$. Since $K \cong \underset{\sim}{\underline{K \times (K - \{0\})}}$, we get that $\underset{\sim}{\underline{S \times (S - \{0\})}}$ is isomorphic to a subsemifield of K and $\underset{\sim}{\underline{S \times (S - \{0\})}}$ is the smallest semifield containing S up to isomorphism. #

$\mathbb{N} \cup \{0\}$ with the usual addition and multiplication is an example of a semiring with 0 as multiplicative zero having 0-multiplicative cancellation. We also see that 0 is also the additive identity for this semiring.

If we extend + on $\mathbb{N}$ with the usual addition and multiplication to $\mathbb{N} \cup \{0\}$ by $n + 0 = 0 + n = 0$ and $0n = n0 = 0$ $\forall n \in \mathbb{N} \cup \{0\}$, then $\mathbb{N} \cup \{0\}$ is also a semiring with 0 as multiplicative and additive zero having 0-multiplicative cancellation.

<u>Corollary 3.24</u>. Let S be a semiring of order > 1 with multiplicative zero (0) having 0-multiplicative cancellation. Then the following hold :

(1) If 0 is the additive identity, then the smallest semifield containing S also has 0 as the additive identity.

(2) If 0 is the additive zero then the smallest semifield containing S also has 0 as the additive zero.

<u>Proof</u> : From Proposition 3.23, we have that $\underset{\sim}{\underline{S \times (S - \{0\})}}$ up to isomorphism is the smallest semifield containing S and 0 corresponds with $[(0, a)]$ $\forall a \in S - \{0\}$ in $\underset{\sim}{\underline{S \times (S - \{0\})}}$.

Let $a \in S - \{0\}$ and $\alpha \in \underset{\sim}{\underline{S \times (S - \{0\})}}$. Choose $(c, d) \in \alpha$.

If 0 is the additive identity for S, then $[(0, a)] + \alpha = [(ac, ad)] = [(c, d)] = \alpha$. Hence $[(0, a)]$ is the additive identity for $\underset{\sim}{\underline{S \times (S - \{0\})}}$ and we have (1).

If 0 is the additive zero for S, then $[(0, a)] + \alpha = [(0, ad)] = [(0, a)]$. Hence $[(0, a)]$ is the additive zero for $\underset{\sim}{\underline{S \times (S - \{0\})}}$ and we have (2). #

Now we shall determine the prime semifield of a semifield up to isomorphism.

<u>Theorem 3.25</u>. If K is a semifield of zero type, then the prime semifield of K is either isomorphic to $\mathbb{Q}^+ \cup \{0\}$ with the usual addition and multiplication or $\mathbb{Z}_p$ where p is a prime number or the semifield in Table 3, page 25 . Furthermore if the prime semifield of K is isomorphic to $\mathbb{Z}_p$ for some prime p, then K is a field by Proposition 3.12.

<u>Proof</u> : Let K' be the prime semifield of K. Let $n \in \mathbb{N} \cup \{0\}$. Then define $n1 = 1 + 1 + \ldots + 1$ (n times) if $n \neq 0$ and $n1 = 0$ if $n = 0$, so we have $\{n1\}_{n \in \mathbb{N} \cup \{0\}} \subseteq K'$.

<u>Case $\forall$ m, n $\in \mathbb{N} \cup \{0\}$ if $m \neq n$, then $m1 \neq n1$.</u>

By Proposition 3.23, $\underset{\sim}{\underline{(\mathbb{N} \cup \{0\}) \times \mathbb{N}}}$ is the smallest semifield containing $\mathbb{N} \cup \{0\}$ with the usual addition and multiplication.

And we have that $\underset{\sim}{\underline{(\mathbb{N}\cup\{0\}) \times \mathbb{N}}} \cong \mathbb{Q}^{+}\cup\{0\}$ with the usual addition and multiplication.

Define $\phi : \mathbb{N}\cup\{0\} \longrightarrow K$ by $\phi(n) = n1$ $\forall n \in \mathbb{N}\cup\{0\}$. Then clearly we have that ϕ is a monomorphism. Hence $\phi(\mathbb{N}\cup\{0\}) \cong \mathbb{N}\cup\{0\}$, so up to isomorphism $\underset{\sim}{\underline{\phi(\mathbb{N}\cup\{0\}) \times \phi(\mathbb{N})}}$ is the smallest subsemifield of K containing $\phi(\mathbb{N}\cup\{0\})$. Since $0, 1 \in K'$, $n1 \in K'$ $\forall n \in \mathbb{N}\cup\{0\}$. Hence $\phi(\mathbb{N}\cup\{0\}) \subseteq K'$, so we have that up to isomorphism $\underset{\sim}{\underline{\phi(\mathbb{N}\cup\{0\}) \times \phi(\mathbb{N})}} \subseteq K'$. Since $\underset{\sim}{\underline{\phi(\mathbb{N}\cup\{0\}) \times \phi(\mathbb{N})}}$ is a subsemifield of K, up to isomorphism we have that $K' \subseteq \underset{\sim}{\underline{\phi(\mathbb{N}\cup\{0\}) \times \phi(\mathbb{N})}}$. Therefore $K' \cong \underset{\sim}{\underline{\phi(\mathbb{N}\cup\{0\}) \times \phi(\mathbb{N})}}$.

Let $\theta : \underset{\sim}{\underline{(\mathbb{N}\cup\{0\}) \times \mathbb{N}}} \rightarrow \underset{\sim}{\underline{\phi(\mathbb{N}\cup\{0\}) \times \phi(\mathbb{N})}}$ be defined in the following way : Let $\alpha \in \underset{\sim}{\underline{(\mathbb{N}\cup\{0\}) \times \mathbb{N}}}$. Choose $(m, n) \in \alpha$ and let $\theta(\alpha) = [(\phi(m), \phi(n))]$. It is clear that θ is well-defined and is an isomorphism. Thus $K' \cong \underset{\sim}{\underline{\phi(\mathbb{N}\cup\{0\}) \times \phi(\mathbb{N})}} \cong \underset{\sim}{\underline{(\mathbb{N}\cup\{0\}) \times \mathbb{N}}} \cong$ $\mathbb{Q}^{+}\cup\{0\}$ with the usual addition and multiplication.

<u>Case $\exists\, m, n \in \mathbb{N}\cup\{0\}$, $m < n$ and $m1 = n1$.</u>

Let $m_o = \min.\{m \in \mathbb{N}\cup\{0\} \mid \exists\, n \in \mathbb{N}\ \ n > m$ such that $m1 = n1\}$ and let $n_o = \min.\{n \in \mathbb{N} \mid n > m_o$ and $m_o 1 = n1\}$.

(1) Suppose that $m_o = 1$ and $n_o = 2$. Then $1 = 1 + 1$. Since $0 + 1 = 1$, we have that $\{0, 1\}$ as in Table 3, page 25 is a subsemifield of K. Hence $K' \cong \{0, 1\}$ as in Table 3, page 25.

(2) Assume that $m_o \neq 1$ or $n_o \neq 2$.

(2.1) Suppose that $m_o \neq 1$. Then there are two cases to consider either $m_o = 0$ or $m_o > 1$.

If $m_o = 0$, then n_o can not be 1 since $0 \neq 1$, so $n_o > 1$. Suppose

$n_o = 2$, then $0 = 1 + 1$. Since $0 + 1 = 1$, we have that $\{0, 1\} \cong \mathbb{Z}_2$ is a subsemifield of K. So in this case we have that $K' \cong \mathbb{Z}_2$. Suppose that $n_o > 2$, then $n_o - 1 \geqslant 2$ and $\forall\, m \in \mathbb{N} \cup \{0\}$, $ml \in \{nl\}_{0 \leqslant n \leqslant n_o - 1}$ ——— (a)

If $m_o > 1$, then $n_o > 2$, so $n_o - 1 \geqslant 2$ and $\forall\, m \in \mathbb{N} \cup \{0\}$, $ml \in \{nl\}_{0 \leqslant n \leqslant n_o - 1}$ ——— (b)

(2.2) Suppose that $n_o \neq 2$. Again n_o can not be 0 or 1, so $n_o > 2$. Hence $n_o - 1 \geqslant 2$ and $\forall\, m \in \mathbb{N} \cup \{0\}$, $ml \in \{nl\}_{0 \leqslant n \leqslant n_o - 1}$ ——— (c)

From (a), (b), (c), we see that in all these cases $n_o > 2$ and $\forall\, m \in \mathbb{N} \cup \{0\}$, $ml \in \{nl\}_{0 \leqslant n \leqslant n_o - 1}$. From now on we shall assume that the cases (a), (b), (c) hold.

Let $B = \{nl \mid nl \neq 0,\ n \in \mathbb{N}\}$. Then $2 \leqslant |B| < \infty$.

Let $C = \{(nl)(ml)^{-1} \mid nl,\ ml \in B\}$. Again $2 \leqslant |C| < \infty$ and $0 \notin C$.

Claim that $C \cup \{0\}$ is a subsemifield of K.

We first show that if $m_1 1, m_2 1 \in B$, then $(m_1 m_2)1 \in B$. To prove this, we let $m_1 1, m_2 1 \in B$. Since $m_1 1 \neq 0$ and $m_2 1 \neq 0$, $(m_1 1)(m_2 1) \neq 0$. Hence $(m_1 m_2)1 \neq 0$.

Let $(n_1 1)(m_1 1)^{-1}, (n_2 1)(m_2 1)^{-1} \in C$. Then

$$\begin{aligned}
(n_1 1)(m_1 1)^{-1} + (n_2 1)(m_2 1)^{-1} &= (n_1 1)(m_1 1)^{-1}(m_2 1)(m_2 1)^{-1} + (n_2 1)(m_2 1)^{-1}(m_1 1)(m_1 1)^{-1} \\
&= ((n_1 1)(m_2 1) + (n_2 1)(m_1 1))((m_1 1)^{-1}(m_2 1)^{-1}) \\
&= ((n_1 m_2)1 + (n_2 m_1)1)((m_2 1)(m_1 1))^{-1} \\
&= ((n_1 m_2 + m_1 n_2)1)((m_1 m_2)1)^{-1}.
\end{aligned}$$

If $(n_1 m_2 + m_1 n_2)1 = 0$, then $(n_1 1)(m_1 1)^{-1} + (n_2 1)(m_2 1)^{-1} = 0 \in C \cup \{0\}$. If $(n_1 m_2 + m_1 n_2)1 \neq 0$, then $(n_1 m_2 + m_1 n_2)1 \in B$ and so we have that $(n_1 1)(m_1 1)^{-1} + (n_2 1)(m_2 1)^{-1} \in C$. Since $0 + x = x \ \ \forall x \in K$, $(C \cup \{0\}, +)$ is a subsemigroup of $(K, +)$.

Let $(n_1 1)(m_1 1)^{-1}, (n_2 1)(m_2 1)^{-1} \in C$. Then
$((n_1 1)(m_1 1)^{-1})((n_2 1)(m_2 1)^{-1}) = (n_1 1)(n_2 1)(m_1 1)^{-1}(m_2 1)^{-1} = (n_1 1)(n_2 1)((m_2 1)(m_1 1))^{-1}$
$= ((n_1 n_2)1)((m_1 m_2)1)^{-1}$. Since $n_1 1, n_2 1, m_1 1, m_2 1 \in B$, $(m_1 m_2)1, (n_1 n_2)1 \in B$
so $((n_1 n_2)1)((m_1 m_2)1)^{-1} \in C$. Since $(m_1 1)(n_1 1)^{-1} \in C$ and
$((m_1 1)(n_1 1)^{-1})((n_1 1)(m_1 1)^{-1}) = 1$, we have that $\forall x \in C$, $x^{-1} \in C$. Thus $(C, \cdot)$ is a subgroup of $(K - \{0\}, \cdot)$. Therefore we have the claim and clearly $C \cup \{0\}$ is also of zero type.

Since $2 < |C \cup \{0\}| < \infty$, by Theorem 3.13 $C \cup \{0\}$ is a field. We have that $K' \subseteq C \cup \{0\}$ since K' is the prime semifield of K. Since $0, 1 \in K'$, $n1 \in K'$ $\forall n \in \mathbb{N} \cup \{0\}$. Hence $B \cup \{0\} \subseteq K'$ and so $C \cup \{0\} \subseteq K'$. Thus $K' = C \cup \{0\}$ and so $K' \cong \mathbb{Z}_p$ for some prime p.

Therefore if K is a semifield that has property (a) or (b) or (c), then $K' \cong \mathbb{Z}_p$ for some prime $p > 2$ and K is a field. #

<u>Theorem 3.26</u>. If K is a semifield of infinity type, then the prime semifield of K is either isomorphic to $\mathbb{Q}^+ \cup \{0\}$ in Remark 3.7 (i) or the trivial semifield of order 2 or the almost trivial semifield of order 2.

<u>Proof</u> : Let K' be the prime semifield of K. Since $0 + x = 0$ $\forall x \in K$, $0 \in A$ where $A = \{x \in K \mid x + y = 0 \ \ \forall y \in K\}$. Hence $A \neq \phi$. By Theorem 3.9 (2), we have that either $A = \{0\}$ or $A = K$.

<u>Case $A = K$</u>. Then $1 + 1 = 0$ and we have $0 + 1 = 0$. Thus $\{0, 1\}$ is the trivial semifield of order 2 and the trivial semifield on $\{0, 1\} \cong K'$.

<u>Case $A = \{0\}$</u>. Let $n \in \mathbb{N} \cup \{0\}$. Then define $n1 = 1 + 1 + \ldots + 1$ (n times) if $n \neq 0$ and $n1 = 0$ if $n = 0$. Hence we have that $\{n1\}_{n \in \mathbb{N} \cup \{0\}} \subseteq K'$.

Subcase $\forall$ m, n $\in \mathbb{N} \cup \{0\}$ if $m \neq n$, then $m1 \neq n1$.

Let $B = \{(n1)(m1)^{-1}\}_{m, n \in \mathbb{N}}$. Then by the isomorphism $\theta : \mathbb{Q}^+ \longrightarrow B$ given by $\theta(\frac{m}{n}) = (m1)(n1)^{-1}$ we have that $B \cong \mathbb{Q}^+$ with the usual addition and multiplication. Since $0 + x = 0 \ \forall x \in B \cup \{0\}$, we have that $B \cup \{0\} \cong \mathbb{Q}^+ \cup \{0\}$ as in Remark 3.7 (i). Therefore $B \cup \{0\}$ is a subsemifield of K and so $K' \subseteq B \cup \{0\}$ since K' is the prime semifield of K. Since $0, 1 \in K'$, $n1 \in K' \ \forall n \in \mathbb{N} \cup \{0\}$. Hence $B \cup \{0\} \subseteq K'$. Thus $K' = B \cup \{0\} \cong \mathbb{Q}^+ \cup \{0\}$ as in Remark 3.7 (i).

Subcase $\exists$ m, n $\in \mathbb{N} \cup \{0\}$, $m < n$ and $m1 = n1$.

Let $m_o = \min.\{m \in \mathbb{N} \cup \{0\} \mid \exists n \in \mathbb{N} \quad n > m$ such that $m1 = n1\}$ and let $n_o = \min.\{n \in \mathbb{N} \mid n > m_o$ and $m_o1 = n1\}$.

(1) If $m_o = 1$ and $n_o = 2$, then $1 + 1 = 1$ and we have that $K' = \{0, 1\}$ with the almost trivial structure.

(2) Assume that $m_o \neq 1$. There are two cases to consider, either $m_o = 0$ or $m_o > 1$. Suppose $m_o = 0$, then $n_o \geqslant 2$ since $1 \neq 0$. If $n_o = 2$, then $K' = \{0, 1\}$ with the trivial structure. Hence we left to consider the case $m_o = 0$ and $n_o > 2$ ____________ (a)

Claim that $\forall$ $k \geqslant n_o$, $k1 = 0$.

We will prove this claim by using induction on $k \geqslant n_o$. We have that $n_o1 = 0$. Let $k \in \mathbb{N}$ be such that $k > n_o$ and assume that $\forall$ j, $n_o \leqslant j < k$, $j1 = 0$. Thus $k1 = (k - 1)1 + 1 = 0 + 1 = 0$. Therefore by mathematical induction we have the claim.

Since $n_o \geqslant 3$, $n_o^2 \geqslant 3n_o$. Hence $n_o^2 + 1 \geqslant 3\,n_o$ and so $n_o^2 - 2n_o + 1 \geqslant n_o$. By the claim we have that $((n_o - 1)1)((n_o - 1)1) =$

$(n_o^2 - 2n_o + 1)1 = 0$ which is a contradiction since $(n_o - 1)1 \in K - \{0\}$ and $(K - \{0\}, \cdot)$ is a group. Therefore (a) cannot occur. Hence $m_o > 1$ and so $n_o > 2$.

Let $B = \{m1\}_{m \in \mathbb{N}}$. Then $2 \leqslant |B| < \infty$ and $0 \notin B$. Let $C = \{(m1)(n1)^{-1}\}_{m, n \in \mathbb{N}}$. Then $2 \leqslant |C| < \infty$ and clearly C is a P.R.D. which contradicts Theorem 2.5. Therefore the case $m_o > 1$ also cannot occur.

(3) From (1) and (2) we then left to consider the case $m_o = 1$ and $n_o \neq 2$. Hence n_o cannot be 1 since $n_o \neq m_o$, so $n_o > 2$.

Claim that $\exists\, n \in \mathbb{N}$ such that n1 has no multiplicative inverse.

Suppose this claim is not true, then $\forall\, n \in \mathbb{N}$, n1 has a multiplicative inverse. Let $B = \{m1\}_{m \in \mathbb{N}}$. Then $2 \leqslant |B| < \infty$ and $0 \notin B$. Let $C = \{(m1)(n1)^{-1}\}_{m, n \in \mathbb{N}}$. Again we have that $2 \leqslant |C| < \infty$ and $0 \notin C$. Clearly C is a P.R.D. which contradicts Theorem 2.5. Hence we have the claim and $\exists\, n' \in \mathbb{N}$ such that $n'1$ has no multiplicative inverse. Hence $n'1 = 0$. Then $m_o = 0$ which is a contradiction since $m_o = 1$, so this case cannot occur and we have the theorem. #

Example 3.27. $\mathbb{Q}^+ \cup \{0\}$ with the usual multiplication is a group with zero 0. Let + be defined by $x + y = \max.\{x, y\}$ $\forall x, y \in \mathbb{Q}^+ \cup \{0\}$. Then $\mathbb{Q}^+ \cup \{0\}$ is a semifield of zero type and $0 + 1 = 1 + 0$, $1 + 1 = 1$, so its prime semifield is isomorphic to Table 3, page 25.

If we define + on $\mathbb{Q}^+ \cup \{0\}$ by $x + y = \min.\{x, y\}$ $\forall$ x, $y \in \mathbb{Q}^+ \cup \{0\}$, then we have $\mathbb{Q}^+ \cup \{0\}$ is a semifield of infinity type and $1 + 0 = 0 + 1 = 0$, $1 + 1 = 1$, so its prime semifield is isomorphic to the almost trivial semifield of order 2.

Remark 3.28. From Theorem 3.13 we know that a finite semifield of zero type of order ≥ 2 is a field. If we drop the condition that + is commutative in the definition of a semifield, then we can have a finite semifield of zero type of order > 2 which is not a field since for any abelian group G with zero and + defined by $x + y = x$ if x, $y \neq 0$ and $x + 0 = 0 + x = x$ satisfies all the axioms of a semifield except + is not commutative.

Also, if we define + by $x + y = x$ if x, $y \neq 0$ and $x + 0 = 0 + x = 0$, then we have that G is a semifield of infinity type.

In fact, even if $\cdot$ is not commutative then the + defined above distribute over $\cdot$ on both sides so we could get a non-commutative semifield.