CHAPTER III

SEMIRINGS

This chapter will study congruences and partial congruences on semirings, skew rings, P.R.D.'s and semifields.

3.1. Semirings.

First we shall give the same definition of a semiring as given in[5] without assuming additive identity and multplicative zero.

Definition 3.1.1 A semiring is a triple $(S,+,\cdot)$ where S is a set and + (addition), $\cdot$ (multiplication) are binary operations on S such that

i) $(S,\cdot)$ and $(S,+)$ are semigroups,

ii) $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all $x,y,z \in S$.

Remark: A semiring is an algebraic system.

Example Let $(S,\cdot)$ be a semigroup. Define a binary operation + on S by $x + y = x$ for all $x,y \in S$ (or $x + y = y$ for all $x,y \in S$). Then clearly $(S,+,\cdot)$ is a semiring.

Remark: Let $(S,+,\cdot)$ be a semiring. If + is commutative then we shall call S an additively commutative semiring. If . is commutative then we we shall call S a multiplicatively commutative semiring. If + and $\cdot$ are commutative then we shall call S a commutative semiring.

Definition 3.1.2 Let S, S' be semirings. A semiring homomorphism from S to S' is a map $\phi : S \to S$ such that $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(a.b) = \phi(a).\ \phi(b)$ for all $a, b \in S$.

Remark: A semiring homomorphism is an operation preserving map.

This section will consider the following categories :

1) The category $\mathcal{S}_r$ of semirings and semiring homomorphisms.

2) The category $\mathcal{S}_{r,i}$ of semirings and semiring isomorphisms.

We shall define naturally equivalent contravariant functors from $\mathcal{S}_r$ to $\mathcal{L}$ by using congruences and quotient semirings which are defined below.

Remark: We can prove that if ρ is an operation preserving equivalence relation on a semiring $(S,+,\cdot)$ then the set S/ρ of equivalence classes of S can be made into a semiring in natural way and the natural projection map $\pi : S \to S/\rho$ is an onto semiring homomorphism. Hence the definition of a congruence on an object $(S,+,\cdot)$ in $\mathcal{S}_r$ (or $\mathcal{S}_{r,i}$) is the same as the definition of an operation preserving equivalence relation on the semiring $(S,+,\cdot)$.

Definition 3.1.3 A quotient semiring of a semiring S is a pair (K,ϕ) where K is a semiring and $\phi : S \to K$ is an onto semiring homomorphism.

Example $(S/\rho,\pi)$ is a quotient semiring of a semiring S where ρ is a congruence on S.

Theorem 3.1.4 Let S be a semiring and (K,ϕ) a quotient semiring of S. Let $\rho = \{(a,b) \in S \times S | \phi(a) = \phi(b)\}$. Then ρ is a congruence on S and there exists an isomorphism $\psi: S/\rho \to K$ such that the following diagram commutes

$$\begin{tikzcd} & S \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\ S/\rho \arrow[rr, "\psi"'] & & K \end{tikzcd}$$

Proof. It is similar to the proof of Theorem 2.1.2.

Definition 3.1.5 Let (K,ϕ) and (K',ϕ') be quotient semirings of a semiring S. Say that (K,ϕ) is strongly equivalent to (K',ϕ') iff there exists an isomorphism $\psi: K \to K'$ such that the following diagram is commutative

$$\begin{tikzcd} & S \arrow[dl, "\phi"'] \arrow[dr, "\phi'"] & \\ K \arrow[rr, "\psi"'] & & K' \end{tikzcd}$$

Write this as $(K,\phi) \approx (K',\phi')$

Remarks: 1) $\approx$ is an equivalence relation on the set of quotient semiring of a semiring.

2) For each quotient semiring (K,ϕ) of a semiring S, $(K,\phi) \approx (S/\rho,\pi)$ where $\rho = \{(a,b) \in S \times S | \phi(a) = \phi(b)\}$.

Proposition 3.1.6 Let $\phi : S \to S'$ be a semiring homomorphism. If ρ' is a congruence on S' then $(\phi \times \phi)^{-1}(\rho')$ is a congruence on S.

Fix a semiring S let C(S) = the set of congruences on S,
Q(S) = the set of equivalence classes of
quotient semirings of S under $\approx$.

We define natural relations $\subsetneq$ on C(S), Q(S) as $\subsetneq$ on C(S), Q(S) in Section 2.1 respectively. Then the proof that $(C(S), \subseteq)$ and $(Q(S), \subseteq)$ are posets is similar to the proof that $(C(S), \subsetneq)$ and $(Q(S), \subsetneq)$ in Section 2.1 are posets respectively.

Theorem 3.1.7 For each semiring S the posets C(S) and Q(S) are isomorphic.

Proof. It is similar to the proof of Theorem 2.1 5 and the isomorphism has the same form as in Theorem 2.1.5.

We can show that for each semiring S $(C(S), \subsetneq)$ and $(Q(S), \subsetneq)$ are lattices as we showed that for each semigroup S $(C(S), \subsetneq)$ and $(Q(S), \subsetneq)$ are lattices respectively.

We define contravariant functors C, Q from $\mathcal{S}_r$ to $\mathcal{L}$ as the contravariant functors C,Q from $\mathcal{S}_g$ to $\mathcal{L}$ in Section 2.1 respectively. The proof that C is naturally equivalent to Q is similar to the proof that C is naturally equivalent to Q in Section 2.1.

หอสมุดกลาง สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย

Remark: C is the congruence functor of $\mathcal{S}_r$.

Now we shall define naturally equivalent covariant functors from $\mathcal{S}_{r,i}$ to $\mathcal{Q}$ using equivalence classes of congruences and equivalence classes of quotient semirings which are defined below.

Definition 3.1.8 Let ρ_1 and ρ_2 be congruences on a semiring S. Say that ρ_1 is equivalent to ρ_2 ($\rho_1 \sim \rho_2$) iff there exists an automorphism $f:S \to S$ such that $(f \times f)(\rho_1) = \rho_2$.

Remark: $\sim$ is an equivalence relation on the set of congruences on a semiring.

Definition 3.1.9 Let (K,ϕ) and (K',ϕ') be quotient semirings of a semiring S. Say that (K,ϕ) is weakly equivalent to (K',ϕ') iff there exist isomorphisms $f:S \to S$ and $f':K \to K'$ such that the following diagram is commutative.

$$\begin{tikzcd}
S \arrow[r, "f"] \arrow[d, "\phi"'] & S \arrow[d, "\phi'"] \\
K \arrow[r, "f'"'] & K'
\end{tikzcd}$$

Write this as $(K,\phi) \sim (K',\phi')$.

Remarks: 1) $\sim$ is an equivalence relation on the set of quotient semiring of a semiring.

2) $(K,\phi) \cong (K',\phi')$ implies that $(K,\phi) \sim (K',\phi')$.

Fix a semiring S let $C^*(S) =$ the set of equivalence classes of congruences on S under $\sim$,

$Q^*(S) =$ the set of equivalence classes of quotient semirings of S under $\sim$.

We define binary relations $\leqslant$ on $C^*(S)$ and $Q^*(S)$ as $\leqslant$ on $C^*(S)$ and $Q^*(S)$ in Section 2.1 respectively. Then the proof that $(C^*(S), \leqslant)$ and $(Q^*(S), \leqslant)$ are quasi-ordered sets is similar to the proof that $(C^*(S), \leqslant)$ and $(Q^*(S), \leqslant)$ are quasi-ordered sets in Section 2.1 respectively.

Theorem 3.1.10 For each semiring S the quasi-ordered sets $C^*(S)$, $Q^*(S)$ are isomorphic.

Proof. It is similar to the proof of Theorem 2.1.8 and the isomorphism has the same form as in Theorem 2.1.8.

We define covariant functors C^*, Q^* from $\mathcal{S}_{r,i}$ to $\mathcal{Q}$ as the covariant functors C^*, Q^* from $\mathcal{S}_{r,i}$ to $\mathcal{Q}$ in Section 2.1 respectively. Then the proof that C^* is naturally equivalent to Q^* is similar to the proof that C^* is naturally equivalent to Q^* in Section 2.1.

Next we shall consider some theorems which use congruences on semirings.

Theorem 3.1.11 Every additive congruence on $\mathbb{N}$ is a multiplicative congruence also ie. ρ is a congruence on $(\mathbb{N},+)$ iff ρ is a congruence on $(\mathbb{N},+,\cdot)$.

Proof. Let ρ be a congruence on the semigroup $(\mathbb{N},+)$. We must show that ρ is a congruence on the semigroup $(\mathbb{N},\cdot)$. Clearly ρ is an equivalence relation on $\mathbb{N}$. Let $x,y \in \mathbb{N}$ such that $x \,\rho\, y$. To prove that $(n\cdot x) \,\rho\, (n.y)$ $\forall\, n \in \mathbb{N}$ by induction. If $n = 1$ then clearly $(n.x) \,\rho\, (n.y)$. Suppose $(k.x) \,\rho\, (k.y)$. We shall show that $((k + 1) \cdot x) \,\rho\, ((k + 1) \cdot Y)$. Because $(k.x) \,\rho\, (k.y)$, $(k.x + x) \,\rho\, (k.y + x)$ Since $(k.y + x) \,\rho\, (k.y + y)$ and ρ is transitive, $(k.x + x) \,\rho\, (k.y + y)$ ie. $((k + 1).x) \,\rho\, ((k + 1).y)$. Hence $n.x \sim n.y$ $\forall\, n \in \mathbb{N}$. Therefore ρ is a congruence on $(\mathbb{N},\cdot)$. Thus ρ is a congruence on $(\mathbb{N},+,\cdot)$. #

Corollary 3.1.12 Let $m_o,n_o \in \mathbb{N}$ be such that $m_o < n_o$ and $<(m_o,n_o)>$ denote the congruence on the semiring $(\mathbb{N},+,\cdot)$ generated by (m_o,n_o). Then

$<(m_o,n_o)> = \{(a,a) \mid a \in \mathbb{N}\} \cup$

$\{(a,b) \in \mathbb{N} \times \mathbb{N} \mid \exists\, k \in \mathbb{N} \ni a+km_o=b+kn_o \text{ and } b \geqslant m_o \text{ or } a+kn_o=b+km_o \text{ and } a \geqslant m_o\}$

Corollary 3.1.13 Let ρ be a congruence on $(\mathbb{N},+,\cdot)$. Then ρ is generated by one element.

Definition 3.1.14 Let $(S,+,\cdot)$ be a semiring. Say that $(S,+,\cdot)$ is additively cancellative (A.C.) iff $x + y = x + z$ or $y + x = z + x$ implies that $y = z$ for all $x,y,z \in S$. Say that $(S,+,.)$ is multiplicatively cancellative (M.C.) iff $x.y = x.z$ or $y.x = z.x$ implies that $y = z$ for all $x,y, z \in S$.

Definition 3.1.15 Let S be a commutative semiring and $x \in S$. Then x is said to be additively cancellative iff $x + y = x + ~~y~~ z$ implies that $y = z$

for all $y,z \in S$. And an additively cancellative x is said to be <u>partially additively cancellative</u> iff for each $s \in S$ $s.x$ is additively cancellative .

<u>Theorem 3.1.16</u> There exists an extension semiring of an A.C. and M.C. commutative semiring S with a partially additively cancellative element such that every partially additively cancellative element in S has an inverse.

<u>Proof</u>. Let S be an A.C. and M.C. commutative semiring with a partially additively cancellative element a. Let U = the set of partially additively cancellative elements of S. Then clearly U is an ideal in S. Define the binary operations $+, \cdot$ on $S \times U$ by $(s,u) + (s',u') = (s + s', u + u')$ and $(s,u) \, . \, (s',u') = (ss' + uu', su' + s'u)$. Then $(S \times U,+,\cdot)$ is a commutative semiring. Define a relation $\sim$ on $S \times U$ by $(s,u) \sim (s',u')$ iff $s + u' = s' + u$. We shall show that $\sim$ is a congruence on $S \times U$. Clearly $\sim$ is reflexive and symmetric. Let $(s,u) \sim (s',u')$ and $(s',u') \sim (s'',u'')$. Then $s + u' = s' + u$ and $s' + u'' = s'' + u'$ so $s+ u' + u'' = s' + u + u'' = s' + u'' + u = s'' + u' + u$ hence $(s + u'') + u' = (s'' + u) + u'$. Since $u' \in U$, $s + u'' = s'' + u$ ie $(s,u) \sim (s'',u'')$. Therefore $\sim$ is transitive. Let $(s,u) \sim (s',u')$ then $s + u' = s' + u$. Let $(s'',u'') \in S \times U$ so $s'' + s + u'' + u' = s'' + s' + u'' + u$ ie. $(s'',u'') + (s,u) \sim (s'',u'') + (s',u')$. Because $s''s + s''u' = s''s' + s''u$ and $u''s + u''u' = u''s' + u''u$, $s''s + u''u + s''u' + s'u'' = s''s' + u''u' + s''u + su''$ ie. $(s''s + u''u, s''u + su'') \sim (s''s' + u''u', s''u' + s'u'')$ so $(s'',u'').(s,u) \sim (s'',u'').(s',u')$. Hence $\sim$ is a congruence on $S \times U$.

Next we shall show that $(S{\times}U)/\sim$ is an extension semiring of S such that every element in U has an additive inverse. Fix $u \in U$. Define

$\phi : S \to (S\times U)/\sim$ by $\phi(a) = [(a + u,u)]$. Clearly ϕ is a 1-1 homomorphism Hence S is isomorphic to a subsemiring of $(S\times U)/\sim$. Now we shall show that $\forall\, x \in U$ x has an additive inverse in $(S\times U)/\sim$. We have that $\forall\, x \in U$ $[(x,x)]$ is the identity of $((S\times U)/\sim,+)$. Let $x \in U \subsetneq S$. Because $\phi(x) = [(x + u,u)]$, $\phi(x) + [(u,x + u)] = [(x + u,u)] + [(u,x + u)] = [(x + 2u, x + 2u)]$. Hence $-(\phi(x)) = [(u, x + u)] \in (S\times U)/\sim$

#

Remark: The above construction can be applied to any ideal of U.

Review 1) Let S be a commutative semiring with multiplicative identity 1. Then S is embeddable in a ring iff S is A.C.

2) Let R be a commutative ring with multiplicative identity 1. Then R is an integral domain iff R is M.C. ie $x.y = x.z$ implies that $y = z$ for all $y,z \in R$, $x \in R\setminus\{0\}$.

Next we shall show that it is not true that for each commutative semiring S with 1 if S is A.C. and M.C. then S is embeddable in an integral domain.

Theorem 3.1.17 There exists a commutative semiring S with 1 which is A.C. and M.C.and cannot be embedded in an integral domain.

Proof. Let R be an integral domain and $x \in R$ be such that $x^2+ 1 = 2x$. Because $x^2- 2x + 1 = 0$, $(x - 1)^2= 0$ so $x - 1 = 0$ ie. $x = 1$. We shall construct a commutative semiring with 1 which is A.C. and M.C. and contains an element x such that $x^2+ 1 = 2x$ and $x \neq 1$. Then clearly such a semiring cannot be embedded in an integral domain. Let $\mathbb{N}_o[X]$ be the semiring of polynomials with coefficients in $\mathbb{N}_o$. Define a relation $\sim$ on $\mathbb{N}_o[X]$ as follows: say that $F \sim G$ if $\exists\ K,L \in \mathbb{N}_o[X]$ such that $F+(X^2+1)K + 2XL = G+(X^2+1)L + 2XK$. Clearly $\sim$ is a congruence on $\mathbb{N}_o[X]$. Let $S = \mathbb{N}_o[X]/\sim$. Define binary operations $+,\cdot$ on S as follows: given $\alpha,\beta \in S$ choose $F \in \alpha$, $G \in \beta$ then let $\alpha+\beta = [F+G]$ and $\alpha.\beta = [F.G]$. Hence $(S,+,\cdot)$ is a commutative semiring with multiplicative identity $[1]$. Clearly S is A.C. Now we shall show that S is M.C. Let $\alpha,\beta,\gamma \in S$ be such that $\alpha.\gamma = \beta.\gamma$ and $\gamma \neq 0$. Must show that $\alpha=\beta$. Choose $F \in \alpha$, $G \in \beta$ and $H \in \gamma$ so $H \neq 0$. Then $F.H \sim G.H$ so $\exists\ K,L \in \mathbb{N}_o[X]$ such that

$$F.H + (X^2+1).K + 2X.L = G.H + (X^2+1).L + 2X.K \quad .....(*)$$

If H is invertible then done. We may assume that H is not invertible. We can consider $(*)$ as an equation in $\mathbb{Z}[X]$. We get that

$$(F-G).H = (X-1)^2.(L-K) \quad ....(**)$$

Since $\mathbb{Z}$ is U.F.D., $\mathbb{Z}[X]$ is U.F.D. (by Theorem in [3]). Since $H \neq 0$ and H is not invertible, H has irreducible factors. Let P be an irreducible factor of H. Since $\mathbb{Z}[X]$ is a U.F.D., P must be an irreducible factor of R.H.S. of $(**)$. Hence either $P = X-1$ or P is an irreducible factor of $L-K$. If $P = X-1$ then $X-1$ is a factor of H so $H = (X-1).Q$ for some $Q \in \mathbb{Z}[X]$. Then $H(1) = 0$ which is a contradiction. Hence $P \neq X-1$. So P is an irreducible factor of $L-K$. Hence $H|(L-K)$, so $\exists\ R \in \mathbb{Z}[X]$ such that $L-K = H.R$ then $(**)$ becomes

$$(F - G).H \quad = \quad (X - 1)^2.R.H \qquad \text{..........(***)}$$

Because (***) is an equation in $\mathbb{Z}[X]$ and $\mathbb{Z}[X]$ is M.C. and $H \neq 0$, we have that

$$F - G \quad = \quad (X - 1)^2.R$$

Because $R \ \varepsilon \mathbb{Z}[X]$, $\exists \ S,T \ \varepsilon \ \mathbb{N}_0 [X]$ such that $R = S - T$ so we have

$$F - G \quad = \quad (X - 1)^2(S - T)$$

Hence $F \sim G$ ie. $\alpha = \beta$. Therefore S is M.C.

Let $x = [X]$ so $x \ \varepsilon \ S$. Claim that $x^2 + 1 = 2x$. Note that if $X^2 + 1 \sim 2X$ then $[X]^2 + 1 = 2[X]$ ie. $x^2 + 1 = 2x$. So to prove the claim we must show that $X^2 + 1 \sim 2X$. Let $K = 1$, $L = 2$ then we get that $X^2 + 1 \sim 2X$ so we have the claim. To finish the proof we must show that $x \neq 1$ ie. $X \not\sim 1$. Suppose not, so $X \sim 1$ then $\exists \ K,L \ \varepsilon \ \mathbb{N}_0[X]$ such that $X = (X^2 + 1)K + 2XL = 1 + (X^2 + 1)L + 2XK$. Consider this to be an equation in $\mathbb{Z}[X]$. Hence $X - 1 = (X - 1)^2(L - K)$.

<u>case 1</u> $L - K = 0$ so $X - 1 = 0$ which is a contradiction

<u>case 2</u> $L - K \neq 0$. Because $\deg (X - 1) = 1$ but $\deg((X - 1)^2.(L - K)) \geqslant 2$ which is a contradiction. Therefore $X \not\sim 1$ ie. $x \neq 1$.

#

3.2 <u>Semi-modules</u>

In this section we shall work with left congruences on a semiring S. But everything that we prove for left congruences can be similarly proved for right congruences. As in Section 3.1, we shall consider the categories $\mathcal{S}_r$ and $\mathcal{S}_{r,i}$.

We shall define naturally equivalent contravariant functors from $\mathcal{S}_r$ to $\mathcal{L}$ and naturally equivalent covariant functors from $\mathcal{S}_{r,i}$ to $\mathcal{Q}$ by using the following pairs which are defined below.

1) double left congruences and double left semigroup-spaces,

2) multiplicative left congruences and multiplicative left semi-modules,

3) additive left congruences and additive left semi-modules.

Definition 3.2.1 A double left congruence on a semiring $(S,+,\cdot)$ is an equivalence relation ρ on S such that $x \rho y$ implies that $(a + x)\rho(a + y)$ and $(a.x)\rho(a.y)$ for all $a,x,y \in S$.

Definition 3.2.2 A multiplicative left congruence on a semiring $(S,+,\cdot)$ is an equivalence relation ρ on S such that $x \rho y$ implies that $(a + x) \rho (a + y)$, $(x + a) \rho (y + a)$ and $(a.x) \rho (a.y)$ for all $a,x,y \in S$.

Definition 3.2.3 An additive left congruence on a semiring $(S,+,\cdot)$ is an equivalence relation ρ on S such that $x \rho y$ implies that $(a + x) \rho (a + y)$, $(a.x)\rho(a.y)$ and $(x.a)\rho(y.a)$ for all $a,x,y \in S$.

Definition 3.2.4 Let S be a semiring. A double left S-space is a triple $(M,+,\cdot)$ where $(M,+)$ and $(M,\cdot)$ are left S-space such that $r(s + m) = r.s + r.m$ for all $m \in M$, $r,s \in S$.

Definition 3.2.5 Let $(S,+,\cdot)$ be a semiring. A multiplicative left S-semimodule is a triple $(M,+,\cdot)$ where $(M,+)$ is a semigroup, $(M,\cdot)$ is a left S-space such that $r.(n + m) = r.n + r.m$ for all $r \in S$, $m,n \in M$.

Definition 3.2.6 Let $(S,+,\cdot)$ be a semiring. An additive left S-semimodule is a triple $(M,+,\cdot)$ where $(M,+)$ is a left S-space, $(M,\cdot)$ is a semigroup.

Remark: For each semiring S , S is a double left S-space and multiplicative (additive) left S-semimodule.

Next we shall only work with double left congruences. But everything that we prove for double left congruences can be similarly proved for multiplicative left congruences and additive left congruences.

Definition 3.2.7 Let S be a semiring, M,M' double left S-spaces and $\phi:M \to M'$ a map. Then ϕ is said to be double left S-equivariant iff $\phi(s + m) = s + \phi(m)$ and $\phi(s.m) = s.\phi(m)$ for all $s \in S$, $m \in M$.

Remarks 1) If ϕ is a bijectively double left S-equivalent map then ϕ^{-1} is double left S-equivalent. We shall call a map a double left S-space isomorphism.

2) If ρ is a double left congruence on a semiring $(S,+,\cdot)$ then the set S/ρ of equivalence classes of S can be made into a double left S-space in natural way and the natural projection map $\pi:S \to S/\rho$

.is an onto double left S-equivariant map.

Definition 3.2.8 Let S be a semiring. A quotient double left S-space is a pair (K,ϕ) where K is a double left S-space and $\phi:S \to K$ is an onto double left S-equivariant map.

Example $(S/\rho,\pi)$ is a quotient double left S-space where ρ is a double left congruence on S.

Theorem 3.2.9 Let S be a semiring and M a double left S-space. Let $\phi:S \to M$ be an onto double left S-equivariant map and $\rho = \{(a,b) \in S \times S \mid \phi(a) = \phi(b)\}$. Then ρ is a double left congruence on S and there exists a double left S-space isomorphism ψ from S/ρ onto M such that the following diagram commutes

$$\begin{tikzcd}
 & S \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\
S/\rho \arrow[rr, "\psi"'] & & M
\end{tikzcd}$$

Proof. It is similar to the proof of Theorem 2.1.2.

Definition 3.2.10 Let S be a semiring. Let (K,ϕ) and (K',ϕ') be quotient double left S-spaces. Say that (K,ϕ) is strongly equivalent to (K',ϕ') iff there exists a double left S-space isomorphism $\psi:K \to K'$ such that the following diagram commutes

$$\begin{tikzcd} & S \arrow[dl, "\phi"] \arrow[dr, "\phi'"] & \\ K \arrow[rr, "\psi"'] & & K' \end{tikzcd}$$

Write this as $(K,\phi) \approx (K',\phi')$

Remarks: 1) $\approx$ is an equivalence relation on the set of quotient double left S-spaces.

2) For each quotient double left S-space (K,ϕ), $(K,\phi) \approx (S/\rho,\pi)$ where $\rho = \{(a,b) \in S \times S \mid \phi(a) = \phi(b)\}$

Fix a semiring S, let LC(S) = the set of double left congruences on S,

LQ(S) = the set of equivalence classes of quotient double left S-spaces under $\approx$.

We define natural relations $\subsetneq$ on LC(S), LQ(S) as $\subsetneq$ on C(S) and Q(S) in Section 3.1, respectively. Then the proof that (LC(S), $\subsetneq$) and (LQ(S), $\subsetneq$) are posets is similar to the proof that (C(S), $\subsetneq$) and (Q(S), $\subsetneq$) are posets, respectively.

Theorem 3.2.11 For each semiring S the posets LC(S) and LQ(S) are isomorphic.

Proof. It is similar to the proof of Theorem 3.17, and the isomorphism has the same form as in Theorem 3.1.7.

Remark: Fix a semiring S .Let $\rho_1, \rho_2 \in LC(S)$. Then $\rho_1 \cap \rho_2 =$ g.l.b.$\{\rho_1, \rho_2\}$ and the double left congruence on S generated by $\rho_1 \cup \rho_2 =$ l.u.b. $\{\rho_1, \rho_2\}$. Hence LC(S) is a lattice. Therefore LQ(S) is a lattice also.

We define contravariant functors LC and LQ from $\mathcal{S}_r$ to $\mathcal{L}$ as we defined the contravariant functors C and Q from $\mathcal{S}_r$ to $\mathcal{L}$ in Section 3.1, respectively. Then the proof that LC is naturally equivalent to LQ is similar to the proof that C is naturally equivalent to Q.

Definition 3.2.12 Let ρ_1 and ρ_2 be double left congruences on a semiring S. Say that ρ_1 is equivalent to $\rho_2(\rho_1 \sim \rho_2)$ iff there exists a semiring automorphism $\phi : S \to S$ such that $(\phi \times \phi)(\rho_1) = \rho_2$.

Remark: $\sim$ is an equivalence relation on the set of double left congruences on a semiring.

Definition 3.2.13 Let (K,ϕ) and (K',ϕ') be quotient double left S-space where S is a semiring. Say that (K,ϕ) is weakly equivalent to (K',ϕ') iff there exist a semiring automorphism $f : S \to S$ and a double left S-space isomorphism $f' : K \to K'$ such that the following diagram commutes

$$\begin{tikzcd}
S \arrow[r, "f"] \arrow[d, "\phi"'] & S \arrow[d, "\phi'"] \\
K \arrow[r, "f'"'] & K'
\end{tikzcd}$$

Write this as $(K,\phi) \sim (K',\phi')$

Remarks: 1) $\sim$ is an equivalence relation on the set of quotient double left S-spaces.

2) $(K,\phi) \cong (K',\phi')$ implies that $(K,\phi) \sim (K',\phi')$.

Fix a semiring S, let $LC^*(S)$ = the set of equivalence classes of double left congruence on S,

$LQ^*(S)$ = the set of equivalence classes of quotient double left S-spaces under $\sim$.

We define binary relations $\leqslant$ on $LC^*(S)$ and $LQ^*(S)$ as $\leqslant$ on $C^*(S)$ and $Q^*(S)$ in Section 3.1, respectively. Then the proof that $(LC^*(S),\leqslant)$ and $(LQ^*(S),\leqslant)$ are quasi-ordered sets is similar to the proof that $(C^*(S),\leqslant)$ and $(Q^*(S),\leqslant)$ are quasi-ordered sets.

Theorem 3.2.14 For each semiring S, the quasi-ordered sets $LC^*(S)$ and $LQ^*(S)$ are isomorphic.

Proof. It is similar to the proof of Theorem 3.1.10 and the isomorphism has the same form as in Theorem 3.1.10.

We define covariant functors LC^* and LQ^* from $\mathcal{S}_{r,i}$ to $\mathcal{Q}$ as we defined the covariant functors C^* and Q^* from $\mathcal{S}_{r,i}$ to $\mathcal{Q}$ in Section 2.1, respectively. Then the proof that LC^* is naturally equivalent to LQ^* is similar to the proof that C^* is naturally equivalent to Q^*.

3.3 Skew Rings.

Definition 3.3.1 A skew ring is a semiring $(R,+,\cdot)$ such that $(R,+)$ is a group. We shall let 0 denote the additive identity of $(R,+)$.

Remark: A skew ring is an algebraic system.

Examples 1) Let $(G,+)$ be a group with 0 as its identity. Define a binary operation $\cdot$ on G by $x.y = 0$ for all $x,y \varepsilon G$. Then $(G,+,\cdot)$ is a skew ring which we shall call a zero skew ring.

2) Every ring is a skew ring.

Definition 3.3.2 Let R,R' be skew ring. A skew ring homomorphism from R to R' is a map $\phi:R \to R'$ such that $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(a.b) = \phi(a).\phi(b)$ for all $a,b \varepsilon R$.

This section will consider the following subcategories of $\mathcal{S}_r$:

1) The category $\mathcal{R}$ of skew rings and skew ring homomorphisms.

2) The category $\mathcal{R}_o$ of skew rings and onto skew ring homomorphisms.

3) The category $\mathcal{R}_i$ of skew rings and skew ring isomorphisms.

We shall show that $\mathcal{R}$ has a congruence set so we shall define naturally equivalent contravariant functors from $\mathcal{R}$ to $\mathcal{L}$ by using congruences, ideals and quotient skew rings which are defined below.

Remark: If ρ is an operation preserving equivalence relation on a skew ring R. then the set R/ρ of equivalence classes of R can be made into a akew ring in natural way and the natural projection map $\pi : R \to R/\rho$ is an onto skew ring homomorphism. Hence the definition of a congruence on an object $(R,+,\cdot)$ in $\mathcal{R}$ is the same as the definition of an operation preserving equivalence relation on the skew ring $(R,+,\cdot)$.

Definition 3.3.3 An ideal I of a skew ring R $(I \trianglelefteq R)$ is an additive subgroup of R such that $a + i - a \varepsilon I$ and $a.i, i.a \varepsilon I$ for all $a \varepsilon R$, $i \varepsilon I$.

Examples 1) Let ρ be a congruence on a skew ring R. Then $[0]_\rho = \{a \varepsilon R | a\rho o\} \trianglelefteq R$.

2) Let I be an ideal of a skew ring R. Then $\{(a,b) \varepsilon R \times R | a - b \varepsilon I\}$ is a congruence on R.

Definition 3.3.4 A quotient skew ring of a skew ring R is a pair (K,ϕ) where K is a skew ring and $\phi : R \to K$ is an onto skew ring homomorphism.

Examples 1) $(R/\rho,\pi)$ is a quotient skew ring of a skew ring R where ρ is a congruence on R.

2) Let I be an ideal of a skew ring R. Let $\rho = \{(a,b) \varepsilon R \to R | a - b \varepsilon I\}$ and $R/I = R/\rho$. Then $(R/I,\pi)$ is a quotient skew ring of R.

Theorem 3.3.5 Let (K,ϕ) be a quotient skew ring of a skew ring R and

$\rho = \{(a,b) \varepsilon R \times R | \phi(a) = \phi(b)\}$. Then ρ is a congruence on R and there exists an automorphism $\psi: R/\rho \to K$ such that $\psi \circ \pi = \phi$.

Proof. It is similar to the proof of Theorem 2.1.2.

Theorem 3.3.6 Let $\phi: R \to R'$ be an onto skew ring homomorphism. Then $\ker\phi \triangleleft R$ and there exists a natural isomorphism $\psi: R/\ker\phi \to R'$ such that the following diagram is commutative

$$\begin{tikzcd}
& R \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\
R/\ker\phi \arrow[rr, "\psi"'] & & R'
\end{tikzcd}$$

Proof. It is similar to the proof of Theorem 2.3.3.

We shall call the above Theorem the first isomorphism Theorem of Skew ring theory.

Definition 3.3.7 Let (K,ϕ) and (K',ϕ') be quotient skew rings of a skew ring R. Say that (K,ϕ) is strongly equivalent to (K',ϕ') iff there exists an isomorphism $\psi: K \to K'$ such that the following diagram is commutative

$$\begin{tikzcd}
& R \arrow[dl, "\phi"'] \arrow[dr, "\phi'"] & \\
K \arrow[rr, "\psi"'] & & K'.
\end{tikzcd}$$

Write this as $(K,\phi) \simeq (K',\phi')$.

Remarks 1) $\simeq$ is an equivalence relation on the set of quotient skew rings of a skew ring.

2) For each quotient skew ring (K,ϕ) of a skew ring R, $(K,\phi) \simeq (R/\rho,\pi)$ where $\rho = \{(a,b) \in R \times R \mid \phi(a,) = \phi(b)\}$.

3) For each quotient skew ring (K,ϕ) of a skew ring R, $(K,\phi) \simeq (R/\ker \phi,\pi)$.

Proposition 3.3.8 Let $\phi: R \to R'$ be a skew ring homomorphism. If ρ' is a congruence on R' then $(\phi \times \phi)^{-1}(\rho')$ is a congruence on R. If I' is an ideal of R' then $\phi^{-1}(I')$ is an ideal of R.

Proposition 3.3.9 Let $\phi: R \to R'$ be an onto skew ring homomorphism. If ρ is a congruence on R then $(\phi \times \phi)(\rho)$ is a congruence on R'. If I is an ideal of R then $\phi(I)$ is an ideal of R'.

Proof. It is similar to the proof of Proposition 2.3.6.

Fix a skew ring R let $C(R)$ = the set of congruences on R,
$I(R)$ = the set of ideals of R,
$Q(R)$ = the set of equivalence classes of quotient skew rings of R under $\simeq$.

We define natural relations $\subsetneq$ on $C(R)$, $I(R)$, $Q(R)$ as $\subsetneq$ on $C(G)$, $N(G)$, $Q(G)$ in Section 2.3, respectively. Then the proof that $(C(R),\subsetneq)$, $(I(R),\subsetneq)$, $(Q(R),\subsetneq)$ are posets is similar to the proof that $(C(G),\subsetneq)$, $(N(G),\subsetneq)$, $(Q(G),\subsetneq)$ are posets respectively.

Theorem 3.3.10 For each skew ring R the posets C(R), Q(R), I(R) are isomorphic.

Proof. It is similar to the proof of Theorem 2.3.7, Theorem 2.3.8 and the isomorphisms have the same form as in Theorem 2.3.7, Theorem 2.3.8.

Proposition 3.3.11 Let I_1,I_2 be ideals of a skew ring R. Then $I_1+ I_2= \{i_1+ i_2 | i_1 \varepsilon I_1, i_2 \varepsilon I_2\}$ is the ideal of R generated by $I_1 \cup I_2$

Proof. It is standard.

Proposition 3.3.12 Let ρ_1,ρ_2 be congruences on a skew ring R. Then $\rho_1+ \rho_2 = \{(a_1,b_1)+(a_2,b_2) | (a_1,b_1) \varepsilon \rho_1,(a_2,b_2) \varepsilon \rho_2\}$ is the congruence on R generated by $\rho_1 \cup \rho_2$.

Proof. We can show that $\rho_1+ \rho_2$ is an equivalence relation on R as we showed that $\rho_1 \cdot \rho_2$ is an equivalence relation on G in the proof of Proposition 2.3.14. Let $(a,b) \varepsilon \rho_1+ \rho_2$ and $c \varepsilon R$. Then $a = a_1+ a_2$, $b = b_1+ b_2$ where $(a_1,b_1) \varepsilon \rho_1$, $(a_2,b_2) \varepsilon \rho_2$. So $(c + a, c + b) =(c+a_1, c + b_1)+(a_2,b_2) \varepsilon \rho_1+ \rho_2$, $(a + c,b + c) = (a_1,b_1)(a_2+ c,b_2+ c) \varepsilon \rho_1 + \rho_2$,$(ca,cb) = (ca_1,cb_1)+(ca_2,cb_2) \varepsilon \rho_1+ \rho_2$ and $(a_1c,b_1c)+(a_2c,b_2c) \varepsilon \rho_1+ \rho_2$. Hence $\rho_1+ \rho_2$ is a congruence on R. It is easy to show that $\rho_1+ \rho_2$ is the congruence on R generated by $\rho_1 \cup \rho_2$. #

We shall show that $(C(R),\subseteq)$, $(I(R),\subseteq)$ and $(Q(R),\subseteq)$ are lattices for all skew rings R. Let R be a skew ring. Let $I_1, I_2 \in I(R)$. Then $I_1 \cap I_2 = \text{g.l.b.}\{I_1, I_2\}$ and $I_1 + I_2 = \text{l.u.b.}\ \{I_1, I_2\}$. Hence $(I(R), \subseteq)$ is a lattice. Let $\rho_1, \rho_2 \in C(R)$. Then $\rho_1 \cap \rho_2 = \text{g.l.b.}\{\rho_1, \rho_2\}$ and $\rho_1 + \rho_2 = \text{l.u.b.}\ \{\rho_2, \rho_2\}$. Hence $(C(R), \subseteq)$ is a lattice. Therefore $(Q(R), \subseteq)$ is a lattice also.

We define contravariant functors C,I,Q from $\mathcal{R}$ to $\mathcal{L}$ as the contravariant functors C,N,Q from $\mathcal{G}$ to $\mathcal{L}$ in Section 2.3, respectively. Then the proof that C,I,Q are naturally equivalent is similar to the proof that C,N,Q are naturally equivalent in Section 2.3.

Remark As a result we see that C is the congruence functor of $\mathcal{R}$ and $\mathcal{R}$ has a congruence set and ideals of a skew ring are congruence sets with respect to I.

Next we shall define covariant functors C', I', Q' from $\mathcal{R}_o$ to $\mathcal{L}$ as the covariant functors C', N', Q' from $\mathcal{G}_o$ to $\mathcal{L}$ in Section 2.3 respectively. Then the proof that C', I', Q' are naturally equivalent covariant functors is similar to the proof that C', N', Q' are naturally equivalent covariant functors in Section 2.3.

Now we shall define naturally equivalent covariant functors from $\mathcal{R}_i$ to $\mathcal{Q}$ using equivalence classes of congruences, equivalence classes of ideals and equivalence classes of quotient skew rings which are defined below.

Definition 3.3.13 Let ρ_1 and ρ_2 be congruences on a skew ring R. Say that ρ_1 is equivalent to ρ_2 ($\rho_1 \sim \rho_2$) iff there exists an automorphism $f:R \to R$ such that $(f \times f)(\rho_1) = \rho_2$.

Remark: $\sim$ is an equivalence relation on the set of congruences on a skew ring.

Definition 3.3.14 Let I_1 and I_2 be ideals of a skew ring R. Say that I_1 is equivalent to $I_2 (I_1 \sim I_2)$ iff there exists an automorphism $f:R \to R$ such that $f(I_1) = I_2$.

Remark: $\sim$ is an equivalence relation on the set of ideals of a skew ring.

Definition 3.3.15 Let (K,ϕ) and (K',ϕ') be quotient skew rings of a skew ring R. Say that (K,ϕ) is weakly equivalent to (K',ϕ') iff there exist isomorphisms $F:R \to R$ and $f:K \to K'$ such that the following diagram is commutative

$$\begin{tikzcd}
R \arrow[r, "F"] \arrow[d, "\phi"'] & R \arrow[d, "\phi'"] \\
K \arrow[r, "f"] & K'
\end{tikzcd}$$

Write this as $(K,\phi) \sim (K',\phi')$.

Remarks: 1) $\sim$ is an equivalence relation on the set of quotient skew rings of a skew ring.

2) $(K,\phi) \simeq (K',\phi')$ implies that $(K,\phi) \sim (K',\phi')$.

Fix a skew ring R let $C^*(R)$ = the set of equivalence classes
of congruences on R under $\sim$,
$I^*(R)$ = the set of equivalence classes
of ideals of R under $\sim$,
$Q^*(R)$ = the set of equivalence
classes of quotient skew rings
or R under $\sim$.

We define binary relations $\leqslant$ on $C^*(R), I^*(R)$, $Q^*(R)$ as $\leqslant$ on $C^*(G)$, $N^*(G)$, $Q^*(G)$ in Section 2.3 respectively. Then the proof that $(C^*(R),\leqslant)$, $(I^*(R),\leqslant),(Q^*(R),\leqslant)$ are quasi-ordered sets is similar to the proof that $(C^*(G),\leqslant)$, $(N^*(G),\leqslant)$, $(Q^*(G),\leqslant)$ are quasi-ordered sets respectively.

Theorem 3.3.16 For each skew ring R the quasi-ordered sets $C^*(R)$, $I^*(R)$, $Q^*(R)$ are isomorphic.

Proof. It is similar to the proofs of Theorem 2.3.15 Theorem 2.3.16. and the isomorphisms have the same form as in Theorem 2.3.15, Theorem 2.3.16.

We define covariant functors C^*, I^*, Q^* from $\mathcal{R}_i$ to $\mathcal{Q}$ as the covariant functors C^*, N^*, Q^* from $\mathcal{S}_i$ to $\mathcal{Q}$ in Section 2.3 respectively. Then the proof that $C^*, I^* Q^*$ are naturally equivalent covariant functors is similar to the proof that C^*, N^*, Q^* are naturally equivalent covariant functors in Section 2.3.

Remark: We can prove that the following subcategories of $\mathcal{R}$ have a congruence set as we proved that $\mathcal{R}$ has a congruence set:

1) The category of rings and ring-homomorphisms.

2) The category of commutative rings and ring-homomorphisms.

Next we shall consider some Theorems which use ideals (ie. congruence sets)

Let R_1 and R_2 be skew rings. Let $R = R_1 \times R_2$ and define binary operations +, $\cdot$ on R as follows: $(x_1,x_2)+(y_1,y_2) = (x_1+y_1,x_2+y_2)$ and $(x_1,x_2)\cdot(y_1,y_2) = (x_1 \cdot y_1,x_2 \cdot y_2)$. Then clearly $(R,+,\cdot)$ is a skew ring. Let $S_1 = \{(x,0) \mid x \in R_1\}$ and $S_2 = \{(0,y) \mid y \in R_2\}$. Then

1) S_1 and S_2 are ideals in R,

2) $S_1 \cap S_2 = \{(0,0)\}$,

3) S_1 and S_2 generate R.

หอสมุดกลาง สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย

Theorem 2.3.17 Let R be a skew ring having two ideals S_1, S_2 such that $S_1 \cap S_2 = \{0\}$ and S_1, S_2 generate R. Then $R \cong S_1 \times S_2$.

Proof. Claim 1. $\forall s_1 \in S_1 \, \varepsilon \forall s_2 \in S_2 \quad s_1 \cdot s_2 = s_2 \cdot s_2 = 0.$ To prove this, let $s_1 \in S_1$ and $s_2 \in S_2$. Because $S_1 \trianglelefteq R$ and $S_2 \trianglelefteq R$, $s_1 s_2 \in S_1$ and $s_1 s_2 \in S_2$ so $s_1 s_2 \in S_1 \cap S_2 = \{0\}$ hence $s_1 s_2 = 0$.

Similarly $s_2s_1 = 0$. Hence we have the claim 1. Claim 2. $\forall s_1 \varepsilon S_1$ $\forall s_2 \varepsilon S_2$ $s_1+ s_2= s_2+ s_1$. To prove this, lets $s_1 \varepsilon S_1$ and $s_2 \varepsilon S_2$. Then $s_1+ s_2- s_1 \varepsilon S_2$ and $s_2- s_1- s_2 \varepsilon S_1$ hence $s_1+ s_2- s_1- s_2 \varepsilon S_1 \cap S_2 = \{0\}$. Therefore $s_1+ s_2- s_1- s_2 = 0$ ie. $s_1+ s_2 = s_2 + s_1$ hence we have the claim 2.

Define $\phi:S_1 \times S_2 \to R$ by $\phi(a_1,a_2) = a_1+ a_2$ $\forall (a_1,a_2) \varepsilon S_1 \times S_2$. Clearly ϕ is well-defined. First we shall show that ϕ is 1-1. Let $(a_1,a_2),(b_1,b_2) \varepsilon S_1\times S_2$ be such that $a_1+ a_2 = b_1+ b_2$ then $-b_1+ a_1 = b_2- a_2 \varepsilon S_1 \cap S_2 = \{0\}$ so $a_1= b_1$ and $a_2= b_2$ ie. $(a_1,a_2)=(b_1,b_2)$. Hence ϕ is 1-1. Next we shall show that ϕ is onto. Because $S_1 \trianglelefteq R$, $S_2 \trianglelefteq R$ and S_1,S_2 generate R, $R = S_1+ S_2$. Let $a \varepsilon R$ then $\exists a_1 \varepsilon S_1$, $a_2 \varepsilon S_2$ such that $a = a_1+ a_2$. So $(a_1,a_2) \varepsilon S_1 \times S_2$ and $\phi(a_1,a_2) = a_1+ a_2 = a$. Hence ϕ is onto. Lastly we shall show that ϕ is a homomorphism. Let $(s_1,s_2),(s_1',s_2') \varepsilon S_1 \times S_2$ then $\phi(s_1,s_2) + \phi(s_1',s_2') = (s_1+ s_2) + (s_1'+ s_2') = (s_1+ s_1') + (s_2+ s_2') = \phi((s_1+ s_1'),(s_2+ s_2')) = \phi((s_1,s_2) + (s_1',s_2'))$ (by the claim 2.) and $\phi(s_1,s_2).\phi(s_1',s_2') = (s_1+ s_2).(s_1'+ s_2') = s_1s_1'+ s_2s_1' + s_1s_2' + s_2s_2' = s_1s_1' + s_2s_2' = \phi(s_1s_1',s_2s_2') = \phi((s_1,s_2)\cdot(s_1',s_2'))$ (because $s_2s_1'+ s_1s_2' = 0$). Hence ϕ is a homomorphism. Thus $R \cong S_1 \times S_2$. #

Remark: We see that ideals (congruence sets) are factors in the direct product of skew rings.

Definition 3.3.18 Let R be a skew ring and S a subskew ring of R. Then R is said to be an extension of S by a skew ring T iff $S \trianglelefteq R$ and $R/S \cong T$.

Lemma 3.3.19 Let R be a skew ring and $A = \{x\,y \mid x,y \in R\}$. Then for each $\alpha,\beta \in A$ $\alpha + \beta = \beta + \alpha$.

Proof. Let $\alpha,\beta \in A$ so $\exists$ $a,b,c,d \in R$ such that $\alpha = a.b$, $\beta = c.d$ Then $(a + c).(d + b) = (a + c).b = a,d + c,d + a.b + c.b$ and $(a + c).(d + b) = a.(d + b)+ c.\ (d + b) = a.d + a.b + c.d + c.b$ so $a.d + a.b + c.d + c.b = a.d + c.d + a.b + c.b$ and therefore $a.b + c.d = c,d + a.b$ ie. $\alpha + \beta = \beta + \alpha$. #

Theorem 3.3.20 Let R be a skew ring. Then there exists an exact sequence of skew rings and skew ring homomorphisms

$$\begin{tikzcd} 0 \arrow[r] & S \arrow[r, "\phi"] & R \arrow[r, "\psi"] & T \arrow[r] & 0 \end{tikzcd}$$

such that T is a ring and S is a zero skew ring.

Proof. Let $S = \{x \in R \mid xy = yx = 0 \quad \forall\, y \in R\}$. Claim that S is a skew ring. To prove this, let $a,b \in S$ and $y \in R$. Then $ay = ya = 0 = by = yb$, hence $(ab)y = a(by) = a0 = 0 = 0b = (ya)b = y(ab)$ and $(a - b)y = ay - by = 0 = ya - yb = y(a - b)$. so $ab,\ a - b \in S$. Therefore S is a skew ring. So we have the claim. By definition of S,

S is a zero skewring. Next we shall show that $S \lhd R$. Let $x \in S$ and $r, y \in R$. Then $(r + x - r)y = 0 = y\ (r + x - r)$ and $(rx)y = 0 = y(rx)$ so $r + x - r$, $rx \in S$. Similarly $xr \in S$. Therefore $S \lhd R$. Put $T = R/S$. Then T is a skew ring. We must show that T is a ring ie. $+$ is commutative. Let $\alpha, \beta \in T$. Choose $a \in \alpha$ and $b \in \beta$. We shall show that $[a + b] = [b + a]$ ie. $(a + b) - (b + a) \in S$. Let $y \in R$ so $((a + b) - (b + a))\ y = ay + by - ay - by$. By above Lemma, $ay + by = by + ay$ so $ay + by - ay - by = 0$. Therefore $((a + b) - (b + a))y = 0$. Similarly $y((a + b)-(b + a)) = 0$. Hence $(a + b)-(b + a) \in S$. Therefore $[a + b] = [b + a]$. Hence $\alpha + \beta = \beta + \alpha$. Thus T is a ring. Define $\phi : S \to R$ by $\phi(s)=s$ and $\psi : R \to T$ by $\psi(r) = [r]$. Then ϕ is a 1-1 homomorphism and ψ is an onto homomorphism. Because $\ker \psi = \operatorname{Im} \phi$,

$$\begin{tikzcd} 0 \arrow[r] & S \arrow[r, "\phi"] & R \arrow[r, "\psi"] & T \arrow[r] & 0 \end{tikzcd}$$

is an exact sequence of skew rings and skew ring homomorphisms. #

This theorem shows that every skew ring is an extension of a zero skew ring by a ring.

Theorem 3.3.21 Let I be an ideal of a skew ring R. Then there exists a bijection between the set of subskew rings of R containing I and the set of subskew rings of R/I, and this bijection takes maximal subskew rings to maximal subskew rings, ideals to ideals and maximal ideals to maximal ideals.

Proof. It is similar to the proof of Theorem 2.3.19 and the bijection is the same form as the bijection in Theorem 2.3.19.

Definition 3.3.22 Let R be a skew ring. Then R is said to be simple iff the only ideals of R are R and $\{0\}$.

Example Let R be a zero skew ring such that $(R,+)$ is a simple group. Then R is a simple skew ring.

Corollary 3.3.23 Let I be a maximal ideal of a skew ring R. Then R/I is simple.

Lemma 3.3.24 Let R be a skew ring and $a \in R$. Let B be the set of all of finite sums of terms of the forms ras, ra, as, na, $b + ras - b$, $b + ra - b$, $b + as - b$, $b + na - b$ where $b,r,s \in R$ and $n \in \mathbb{Z}$. Then B is the ideal of R generated by a which denoted by $\langle a \rangle$.

Proof. It is standard.

Theorem 3.3.25 Let R be a simple skew ring. Then for each $a \in R\backslash\{0\}$, $c \in R$ c can be written as a finite sum of terms of the forms ras, ra as, na, $b + ras - b$, $b + ra - b$, $b + as - b$, $b + na - b$ where $b,r,s \in R$ and $n \in \mathbb{Z}$.

Proof. Let $a \in R\backslash\{0\}$. Since R is simple, $\langle a \rangle = R$ or $\{0\}$. Because $a \neq 0$ and $a \in \langle a \rangle$, $\langle a \rangle \neq \{0\}$. so $c \in R = \langle a \rangle$. Therefore c can be written as a finite sum of terms of form ras, ra, as, na, $b + ras - b$, $b + ra - b$, $b + as - b$, $b + na - b$ where $b,r,s \in R$ and $n \in \mathbb{Z}$. #

Corollary 3.3.26 If R is a simple ring then for each $a,b \in R\setminus\{0\}$ there exist $m \in \mathbb{N}, r_i, r_i', s_i, s_i' \in R$ for all $i \in \{1,2,\dots,m\}$ and $n \in \mathbb{Z}$ such that $b = \sum_{i=1}^{m} r_i a s_i + r_i' a + a s_i' + na$.

Proof. Let R be a simple ring. Let $a,b \in R\setminus\{0\}$. Then $\{\sum_{i}^{\text{finite}} r_i a s_i + r_i' a + a s_i' + na \mid r_i, r_i', s_i, s_i' \in R,\ n \in \mathbb{Z}\}$ is the ideal of R generated by $a = \langle a\rangle$. Because R is simple, $\langle a\rangle = R$ or $\{0\}$. Since $a \neq 0$ and $a \in \langle a\rangle, \langle a\rangle \neq \{0\}$ so $b \in R = \langle a\rangle$. Therefore $\exists m \in \mathbb{N}$, $r_i, r_i', s_i, s_i' \in R$ $\forall i \in \{1,2,\dots,m\}$ and $\exists n \in \mathbb{Z}$ such that $b = \sum_{i=1}^{m} r_i a s_i + r_i' a + a s_i' + na$. #

Corollary 3.3.27 If R is a simple ring with multiplicative identity 1 then for each $a \in R\setminus\{0\}$ there exist $n \in \mathbb{N}, r_i, s_i \in R$ for all $i \in \{1,2,\dots,n\}$ such that $1 = \sum_{i=1}^{n} r_i a s_i$.

Proof. Let R be a simple ring with 1. Let $a \in R\setminus\{0\}$. Then $\{\sum_{i}^{\text{finite}} r_i a s_i \mid r_i, s_i \in R\}$ is the ideal in R generated by $a = \langle a\rangle$. Because R is simple, $\langle a\rangle = \{0\}$ or R. Since $a \neq 0$ and $a \in \langle a\rangle$, $\langle a\rangle \neq \{0\}$ so $1 \in R = \langle a\rangle$. Therefore $\exists\, n \in \mathbb{N}$, $r_i, s_i \in R$ for all $i \in \{1,2,\dots,n\}$ such that $1 = \sum_{i=1}^{n} r_i a s_i$. #

3.4 Modules.

In this section we shall work with left congruences on a skew ring. But everything that we prove for left congruences can be similarly proved for right congruences. As in Section 3.3, we shall consider the categories $\mathcal{R}$, $\mathcal{R}_o$ and $\mathcal{R}_i$.

We shall define naturally equivalent contravariant functors from $\mathcal{R}$ to $\mathcal{L}$, naturally equivalent covariant functors from $\mathcal{R}_o$ to $\mathcal{L}$ and naturally equivalent covariant functors from $\mathcal{R}_i$ to $\mathcal{Q}$ by using

1) double left congruences, double left semigroup-spaces and double left ideals,

2) multiplicative left congruences, multiplicative left modules and multiplicative left ideals,

3) additive left congruences, additive left modules and additive left ideals.

Definition 3.4.1 A double left congruence on askew ring R is an equivalence relation ρ on R such that $x \rho y$ implies that $(a + x)\rho(a + y)$ $(a.x)\rho(a.y)$ for all $a,x,y \in R$.

Definition 3.4.2 A multiplicative left congruence on a skew ring R is an equivalence relation ρ on R such that $x \rho y$ implies that $(a + x)\rho(a + y)$, $(x + a)\rho(y + a)$ and $(a.x)\rho(a.y)$ for all $a,x,y \in R$.

Definition 3.4.3 An additive left congruence on a skew ring R is an equivalence relation ρ on R such that $x \rho y$ implies that $(a + x)\rho(a + y)$, $(x.a)\rho(y.a)$ and $(a.x)\rho(a.y)$ for all $a,x,y \varepsilon R$.

Definition 3.4.4 Let R be a skew ring. A double left R-space is a triple $(M,+,\cdot)$ where $(M,+)$ and $(M,\cdot)$ are left R-spaces such that $r.(s + m) = r.s + r.m$ for all $m \varepsilon M, r,s \varepsilon R$.

Definition 3.4.5 Let R be a skew ring. A multiplicative left R-module is a triple $(M,+,\cdot)$ where $(M,+)$ is a group and, $(M,\cdot)$ is a left R-apace such that $r.(n + m) = r.n + r.m$ and $(r + s).m = r.m + s.m$ for all $r,s \varepsilon R$, $m,n \varepsilon M$.

Definition 3.4.6 Let R be a skew ring. An additive left R-module is a triple $(M,+,\cdot)$ where $(M,+)$ is a left R-space and $(M,\cdot)$ is a semigroup.

Remark: For each skew ring R,R is a double left R-space and multiplicative (additive) left R-module.

Definition 3.4.7 A double left ideal I of a skew ring R is an additive subgroup of R such that for each $x \varepsilon I$, $y \varepsilon R$ $y.x \varepsilon I$.

Definition 3.4.8 A multiplicative left ideal I of a skew ring R is an additive subroup of R such that for each $x \varepsilon I$, $y \varepsilon R$ $y + x - y \varepsilon I$ and $y.x \varepsilon I$

Definition 3.4.9 An additive left ideal I of a skew ring R is an additive subgroup of R such that for each $x \varepsilon I$, $y \varepsilon R$ $y.x, x.y \varepsilon I$.

. We shall only work with double left congruences and everything that we prove for double left congruences can be similarly proved for multiplicative left congruences and additive left congruences.

Definition 3.4.10 Let R be a skew ring, M, M' double left R-spaces and $\phi : M \to M'$ a map. Say that ϕ is double left R-equivariant iff $\phi(s + m) = s + \phi(m)$ and $\phi(s.m) = s.\phi(m)$ for all $s \in S$, $m \in M$.

Remarks: 1) If ϕ is a bijectively double left R-equivariant map then ϕ^{-1} is double left R-equivariant. We shall call such a map a double left R-space isomorphism.

2) If ρ is a double left congruence on a skew ring R then the set R/ρ of equivalence classes of R can be made into a double left R-space in natural way and the natural projection map $\phi : R \to R/\rho$ is an onto double left R-equivariant map.

3) If ρ is a double left congruence on a skew ring R then $[0]_\rho = \{a \in R \mid a \; \rho \; 0\}$ is a double left ideal of R.

4) If I is a double left ideal on a skew ring R then $\{(a,b) \in R \times R \mid -a + b \in I\}$ is a double left congruence on R.

Proposition 3.4.11 Let $\phi : R \to R'$ be a skew ring homomorphism. If ρ' is a double left congruence on R' then $(\phi \times \phi)^{-1}(\rho')$ is a double left congruence on R. If I' a double left ideal of R' then $\phi^{-1}(I')$ is a double left ideal of R.

Proposition 3.4.12 Let $\phi : R \to R'$ be an onto skew ring homomorphism. If ρ is a double left congruence on R then $(\phi \times \phi)(\rho)$ is a double left congruence on R'. If I is a double left ideal of R then $\phi(I)$ is a double left ideal of R'.

Definition 3.4.13 Let R be a skew ring. A quotient double left R-space is a pair (K,ϕ) where K is a double left R-space and $\phi : R \to K$ is an onto double left R-equivariant map.

Example $(R/\rho, \pi)$ is a quotient double left R-space where ρ is a double left congruence on a skew ring R.

Theorem 3.4.14 Let R be a skew ring and M a double left R-space. Let $\phi : R \to M$ be an onto double left R-equivariant and $\rho = \{a,b) \in R \times R | \phi(a) = \phi(b)\}$. Then ρ is a double left congruence on R and there exists a double left R-space isomomorphism ψ from R/ρ onto M such that the following diagram commutes.

$$\begin{tikzcd}
& R \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\
R/\rho \arrow[rr, "\psi"'] & & M
\end{tikzcd}$$

Proof. It is similar to the proof of Theorem 2.1.2.

Definition 3.4.15 Let R be a skew ring. Let (K,ϕ) and (K',ϕ') be quotient double left R-spaces. Say that (K,ϕ) is strongly equivalent to (K',ϕ') iff there exists a double left R-space isomorpshism $\psi : K \to K'$

such that the following diagram commutes.

$$\begin{tikzcd}
 & R \arrow[dl, "\phi"'] \arrow[dr, "\phi'"] & \\
K \arrow[rr, "\psi"'] & & K'
\end{tikzcd}$$

Write this as $(K,\phi) \approx (K',\phi')$.

Remarks: 1) $\approx$ is an equivalence relation on the set of quotient double left R-spaces.

2) For each quotient double left R-space (K,ϕ), $(K,\phi) \approx (R/\rho,\pi)$ where $\rho = \{(a,b) \in R \times R \mid \phi(a) = \phi(b)\}$

Fix a skew ring R, let LI(R) = the set of double left ideals of R,

LC(R) = the set of double left congruences on R,

LQ(R) = the set of equivalence classes of quotient double left R-spaces under $\approx$.

We define natural relations $\subsetneq$ on LI(R), LC(R) and LQ(R) as $\subsetneq$ on I(R), C(R) and Q(R) in Section 3.3 respectively. Then the proof that $(LI(R),\subsetneq)$,$(LC(R),\subsetneq)$ and $(LQ(R),\subsetneq)$ are posets is similar to the proof that $((I(R),\subsetneq)$,$(C(R),\subsetneq)$ and $(Q(R),\subsetneq)$ are posets respectively.

Theorem 3.4.16 For each skew ring R, the posets LI(R), LC(R) and LQ(R) are isomorphic.

Proof. It is similar to the proof of Theorem 3.3.10 and the isomorphisms have the same form as in Theorem 3.3.10.

Remark: Fix a skew ring R, let $I_1, I_2 \in LI(R)$. Then $I_1 \cap I_2 = \text{g.l.b.}\{I_1, I_2\}$ and the double left ideals of R generated by $I_1 \cup I_2 = \text{l.u.b.}\ \{I_1, I_2\}$. Hence LI(R) is a lattice. Therefore LC(R) and LQ(R) are lattices also.

We define contravariant functors LI,LC and LQ from $\mathcal{R}$ to $\mathcal{L}$ as we defined the contravariant functor I,C and Q from $\mathcal{R}$ to $\mathcal{L}$ in Section 3.3, respectively. Then the proof that LI,LC and LQ are naturally equivalent contravariant functors is similar to the proof that I,C and Q are naturally equivalent contravariant functors.

We define covariant functors LI', LC' and LQ' from $\mathcal{R}_o$ to $\mathcal{L}$ as we defined the covariant functor I',C' and Q' from $\mathcal{R}_o$ to $\mathcal{L}$ in Section 3.3, respectively. Then the proof that LI',LC' and LQ' are naturally equivalent covariant functors is similar to the proof that I',C' and Q' are naturally equivalent covariant functors.

Definition 3.4.17 Let I_1 and I_2 be double left ideals of skew ring R. Say that I_1 is equivalent to I_2 ($I_1 \sim I_2$) iff there exists an skew ring automorphism $\phi : R \to R$ such that $\phi(I_1) = I_2$.

Remark: $\sim$ is an equivalence relation on the set of double left ideals of a skewring.

Definition 3.4.18 Let ρ_1 and ρ_2 be double left congruences on a skew ring R. Say that ρ_1 is equivalent to $\rho_2(\rho_1 \sim \rho_2)$ iff there exists an skew ring automorphism $\phi : R \to R$ such that $(\phi \times \phi)(\rho_1) = \rho_2$.

Remark: $\sim$ is an equivalence relation on the set of double left congruences on a skew ring.

Definition 3.4.19 Let (K, ϕ) and (K', ϕ') be quotient double left R-spaces where R is a skew ring. Say that (K, ϕ) is weakly equivalent to (K', ϕ') iff there exist a skew ring automorphism $f : R \to R$ and a souble left R-space isomorphism $f' : K \to K'$ such that the following diagram commutes.

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d, "\phi"'] & R \arrow[d, "\phi'"] \\
K \arrow[r, "f'"] & K'
\end{tikzcd}$$

Write this an $(K, \phi) \sim (K', \phi')$.

Remarks: 1) $\sim$ is an equivalence relation on the set of quotient double left R-spaces.

2) $(K, \phi) \simeq (K', \phi')$ implies that $(K, \phi) \sim (K', \phi')$.

Fix a skew ring R, let $LI^*(R)$ = the set of equivalence classes of double left C - sets on R,

$LC^*(R)$ = the set of equivalence classes of double left congruences on R,

$LQ^*(R)$ = the set of equivalence classes of quotient double left R-spaces under $\sim$.

We define binary relation $\leqslant$ on $LI^*(R)$, $LC^*(R)$ and $LQ^*(R)$ as $\leqslant$ on $I^*(R)$, $C^*(R)$ and $Q^*(R)$ in Section 2.3 respectively. The proof that $(LI^*(R),\leqslant)$,$(LC^*(R),\leqslant)$ and $(LQ^*(R),\leqslant)$ are quasi-ordered sets is similar to the proof that $(I^*(R),\leqslant)$,$(C^*(R),\leqslant)$ and $(Q^*(R),\leqslant)$ are quasi-ordered sets, respectively.

Theorem 3.4.20 For each skew ring R. the quasi-ordered sets $LI^*(R)$, $LC^*(R)$ and $LQ^*(R)$ are isomorphic.

Proof. It is similar to the proof of Theorem 3.3.16 and the isomorphisms have the same form as in Theorem 3.3.16.

We define covariant functors LI^*, LC^* and LQ^* from $\mathcal{R}_i$ to $\mathcal{Q}$ as we defined the covariant functors I^*,C^* and Q^* from $\mathcal{R}_i$ to $\mathcal{Q}$ in Section 3.3, respectively. Then the proofs that LI^*, LC^* and LQ^* are naturally equivalent covariant functors is similar to the proofs that I^*, C^* and Q^* are naturally equivalent covariant functors.

3.5 Positive Rational Domains (P.R.D.'s)

Definition 3.5.1 A positive rational domain (P.R.D) is a triple $(D,+,\cdot)$ where D is a set, + (addition) and $\cdot$ (multiplication) are binary operations on D such that

i) $(D,\cdot)$ is a group,

ii) $(D,+)$ is a semigroup,

iii) $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all $x,y,z \in D$.

We shall let 1 denote the identity of $(D,\cdot)$.

Remark: A P.R.D. is an algebraic system.

Examples 1) Let $(G,\cdot)$ be a group. Define a binary operation + on G by $x + y = x$ for all $x,y \in G$ (or $x + y = y$ for all $x,y \in G$). Then $(G,+,\cdot)$ is a P.R.D.

2) $\mathbb{Q}^+, \mathbb{R}^+$ are P.R.D.'s.

Definition 3.5.2 Let D,D' be P.R.D.'s and $\phi:D \to D'$ a map. Say that ϕ is a P.R.D. homomorphism iff $\phi(a + b) = \phi(a) + \phi(b)$ and $\phi(a.b) = \phi(a).\ \phi(b).$ for all $a,b \in D$.

Remark: A P.R.D. homomorphism is an operation preserving map.

This section will consider the following subcategories of $\mathcal{S}_r$:

1) The category $\mathcal{D}$ of P.R.D.'s and P.R.D. homomorphisms.

2) The category $\mathcal{D}_o$ of P.R.D.'s and onto P.R.D. homomorphisms.

3) The category $\mathcal{D}_i$ of P.R.D.'s and P.R.D. isomorphisms.

First we shall show that $\mathcal{D}$ has a congruence set so we shall define naturally eauivalent contravariant functors from $\mathcal{D}$ to $\mathcal{L}$ by using congruences, C-sets and quotient P.R.D.'s which are defined below.

<u>Remark:</u> If ρ is an operation preserving equivalence relation on a P.R.D. D then the set D/ρ of equivalence relation ρ on D can be made into a P.R.D. in natural way and the natural projection map $\phi : D \to D/\rho$ is an onto P.R.D. homomorphism. Hence the definition of a congruence on an object $(D,+,\cdot)$ in $\mathcal{D}$ ($\mathcal{D}_o$ or $\mathcal{D}_i$) is the same as the definition of an operation preserving equivalence relation on the P.R.D. D.

<u>Definition 3.5.3</u> A <u>C - set</u> B of a P.R.D. D ($B \triangleleft D$) is a multiplicative subgroup of D such that

i) for each $b \in B$, $d \in D$ $d^{-1}bd \in B$,

ii) for each $b \in B$, $d \in D$ $(d + 1)^{-1}(d + b)$, $(1 + d)^{-1}(b + d) \in B$.

We shall now prove the following two properties of C - sets of a P.R.D. D.

1) If $B \triangleleft D$ then for each $d \in D$, $b \in B$ $(d + b)(d + 1)^{-1}$, $\in B$ $(b + d)(1 + d)^{-1} \in B$

2) Let D be a P.R.D. and B a multiplicative subgroup of D. Then $B \triangleleft D$ iff

a) for each $d \varepsilon D$, $b \varepsilon B$ $d^{-1}bd \varepsilon B$,

b) for each $x,y \varepsilon D$ $[$if $x^{-1}y \varepsilon B$ then $(x + z)^{-1}(y + z)$, $(z + x)^{-1}(z + y) \varepsilon B$ for all $z \varepsilon D]$.

Proof. 1) Let $B \trianglelefteq D$ and $d \varepsilon D$, $b \varepsilon B$. Then $(d + b)(d + 1)^{-1} = (d + 1)(d + 1)^{-1}(d + b)(d + 1)^{-1} \varepsilon B$ (by i and ii). Similarly we can show that $(b + d)(a + d)^{-1} \varepsilon B$.

2) Assume that $B \trianglelefteq D$ then $dbd^{-1} \varepsilon B$ and $(d + 1)^{-1}(d + b)$, $(1 + d)^{-1}(b + d) \varepsilon B$ $\forall d \varepsilon D$, $b \varepsilon B$. We must show that $\forall x,y \varepsilon D$ $[$if $x^{-1}y \varepsilon B$ then $(a + z)^{-1}(y + z)$, $(z + x)^{-1}(z + y) \varepsilon B$ $\forall z \varepsilon D]$. Let $x,y \varepsilon D$ be such that $x^{-1}y \varepsilon B$. Let $z \varepsilon D$. Then $y^{-1}x \varepsilon B$, $y^{-1}z \varepsilon D$ and hence $(x + z)^{-1}(y + z) = (x + z)^{-1}yy^{-1}(y + z) = (y^{-1}x + y^{-1}z))^{-1}(y^{-1}(y + z)) = (y^{-1}x + y^{-1}z)^{-1}(1 + y^{-1}z) \varepsilon B$. Similarly, we can show that $(z + x)^{-1}(z + y) \varepsilon B$. Therefore a) and b) are true. Assume that a) and b) are true. Then $dbd^{-1} \varepsilon B$ $\forall d \varepsilon D, b \varepsilon B$ and $\forall x,y \varepsilon D$ $[$if $x^{-1}y \varepsilon B$ then $(x + z)(y + z)^{-1}$, $(z + x)(z + y)^{-1} \varepsilon B$ $\forall z \varepsilon D]$. We must show that $(d + 1)^{-1}(d + b)$, $(1 + d)^{-1}(b + d) \varepsilon B$. $\forall d \varepsilon D, b \varepsilon B$. Let $d \varepsilon D$, $b \varepsilon B$. Then $d^{-1}(db) = b \varepsilon B$ and hence $(1 + d)^{-1}(b + d) = ((1 + d)^{-1}(d^{-1}d)(b + d)) = (d(1 + d))^{-1}(d(b + d)) = (d + dd)^{-1}(db + dd) \varepsilon B$. Similarly we can show that $(d + 1)^{-1}(d + b) \varepsilon B$. Therefore $B \trianglelefteq D$. #

Examples 1) Let ρ be a congruence on a P.R.D. D. Then $[1]_\rho = \{a \varepsilon D | a \rho 1\} \trianglelefteq D$.

2) Let B be a C - set of a P.R.D. D. Then $\{(a,b) \varepsilon D \times D | a^{-1}b \varepsilon B\}$ is a congruence on D.

Definition 3.5.4 A quotient P.R.D. of a P.R.D. D is a pair (K,ϕ) where K is a P.R.D. and $\phi:D \to K$ is an onto P.R.D homomorphism.

Examples 1) $(D/\rho,\pi)$ is a quotient P.R.D. of a P.R.D. D where ρ is a congruence on D.

2) Let B be a C - set of a P.R.D. D. Let $\rho = \{(a,b) \in D \times D | a^{-1}b \in B\}$ and $D/B = D/\rho$. Then $(D/B,\pi)$ is a quotient P.R.D. of D.

Theorem 3.5.5 Let (K,ϕ) be a quotient P.R.D. of a P.R.D.D and $\rho = \{(a,b) \in D \times D | \phi(a) = \phi(b)\}$. Then ρ is a congruence on D and there exists an isomorphism $\psi:D/\rho \to K$ such that the following diagram is commutative

$$\begin{tikzcd} & D \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\ D/\rho \arrow[rr, "\psi"'] & & K \end{tikzcd}$$

Proof. It is similar to the proof of Theorem 2.3.2.

Definition 3.5.6 Let D,D' be P.R.D.'s and $\phi:D \to D'$ a P.R.D. homomorphism. Then kernel of ϕ, denoted by $\ker \phi$, $= \{d \in D | \phi(d) = 1\}$.

Theorem 3.5.7 Let $\phi:D \to D'$ be an onto P.R.D. homomorphism. Then $\ker \phi \trianglelefteq D$ and there exists a natural isomorphism $\psi:D/\ker \phi \to D'$ such that the following diagram is commutative

$$\begin{tikzcd}
 & D \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\
D/\ker\phi \arrow[rr, "\psi"'] & & D.
\end{tikzcd}$$

Proof. It is similar to the proof of Theorem 2.3.3.

We shall call the above Theorem the first isomorphism Theorem of P.R.D Theory.

Definition 3.5.8 Let (K,ϕ) and (K',ϕ') be quotient P.R.D.'s of a P.R.D. D. Say that (K,ϕ) is strongly equivalent to (K',ϕ') iff there exists an isomorphism $\psi:K \to K'$ such that the following diagram is commutative

$$\begin{tikzcd}
 & D \arrow[dl, "\phi"'] \arrow[dr, "\phi'"] & \\
K \arrow[rr, "\psi"'] & & K'
\end{tikzcd}$$

Write this as $(K,\phi) \simeq (K',\phi')$.

Remarks: 1) $\simeq$ is an equivalence relation on the set of quotient P.R.D.'s of a P.R.D.

2) For each quotient P.R.D. (K,ϕ) of a P.R.D. D, $(K,\phi) \simeq (D/\rho,\pi)$ where $\rho = \{(a,b) \in D \times D | \phi(a) = \phi(b)\}$.

3) For each quotient P.R.D. (K,ϕ) of a P.R.D. D, $(K,\phi) \simeq (D/\ker\phi,\pi)$.

Proposition 3.5.9 Let $\phi : D \to D'$ be a P.R.D. homomorphism. If ρ' is a congruence on D' then $(\phi \times \phi)^{-1}(\rho')$ is a congruence on D. If B' is a C - set of D' then $\phi^{-1}(B')$ is a C - set of D.

Proof. It is standard.

Proposition 3.5.10 Let $\phi : D \to D'$ be an onto P.R.D. homomorphism. If ρ is a congruence on D then $(\phi \times \phi)(\rho)$ is a congruence on D'. If B is a C - set of D then $\phi(B)$ is a C - set of D'.

Proof. It is similar to the proof of Proposition 2.3.6.

Fix a P.R.D. D,let C(D) = the set of congruences on D,

B(D) = the set of C - sets of D,

Q(D) = the set of equivalence classes of quotient P.R.D.'s of D under $\approx$.

We define natural relations $\subsetneq$ on C(D),B(D),Q(D) as $\subsetneq$ on C(G), N(G), Q(G) in Section 2.3, respectively. Then the proof that $(C(D),\subsetneq)$, $(B(D),\subsetneq)$, $(Q(D),\subsetneq)$ are posets is similar to the proof that $(C(G),\subsetneq)$, $(N(G),\subsetneq)$, $(Q(G),\subsetneq)$ are posets respectively.

Theorem 3.5.11 For each P.R.D.D the posets C(D), B(D), Q(D) are isomorphic.

Proof. If is similar to the proof of Theorem 2.3.7. Theorem 2.3.8 and the isomorphisms have the same form as in Theorem 2.3.7, Theorem 2.3.8.

Proposition 3.5.12 Let B_1, B_2 be C - sets of a P.R.D.D. Then $B_1 . B_2 = \{b_1 . b_2 | b_1 \varepsilon B_1, b_2 \varepsilon B_2\}$ is the C - set of D generated by $B_1 \cup B_2$.

Proof. First we shall show that $B_1 . B_2 \trianglelefteq D$. Let $x, y \varepsilon B_1 . B_2$ then $x = b_1 b_2$, $y = c_1 c_2$ for some $b_1, c_1 \varepsilon B_1, b_2, c_2 \varepsilon B_2$. So $xy^{-1} = b_1 b_2 (c_1 c_2)^{-1} = b_1 b_2 c_2^{-1} c_1^{-1} = b_1 c_1 (c_1^{-1} (b_2 c_2^{-1}) c_1) \varepsilon B_1 . B_2$. Let $x \varepsilon B_1 . B_2$ and $d \varepsilon D$ then $x = b_1 b_2$ for some $b_1 \varepsilon B_1, b_2 \varepsilon B_2$. So $d^{-1} x d = d^{-1} (b_1 b_2) d = (d^{-1} b_1 d)(d^{-1} b_2 d) \varepsilon B_1 B_2$ and $(1 + d)^{-1} (x + d) = (1 + d)^{-1} (b_1 b_2 + d) = (b_1 (b_1^{-1} + b_1^{-1} d))^{-1} (b_1 (b_2 + b_1^{-1} d)) = (b_1^{-1} + b_1^{-1} d)^{-1} (b_2 + b_1^{-1} d) = (b_1^{-1} + b_1^{-1} d)^{-1} (1 + b_1^{-1} d)(1 + b^{-1} d)^{-1} (b_2 + b_1^{-1} d) = ((1 + b_1^{-1} d)^{-1} (b_1^{-1} + b_1^{-1} d))^{-1}$. $((1 + b_1^{-1} d)^{-1} (b_2 + b_1^{-1} d)) \varepsilon B_1 . B_2$ Similarly we can show that $(d + 1)^{-1} (d + x) \varepsilon B_1 . B_2$. Hence $B_1 . B_2 \trianglelefteq D$. Clearly $B_1 \subseteq B_1 . B_2, B_2 \subseteq B_1 . B_2$. Next let $B \trianglelefteq D$ be such that $B_1 \subseteq B, B_2 \subseteq B$. We want to show that $B_1 . B_2 \subseteq B$. Let $b_1 \varepsilon B_1$, $b_2 \varepsilon B_2$ then $b_1 \varepsilon B$, $b_2 \varepsilon B$. Since B is a multiplicative subgroup of D, $b_1 b_2 \varepsilon B$. Hence $B_1 . B_2 \subseteq B$. Therefore $B_1 B_2$ is the C - sets of D generated by $B_1 \cup B_2$.

Proposition 3.5.13 Let ρ_1, ρ_2 be congruences on a P.R.D.D. Then $\rho_1 . \rho_2 = \{(a_1 . a_2, b_1 . b_2) | (a_1, b_1) \varepsilon \rho_1, (a_2, b_2) \varepsilon \rho_2\}$ is the congruence on D generated by $\rho_1 \cup \rho_2$.

Proof. We can show that $\rho_1 . \rho_2$ is an equivalence relation on D as we showed that $\rho_1 . \rho_2$ is an equivalence relation on G in the proof of

Proposition 2.3.11. Let $(a,b) \in \rho_1.\rho_2$ and $c \in D$. Then $a = a_1a_2$, $b = b_1b_2$ where $(a_1,b_1) \in \rho_1$ $(a_2,b_2) \in \rho_2$. So $(c.a,c.b) = (ca_1,cb_1)(a_2,b_2) \in \rho_1.\rho_2$ and $(ac,bc) = (a_1.b_1)(a_2c,b_2c) \in \rho_1.\rho_2$. Since $(a_2,b_2) \in \rho_2$, $(a_1a_2 + c, a_1b_2 + c) \in \rho_2 \subseteq \rho_1.\rho_2$. Since $(a_1,b_1) \in \rho_1$, $(a_1b_2 + c, b_1b_2 + c) \in \rho_1 \subseteq \rho_1.\rho_2$. Because $\rho_1.\rho_2$ is transitive, $(a + c, b + c) = (a_1a_2 + c, b_1b_2 + c) \in \rho_1\rho_2$. Similarly we can prove that $(c + a, c + b) \in \rho_1.\rho_2$. Hence $\rho_1.\rho_2$ is a congruence on D. It is easy to show that $\rho_1.\rho_2$ is the congruence on D generated by $\rho_1 \cup \rho_2$. #

We shall show that $(C(D),\subseteq)$, $(B(D),\subseteq)$ and $(Q(D),\subseteq)$ are lattices for all P.R.D.D. Let D be a P.R.D. Let $B_1,B_2 \in B(D)$. Then $B_1 \cap B_2 =$ g.l.b. $\{B_1,B_2\}$ and $B_1.B_2 =$ l.u.b. $\{B_1,B_2\}$. Hence $(B(D),\subseteq)$ is a lattice. Let $\rho_1,\rho_2 \in C(D)$. Then $\rho_1 \cap \rho_2 =$ g.l.b. $\{\rho_1.\rho_2\}$ and $\rho_1.\rho_2 =$ l.u.b. $\{\rho_1,\rho_2\}$. Hence $(C(D),\subseteq)$ is a lattice. Therefore $(Q(D),\subseteq)$ is a lattice. also.

We define contravariant functors C,B,Q from $\mathscr{D}$ to $\mathscr{L}$ as the contravariant functors C,N,Q from $\mathscr{S}$ to $\mathscr{L}$ in Section 2.3, respectively. Then the proof that C,B,Q are naturally equivalent is similar to the proof that C,N,Q are naturally equivalent in Section 2.3.

Remark: As a result we see that C is the congruence functor of $\mathscr{D}$, $\mathscr{D}$ has a congruence set and C - sets of a P.R.D. are congruence sets with respect to B.

Next we shall define covariant functors C', B', Q' from $\mathcal{D}_o$ to $\mathcal{L}$ as the covariant functors C', N', Q' from $\mathcal{D}_o$ to $\mathcal{L}$ in Section 2.3, respectively. Then the proof that C', B', Q' are naturally equivalent covariant functors is similar to the proof that C', N', Q' are naturally equivalent covariant functors. in Section 2.3

Now we shall define naturally equivalent covariant functors from $\mathcal{D}_i$ to $\mathcal{Q}$ using equivalence classes of congruences, equivalence classes of C-sets of a P.R.D. and equivalence classes of quotient P.R.D's which are defined below.

<u>Definition 3.5.14</u> Let ρ_1 and ρ_2 be congruences on a P.R.D.D. Say that ρ_1 is <u>equivalent</u> to $\rho_2 (\rho_1 \sim \rho_2)$ iff there exists an automorphism $f:D \to D$ such that $(f \times f)(\rho_1) = \rho_2$.

<u>Remark</u>: $\sim$ is an equivalence relation on the set of congruences on a P.R.D.

<u>Definition 3.5.15</u> Let B_1, B_2 be C - sets of a P.R.D. D. Say that B_1 is <u>equivalent</u> to $B_2 (B_1 \sim B_2)$ iff there exists an automorphism $f:D \to D$ such that $f(B_1) = B_2$.

<u>Remark</u>: $\sim$ is an equivalence relation on the set of C - sets of a P.R.D.

<u>Definition 3.5.16</u> Let $(K,\phi),(K',\phi')$ be quotient P.R.D.'s of a P.R.D. D. Say that (K,ϕ) is <u>weakly equivalent</u> to (K',ϕ') iff there exist isomorphisms $f:D \to D$ and $f':K \to K'$ such that the following diagram is commutative

$$\begin{tikzcd}
D \arrow[r, "f"] \arrow[d, "\phi"'] & D \arrow[d, "\phi'"] \\
K \arrow[r, "f'"] & K'
\end{tikzcd}$$

หอสมุดกลาง สถาบันวิทยบริการ จุฬาลงกรณ์มหาวิทยาลัย

Write this as $(K,\phi) \sim (K',\phi')$.

Remarks: 1) $\sim$ is an equivalence relation on the set of quotient P.R.D.'s of a P.R.D.

2) $(K,\phi) \simeq (K',\phi')$ implies that $(K,\phi) \sim (K',\phi')$.

Fix a P.R.D.D, let $C^*(D)$ = the set of equivalence classes of congruences on D under $\sim$,

$B^*(D)$ = the set of equivalence classes of C - sets of D under $\sim$,

$Q^*(D)$ = the set of equivalence classes of quotient P.R.D.'s of D under $\sim$.

We define binary relations $\leqslant$ on $C^*(D)$, $B^*(D)$, $Q^*(D)$ as $\leqslant$ on $C^*(G)$, $N^*(G)$, $Q^*(G)$ in Section 2.3, respectively. Then the proof that $(C^*(D),\leqslant)$, $(B^*(D),\leqslant)$, $(Q^*(D),\leqslant)$ are quasi-ordered sets in similar to the proof that $(C^*(G),\leqslant)$ $(N^*(G),\leqslant)$, $(Q^*(G),\leqslant)$ are quasi-ordered set. respectively.

Theorem 3.5.17 For each P.R.D.D the quasi-ordered sets $C^*(D)$, $B^*(D)$, $Q^*(D)$ are isomorphic.

Proof. It is similar to the proofs of Theorem 2.3.15, Theorem 2.3.16 and the isomorphisms have the same form as in Theorem 2.3.15, Theorem 2.3.16.

We define covariant functors C^*, B^*, Q^* from $\mathcal{D}_i$ to $\mathcal{Q}$ as the covariant functors C^*, N^*, Q^* from $\mathcal{S}_i$ to $\mathcal{Q}$ in Section 2.3 respectively. Then the proof that C^*, B^*, Q^* are naturally equivalent covariant functors is similar to the proof that C^*, N^*, Q^* are naturally equivalent covariant functors in Section 2.3.

Remark : We can prove that the following subcategories of $\mathcal{D}$ have a congruence set as we proved that $\mathcal{D}$ has a congruence set:

1) The category of additively commutative P.R.D.'s and P.R.D homomorphisms,

2) The category of multiplicatively commutative P.R.D.'s and P.R.D. homomorphisms,

3) The category of commutative P.R.D.'s and P.R.D. homomorphisms.

Next we shall consider some theorems which use C - sets (congruence sets) of P.R.D.'s.

Proposition 3.5.18 Let C be a C - set of the P.R.D. $\mathbb{Q}^+$. Then $C = \{1\}$ or $\mathbb{Q}^+$.

Proof. Assume that $C \neq \{1\}$. Let $x \in C \setminus \{1\}$. Claim that C must contain an element z in $\mathbb{Q}^+$ such that $z > 1$. To prove this, we have that $x > 1$ or $x < 1$. If $x > 1$ then done. We may assume that

$x < 1$ then $\frac{1}{x} > 1$. Because C is a multiplicative group, $\frac{1}{x} \varepsilon C$. Hence we have the claim. We must show that $C = \mathbb{Q}^+$. Let $y \varepsilon \mathbb{Q}^+$. If $y = 1$ then done. We may assume that $y > 1$ or $y < 1$.

<u>case 1</u> $y > 1$. Let $z \varepsilon C$ be such that $z > 1$. So $z^n \to \infty$ as $n \to \infty$. Therefore $\exists\, n_o \varepsilon \mathbb{N}$ such that $z^{n_o} > y$. Since $z \varepsilon C$, $z^{n_o} \varepsilon C$. Because $y > 1$ and $z^{n_o} > y$, $\frac{z^{n_o} - y}{y - 1} \varepsilon \mathbb{Q}^+$. Let $d = \frac{z^{n_o} - y}{y - 1}$ so $d \varepsilon \mathbb{Q}^+$ and $y = \frac{z^{n_o} + d}{1 + d}$. Because C is a C - set of $\mathbb{Q}^+$ and $z^{n_o} \varepsilon C$, $y \varepsilon C$.

<u>case 2</u> $y < 1$ then $\frac{1}{y} > 1$. So by case 1, $\frac{1}{y} \varepsilon C$. Hence $y \varepsilon C$. Therefore $C = \mathbb{Q}^+$. #

<u>Remark</u>: We can prove that if C is a C - set of the P.R.D. $\mathbb{R}^+$ then $C = \{1\}$ or $\mathbb{R}^+$ as we proved the previous Proposition.

<u>Definition 3.5.19</u> Let D be a P.R.D. Then D is said to be <u>simple</u> iff the only C - sets of D are {1} and D.

<u>Examples</u> $\mathbb{Q}^+$, $\mathbb{R}^+$ are simple P.R.D.'s.Let G be a simple group. Define on operation on G by $x + y = x$ for all $x,y \varepsilon G$ (or $x + y = y$ for all $x,y \varepsilon G$). Then $(G,+,\cdot)$ is a simple P.R.D.

<u>Definition 3.5.20</u> A <u>sub-P.R.D.</u> of a P.R.D.D is a subset of D such that it is a P.R.D.

<u>Definition 3.5.21</u> Let B be a C - set of a P.R.D.D which is different

from D. Then B is said to be a maximal C - set of D iff for all C - sets B' of D $[B \subset B'$ implies that $B' = D]$.

Definition 3.5.22 Let A be a sub-P.R.D. of a P.R.D. D which is different from D. Then A is said to be a maximal sub-P.R.D. of D iff for all sub-P.R.D.'s A of D$[A \subset A$ implies that $A' = D]$.

Theorem 3.5.23 Let B be a C-set of a P.R.D. D. Then there exists a bijection between the set of C - sets of D containing B and the set of C - sets of D/B and this bijection takes maximal C - sets to maximal C - sets.

Proof. It is similar to the proof of Theorem 2.3.19.

Remark: We can define a bijection between the set of sub-P.R.D.'s of D containing a C - set B of D and the set of sub-P.R.D.'s of D/B as we defined the bijection in the above theorem. This bijection takes maximal sub-P.R.D.'s to maximal sub-P.R.D.'s.

Theorem 3.5.24 Let S be a commutative semiring. Then S can be embedded into a commutative P.R.D. D iff S is M.C. Furthermore, if S is also A.C. then the smallest P.R.D. containing S must be A.C.

Proof. The proof of the first part is in [4] where it is shown that $((S \times S)/\sim, +, \cdot)$ is a commutative P.R.D. where $\sim$ is an equivalence on $S \times S$ defined by $(a,b) \sim (c,d)$ iff $ad = cb$, and $+, \cdot$ are binary operations on S defined as follows: given $\alpha, \beta \in (S \times S)/\sim$ choose $(a,b) \in \alpha$, $(c,d) \in \beta$

and then let $\alpha + \beta = [(ad + cb,bd)]$, $\alpha.\beta = [(ac,bd)]$. Next we shall show the second part. Assume that S is A.C. Let $\alpha,\beta,\gamma \varepsilon (S \times S)/\sim$ be such that $\alpha + \beta = \alpha + \gamma$. Choose $(a,b) \varepsilon \beta$, $(c,d) \varepsilon \beta$ and $(e,f) \varepsilon \gamma$. Then $[(ad + cb,bd)] = [(a,b)] + [(c,d)] = [(a,b)] + [(e,f)] = [(af + eb,bf)]$ so $(ad + cb)bf = (af + eb)bd$ ie. $adbf + cbbf = afbd + ebbd$. Since $\cdot$ is commutative and S is A.C., $cbbf = ebbd$. Because $\cdot$ is commutative and S is M.C., $cf = ed$ ie. $[(c,d)] = [(e,f)]$. Therefore $\beta = \gamma$. Hence $(S \times S)/\sim$ is A.C. #

Remarks: 1) The commutative P.R.D. in the previous theorem is the smallest P.R.D. containing S up to isomorphism and we shall call it the fractional P.R.D.

2) Let $\mathbb{Q}^+[X] = \mathbb{Q}^+_0[X]\setminus\{0\}$ where $\mathbb{Q}^+_0[X]$ is the set of polynomials with coffecients in $\mathbb{Q}^+_0$. Then $\mathbb{Q}^+[X]$ is a M.C. commutative semiring. By the previous Theorem, $\mathbb{Q}^+[X]$ can be embedded into its fractional P.R.D. which is denoted by $\mathbb{Q}^+(X)$.

Definition 3.5.25 Let D be a commutative P.R.D. and $x \varepsilon D$. Then a rational expression of x is an expression of the from $\sum_{i<\infty} a_i x_i^{n_i}$ where $a_i \varepsilon D$ and $n_i \varepsilon \mathbb{Z}$ $\forall$ i.

Let D be a commutative P.R.D. and $x \varepsilon D$. We shall define a set B_x. Let $y \varepsilon D$. Then $y \varepsilon B_x$ iff $\exists$ $u,v \varepsilon D$ satisfying the following two properties;

1) $y = uv^{-1}$ and

2) $\exists$rational expressions of x for u,v $u = \sum_{i<\infty} a_i x^{m_i}$ and $v = \sum_{j<\infty} x^{n_i}$ such that $\sum_i a_i = \sum_i b_j$.

We can prove that B_x is a C - set of D.

<u>Remark:</u> We have that $\mathbb{Q}^+(X)$ is a commutative P.R.D. and $X + 1 \; \varepsilon \; \mathbb{Q}^+(X)$ so B_{X+1} is a C - set of $\mathbb{Q}^+(X)$. Now we shall show that B_{X+1} has the following properties:

1) $\{1\} \subset B_{X+1}$ (To prove this, $X + 1 = (1.(X+1)^1).(1.(X+1)^o)^{-1} \; \varepsilon \; B_{X+1}$ so $\{1\} \neq B_{X+1}$)

2) $2 \notin B_{X+1}$ (To prove this, suppose $2 \; \varepsilon \; B_{X+1}$ so $2 = uv^{-1}$ where $u = \sum_i a_i(X+1)^{n_i}$ and $v = \sum_j b_j(X+1)^{m_j}$ for some $a_i, b_j \; \varepsilon \; \mathbb{Q}^+(X)$, $n_i, m_j \; \varepsilon \; \mathbb{Z}$, $i,j \; \varepsilon \; \mathbb{N}_o$ such that $\sum_i a_i = \sum_j b_j$. Suppose $a_i = c_i.d_i^{-1}$, $b_j = x_j.y_j^{-1}$ for some $c_i, d_i x_j, y_j \; \varepsilon \; \mathbb{Q}^+[X]$. Then $2 = (\prod_{k,l} d_k y_l)(\sum_i a_i(X+1)^{n_i}).((\prod_{k,l} d_k y_l)(\sum_i b_i(X+1)^{m_j})^{-1} = (\sum_i a'_i(X+1)^{n_i})(\sum_j b'_j(X+1)^{m_j})$ where $a'_i, b'_j \; \varepsilon \; \mathbb{Q}^+[X]$ and $\sum_i a'_i = \sum_j b'_i$. Hence we may assume that $a_i, b_j \; \varepsilon \; \mathbb{Q}^+[X] \; \forall i,j$.

Then we have that

$$\sum_j 2(X+1)^{m_j} b_j = \sum_i (X+1)^{n_i} a_i \qquad ....(*)$$

Because $a_i, b_j \in \mathbb{Q}^+[X]$, $a_i = \sum_k a_i^{(k)} X^k$ and $b_j = \sum_l b_j^{(l)} X^l$ where $a_i^{(k)}, b_j^{(l)} \in \mathbb{Q}_o^+$ and not all $a_i^{(k)}$ are 0 and not all $b_j^{(l)}$ are 0. Look at the equation (*) and consider the terms of degree 0, we have that $\sum_j (2b_j^{(0)}) = \sum_i a_i^{(0)}$. Because $\sum_l a_i = \sum_j b_j$, $\sum_i a_i^{(0)} = \sum_j b_j^{(0)}$ so $\sum_j 2b_j^{(0)} = \sum_j b_j^{(0)}$. Hence $\sum_j b_j^{(0)} = 0$ so $\sum_i a_i^{(0)} = 0$. Therefore $a_i^{(0)} = 0 \ \forall i$, $b_j^{(0)} = 0 \ \forall j$. Next we shall show that $\sum_j b_j^{(k)} = 0 = \sum_i a_i^{(k)} \ \forall k$. We shall prove this by induction on k. Assume that $\sum_j b_j^{(\alpha)} = 0 = \sum_i a_i^{(\alpha)} \ \forall \alpha \leq k$. We shall show that $\sum_j b_j^{(k+1)} = \sum_i a_i^{(k+1)}$. We have that $a_i^{(\alpha)} = 0 = b_j^{(\alpha)}$ $\forall \alpha \leq k$, $\forall i,j$. Then look at the equation (*) and consider the terms of degree k + 1, we get that $\sum_j 2b_j^{(k+1)} = \sum_i a_i^{(k+1)}$. Because $\sum_j b_j = \sum_i a_i$, $\sum_j b_j^{(k+1)} = \sum_i a_i^{(k+1)}$ so $\sum_j b_j^{(k+1)} = \sum_j 2b_j^{(k+1)}$. Therefore $\sum_j b_j^{(k+1)} = 0 = \sum_i a_i^{(k+1)}$. Thus $\sum_j b_j^{(k)} = 0 = \sum_i a_i^{(k)} \ \forall k$. Hence $a_i^{(k)} = 0 = b_j^{(k)} \ \forall i,j,k$, which is a contradiction. Hence $2 \notin B_{X+1}$).

1) and 2) implies that $\{1\} \subset B_{X+1} \subset \mathbb{Q}^+(X)$ ie. $\mathbb{Q}^+(X)$ is not simple.

Theorem 3.5.26 There exists an extension P.R.D. of $\mathbb{Q}^+$ which is not A.C.

Proof. Put $D = \mathbb{Q}^+(X)/B_{X+1}$. Then D is a P.R.D. Fist we shall show that D is not A.C. ie. $\exists \alpha, \beta, \gamma \in D$ such that $\alpha + \gamma = \beta + \gamma$ but $\alpha \neq \beta$. Put $\alpha = [X]$, $\beta = \alpha + \alpha$ and $\gamma = [1]$. Then $\alpha + [1] = [X] + [1] = [X + 1] = [1]$ so $\beta + \gamma = \alpha + \alpha + [1] = \alpha + [1] = \alpha + \gamma$. Suppose $\beta = \gamma$. Then $[2] \cdot \alpha = \alpha + \alpha = \alpha$. Because $\alpha \in D$ and D is a P.R.D, $[2] = [1]$. So $2 \in B_{X+1}$ which is a contradiction. Hence $\alpha \neq \beta$. Therefore D is not A.C. Next we shall show that D is an extension P.R.D. of $\mathbb{Q}^+$. Define $\phi: \mathbb{Q}^+ \rightarrow D$ by $\phi(a) = [a]$. Clearly ϕ is a P.R.D. homomorphism. So $\ker \phi \trianglelefteq \mathbb{Q}^+$. By Proposition 3.5.18, $\ker \phi = [1]$ or $\mathbb{Q}^+$. If $\ker \phi = \mathbb{Q}^+$ then $[1] = [2]$ which is a contradiction. Hence $\ker \phi = \{1\}$ so ϕ is 1-1. Therefore $\mathbb{Q}^+ \cong \phi(\mathbb{Q}^+)$. Thus D is an extension P.R.D. of $\mathbb{Q}^+$ which is not A.C. #

Theorem 3.5.27 There exists an A.C. P.R.D. which can not be embedded is a field.

Proof. Let k be a field and x an element of k such that $x^2 + 1 = 2x$. Then $(x - 1)^2 = x^2 + 1 - 2x = 0$ so $x = 1$. So we want to construct an A.C. P.R.D. having an element x such that $x^2 + 1 = 2x$ and $x \neq 1$. Such a P.R.D. cannot be embedded in a field.

We have that $\mathbb{Q}^+[X]$ is a commutative semiring. Define a binary realtion $\sim$ on $\mathbb{Q}^+[X]$ as follows: say that $F \sim G$ iff $\exists K_1, K_2 \in \mathbb{Q}^+[X]$ such that $F + (X^2 + 1)K_1 + 2XK_2 = G + (X^2 + 1)K_2 + 2XK_1$. Clearly $\sim$ is a congruence on $\mathbb{Q}^+[X]$. Let $S = \mathbb{Q}^+[X]/\sim$. Then S is a semiring in a natural way.

Note that $x^2 + 1 \sim 2x$ (Just let $K_1 = 1$ and $K_2 = 2$). Let $x = [X]$ so $x^2 + 1 = 2x$ in S. Claim that $x \neq 1$ ie. $X \not\sim 1$. To prove this, suppose not. Then $X \sim 1$. Hence $\exists K_1, K_2 \in \mathbb{Q}^+[X]$ such that

$$X + (X^2 + 1)K + 2XK_2 = 1 + (X^2 + 1)K_2 + 2XK_1 \quad ....(*)$$

Since $\mathbb{Q}^+[X] \subset \mathbb{Q}[X]$, we can consider the equation (*) to be an equation in $\mathbb{Q}[X]$ where we can subtract. Subtracting we get that $X - 1 = (X^2 - 1)(K_2 - K_1) - 2(K_2 - K_1) = (X - 1)^2(K_2 - K_1)$ which is a contradiction. So we have the claim.

Just as we construct the fractional field of an integral domain we want to construct a fractional P.R.D. of S. To do this we must show that S is M.C. Let $\alpha, \beta, \gamma \in S$ be such that $\alpha\gamma = \beta\gamma$ and $\gamma \neq 0$. We must show that $\alpha = \beta$. Choose $F \in \alpha$, $G \in \beta$ and $H \in \gamma$. If $F = G$ then $\alpha = \beta$ so done. Hence we may assume that $F \neq G$. Then $FH \sim GH$ so $\exists K_1, K_2 \in \mathbb{Q}^+[X]$ such that

$$FH + (X^2 + 1)K_1 + 2XK_2 = GH + (X^2 + 1)K_2 + 2XK_1 \quad .....(**)$$

<u>case 1</u> deg H = 0. Because $H \in \mathbb{Q}^+[X]$, $H \neq 0$, so H is a nonzero constant. Divide both sides of the equation (**) by H and we get that $F \sim G$. Therefore $\alpha = \beta$ so we are done.

<u>case 2</u> deg H > 0. Consider (**) to be an equation in $\mathbb{Q}[X]$ where can subtract. Subtracting we get that $(F - G)H = (X - 1)^2(K_2 - K_1)$ Since deg H > 0, H has irreducible factors. Let P be an irreducible

factor of H. Since $\mathbb{Q}[X]$ is a U.F.D, either $P = X - 1$ or P is an irreducible factor of $K_2 - K_1$. If $P = X - 1$ then $H = (X - 1)Q$ for some $Q \varepsilon \mathbb{Q}[X]$. Hence $H(1) = 0$ which is a contradiction since $H \varepsilon \mathbb{Q}^+[X]$. Hence P is an irreducible factor of $K_2 - K_1$. So we see that every irreducible factor of H is an irreducible factor of $K_2 - K_1$. Hence $H|(K_2 - K_1)$ so $K_2 - K_1 = HL$ for some $L \varepsilon \mathbb{Q}[X]$. So the equation (**) becomes $(F - G)H = (X - 1)^2 LH$

Cancelling H (remember $H \neq 0$) we get that

$$F - G = (X - 1)^2 L \qquad \text{...........(***)}$$

Because $L \varepsilon \mathbb{Q}[X]$, $L = L_2 - L_1$ for some $L_1, L_2 \varepsilon \mathbb{Q}^+[X]$. So (***) becomes

$$F - G = (X^2 + 1 - 2X)(L_2 - L_1)$$

Hence $F \sim G$ therefore $\alpha = \beta$. So we have that S is M.C.. Clearly S is a commutative semiring. Next we shall show that S is A.C. Let $\alpha, \beta, \gamma \varepsilon S$ be such that $\alpha + \gamma = \beta + \gamma$. Choose $F \varepsilon \alpha$, $G \varepsilon \beta$, $H \varepsilon \gamma$. Then $F + H \sim G + H$. Clearly $F \sim G$. Hence $\alpha = \beta$. So S is A.C. By Theorem 3.5.24, there exists an A.C. P.R.D. D containing S. We prove that $\exists x \varepsilon S \subsetneq D$ such that $x^2 + 1 = 2x$ and $x \neq 1$. Hence D cannot be embedded in a field.

#

Theorem 3.5.28 Every finite semigroup has an idempotent.

Proof. See [2].

Corollary 3.5.29 For finite P.R.D. with the multiplicative identity 1, $1 + 1 = 1$.

Proof. Let $(D,+,\cdot)$ be a finite P.R.D. with the multiplicative identity 1. So $(D,+)$ has an idempotent e ie. $e + e = e$. Hence $1 + 1 = 1$

#

Let D_1,D_2 be finite P.R.D.'s. Let $D = D_1 \times D_2$ and define binary operations $+,\cdot$ on D as follows $(x_1,x_2) + (y_1,y_2) = (x_1+ y_1,x_2+ y_2)$ and $(x_1,x_2).(y_1,y_2) = (x_1 \cdot y_1,x_2 \cdot y_2)$. Then $(D,+,\cdot)$ is a P.R.D. Let $B_1= \{(x_1,1)|x \varepsilon D_1\}$ and $B_2= \{(1,y)|y \varepsilon D_2\}$. Then

1) B_1 and B_2 are C - sets of D. (To prove this, let $(x_1,1),(y_1,1) \varepsilon B_1$ then clearly $(x_1,1).(y_1,1)^{-1} \varepsilon B_1$ Let $(a,b) \varepsilon D$ and $(x,1) \varepsilon B_1$ then $((a,b) + (1,1))^{-1}.((a,b)+(x,1)) =((a + 1,b + 1))^{-1}.(a + x,b + 1) = ((a + 1)^{-1}.(a + x),1) \varepsilon B_1$. Hence $B_1 \trianglelefteq D$. Similarly we can prove that $B_2 \trianglelefteq D$).

2) $B_1 \cap B_2 = \{(1,1)\}$.

3) B_1,B_2 generate D.

4) B_1,B_2 satisfy $(\alpha_1+ \beta_1)\cdot(\alpha_2+ \beta_2) = \alpha_1 \cdot \alpha_2 + \beta_1 \cdot \beta_2$ for all $\alpha_1,\beta_1 \varepsilon B_1$ and $\alpha_2,\beta_2 \varepsilon B_2$. (To prove this, let $(x_1,1),(y_1,1) \varepsilon B_1$ and $(1,x_2)$, $(1,y_2) \varepsilon B_2$ then $(x_1,1).(1,x_2) + (y_1,1).(1,y_2) = (x_1,x_2) + (y_1,y_2) = (x_1+y_1,x_2+ y_2) = (x_1+ y_1,1)\cdot(1,x_2+ y_2)$ and

$((x_1,1)\cdot(y_1,1))\cdot((1,x_2)+(1,y_2)) = (x_1+ y_1,1 + 1).(1 + 1,x_2+ y_2) =$ $(x_1+ y_1,1)\cdot(1,x_2+ y_2)$, by Corollary 3.5.29. Hence $((x_1,1)+(y_1,1))\cdot$ $((1,x_2)+(1,y_2)) = (x_1,1)(1,x_2)+(y_1,1)(1,y_2))$.

Theorem 3.5.30 Let D be a finite P.R.D. having two C - sets B_1,B_2 such that $B_1 \cap B_2 = \{1\}$, B_1 and B_2 generate D and $(\alpha_1+ \beta_2)\cdot(\alpha_2+ \beta_2) =$ $\alpha_1.\alpha_2 + \beta_1.\beta_2$ for all $\alpha_1,\beta_1 \varepsilon B_1$, $\alpha_2,\beta_2 \varepsilon B_2$. Then $D \cong B_1 \times B_2$.

Proof. First we shall show that B_1 and B_2 are P.R.D.'s. Let $a,b \varepsilon B_1$. Then $a + b = (1 + 1)^{-1}(a + b) = (1 + 1)^{-1}(1 + b)(1 + b)^{-1}$ $(a + b) \varepsilon B_1$. Because $B_1 \trianglelefteq D$, B_1 is a P.R.D. Similarly we can prove that B_2 is a P.R.D. Claim that $\forall a_1 \varepsilon B_1$, $a_2 \varepsilon B_2$ $a_1.a_2= a_2.a_1$. To prove this, let $a_1 \varepsilon B_1,a_2 \varepsilon B_2$. Then $a_1.a_2.a_1^{-1}.a_2^{-1} \varepsilon B_1 \cap B_2 = \{1\}$ so $a_1.a_2 = a_2.a_1$. Hence we have the claim. Because B_1 and B_2 generate D, $D = B_1.B_2$.

Define $\phi:B_1\times B_2 \to D$ by $\phi(x_1,x_2) = x_1.x_2$. Clearly ϕ is well-defined. We shall show that ϕ is 1-1. Let $(x_1,x_2),(y_1,y_2) \varepsilon B_1 \times B_2$ be such that $x_1.x_2 = y_1.y_2$ so $y_1^{-1}.\ x_1 = y_2.x_2^{-1} \varepsilon B_1 \cap B_2 = \{1\}$ therefore $y_1= x_1$ and $y_2= x_2$ ie. $(x_1,x_2) = (y_1,y_2)$. Hence ϕ is 1-1. Next we shall show that ϕ is onto. Let $d \varepsilon D$. By the claim, $D = B_1.B_2$ so $d = b_1.b_2$ for some $b_1\varepsilon B_1$, $b_2 \varepsilon B_2$. Then $\phi(b_1,b_2) = b_1.b_2 = d$. Hence ϕ is onto. Lastly we shall show that ϕ is a homomorphism. Let $(x_1,x_2),(y_1,y_2) \varepsilon B_1\times B_2$

then $\phi(x_1,x_2) + \phi(y_1,y_2) = x_1.x_2+ y_1y_2 = (x_1+ y_1).(x_2+ y_2) =$ $\phi(x_1+ y_1,x_2+ y_2) = \phi((x_1,x_2) + (y_1,y_2))$ and $\phi(x_1,x_2)\cdot \phi(y_1,y_2) =$ $(x_1.x_2).(y_1.y_2) = (x_1.y_1).(x_2.y_2) = \phi(x_1.y_1,x_2.y_2) = \phi((x_1,x_2).(y_1,y_2))$ (by the claim). Hence $D \cong B_1 \times B_2$.

#

Remark: We see that C - sets of a finite P.R.D. D are factors in the direct product of D.

Theorem 3.5.31 Let D be a finite P.R.D. Then $D \simeq D_1 \times D_2$ where D_1 is a P.R.D. having the property that $x + y = x$ for all $x,y \in D_1$ and D_2 is a P.R.D. having the property that $x + y = y$ for all $x,y \in D_2$.

Proof. Let $D_1 = \{z \in D | z + 1 = z\}$ and $D_2 = \{z \in D | z + 1 = 1\}$. Then $D_1 \neq \emptyset$, $D_2 \neq \emptyset$ since $1 \in D_1 \cap D_2$. First we shall show that D_1, D_2 are P.R.D.'s. Let $a,b \in D_1$. Then $(a + b) + 1 = a + (b + 1) = a + b$ and $a.b + 1 = (a + 1).b + 1 = a.b + b + 1 = a.b + b = (a+ 1).b = a.b$. Therefore $a + b \in D_1$ and $a.b \in D_1$. Let $a \in D_1$. If $a = 1$ then $a^{-1} = 1 \in D_1$. We may assume that $a \neq 1$. We have that $a^n \in D_1 \ \forall n \in \mathbb{N}$. Since $a \in D$ and $(D,\cdot)$ is a finite group, $\exists n \in \mathbb{N} \setminus \{1\} \ni a^n = 1$ ie. $a^{n-1}.a = 1$. so $a^{-1} = a^{n-1} \in D_1$. Hence D_1 is a P.R.D. Let $a,b \in D_2$. Then $(a + b) + 1 = a + (b + 1) = a + 1 = 1$ and $a.b + 1 = a.b + (a + 1) = a.(b + 1) + 1 = a.1 + 1 = 1$. So $a + b, a.b \in D_2$. We can show that $a^{-1} \in D_2 \ \forall a \in D_2$ as we showed that $a^{-1} \in D_1 \ \forall a \in D_1$. Hence D_2 is a P.R.D.

Next we shall show that $\forall\, x,y \in D_1 \quad x + y = x$ and $\forall\, x,y \in D_2$ $x + y = y$. Let $x,y \in D_1$. Then $x.y^{-1} \in D_1$ so $x.y^{-1} + 1 = x.y^{-1}$. Therefore $x + y = (x.y^{-1} + 1).y = (x.y^{-1}).y = x$. Let $x,y \in D_2$. Then $x.y^{-1} \in D_2$ so $x.y^{-1} + 1 = 1$. Therefore $x + y = (x.y^{-1} + 1).y = 1.y = y$.

Now we shall show that D_1 and D_2 satisfy all conditions of Theorem 3.5.30. Clearly $D_1 \cap D_2 = \{1\}$. Claim that $d' + d + d' = d'$ $\forall\, d,d' \in D$. To prove this, we can show that $1 + d + 1 = 1 \quad \forall\, d \in D$ since $d + 1 \in D_1$. Let $d,d' \in D$. Then $d.d'^{-1} \in D$ so $1 + d.d'^{-1} + 1 = 1$. Therefore $d' + d + d' = (1 + d.d'^{-1} + 1)d' = 1.d' = d'$. Hence we have the claim. We shall show that $D_1 \lhd D$ and $D_2 \lhd D$. Let $a \in D_1$, $x \in D$. Then $x^{-1}ax + 1 = x^{-1}.a.x + x^{-1}.x = x^{-1}.(a + 1).x = x^{-1}.a.x$, and $(x + 1)^{-1}.(x + a) + 1 = (x + 1)^{-1}.(x + a) + (x + 1)^{-1}.(x + 1) = (x + 1)^{-1}.(x + a + x + 1) = (x + 1)^{-1}.(x + a + 1 + x + 1) = (x + 1)^{-1}.(x + a + 1) = (x + 1)^{-1}.(x + a)$. Therefore $x^{-1}.a.x$, $(x + 1)^{-1}.(x + a) \in D_1$. Similarly we can prove that $(1 + x)^{-1}.(a + x) \in D_1$. Thus $D_1 \lhd D$. Let $a \in D_2, x \in D$. Then $x^{-1}.a.x + 1 = x^{-1}.a.x + x^{-1}.x = x^{-1}.(a + 1).x = x^{-1}.1.x = 1$, and $(x + 1)^{-1}.(x + a) + 1 = (x + 1)^{-1}.(x + a) + (x + 1)^{-1}.(x + 1) = (x + 1)^{-1}.(x + a + x + 1) = (x + 1)^{-1}.(x + 1) = 1$. Therefore $x^{-1}.a.x$, $(x + 1)^{-1}.(x + a) \in D_2$. Similarly we can prove that $(1 + x)^{-1}.(a + x) \in D_2$. Thus $D_2 \lhd D$. Next we shall show that $D = D_1.D_2$. Let $d \in D$. Then $d + 1 \in D_1$ and $(d + 1)^{-1}.d + 1 = (d + 1)^{-1}.d + (d + 1)^{-1}.(d + 1) = (d + 1)^{-1}.(d + d + 1) = (d + 1)^{-1}.(d + 1) = 1$ ie. $(d + 1)^{-1}.d \in D_2$. Because $d = (d + 1).(d + 1]^{-1}.d \in D_1.D_2$ hence D_1 and D_2 generate D.

Lastly we shall show that $\forall a_1, b_1 \varepsilon D_1$, $\forall a_2, b_2 \varepsilon D_2 (a_1 + b_1).(a_2 + b_2) = a_1.a_2 + b_1.b_2$. Let $a_1, b_1 \varepsilon D_1$ and $a_2, b_2 \varepsilon D_2$. Then $a_1.a_2 + b_1.b_2 = (a_1 + b_1).\ a_2 + (b_1 + a_1)\ .\ b_2 = a_1.a_2 + b_1.a_2 + b_1.b_2 + a_1.b_2 = a_1.a_2 + b_1.a_2 + b_1.b_2 + (a_1 + b_1).(a_2 + b_2) = a_1.a_2 + b_1.a_2 + b_1.b_2 + a_1.a_2 + b_1.a_2 + a_1.b_2 + b_1.b_2 = a_1.a_2 + b_1.b_2 + a_1.b_2 + b_1.b_2 = (a_1 + b_1).(a_2 + b_2)$. By Theorem 3.5.30, $D \cong D_1 \times D_2$. #

Definition 3.5.32 Let B be a C - set of a P.R.D. D. Then B is a prime C - set iff if $(a + 1)^{-1}(a + x) \varepsilon B$ or $(1 + a)^{-1}(x + a) \varepsilon B$ then $a \varepsilon B$.

Theorem 3.5.33 Let B be a C - set of a P.R.D. D. Then B is a prime C - set iff D/B is A.C.

Proof. Assume that B is a prime C - set. Let $\alpha, \beta \varepsilon D/B$ be such that $\alpha + \gamma = \beta + \gamma$. Choose $a \varepsilon \alpha$, $b \varepsilon \beta$ and $c \varepsilon \gamma$. Then $[a + c] = [b] + [c] = [b + c]$. hence $(a + c)^{-1}(b + c) \varepsilon B$ ie. $(b^{-1}.a + b.^{-1}c)^{-1}.(1 + b^{-1}.c) \varepsilon B$ so $b^{-1}.\ a \varepsilon B$. Therefore $[a] = [b]$. Hence D/B is A.C.

Assume that D/B is A.C. Let $a, b \varepsilon D$ be such that $(a + 1)^{-1}.(a + b) \varepsilon B$ so $[a] + [1] = [a + b] = [a] + [b]$. Hence $[1] = [b]$ ie. $b \varepsilon B$. Therefore B is a prime C - set. #

3.6 P.R.D. modules.

In this section we shall work with left congruences on a P.R.D. But everything that we prove for left congruences can be similarly proved for right congruences also. As in Section 3.5 we shall consider the categories $\mathscr{D}$, $\mathscr{D}_o$, $\mathscr{D}_i$.

We shall define naturally equivalent contravariant functors from $\mathscr{D}$ to $\mathscr{L}$, naturally equivalent covariant functors from $\mathscr{D}_o$ to $\mathscr{L}$ and naturally equivalent covariant functors from $\mathscr{D}_i$ to $\mathscr{Q}$ by using

1) double left congruences, double left C - sets and double left semigroup-spaces,

2) multiplicative left congruences, multiplicative left C - sets and left semimodules,

3) additive left congruences, additive left C - sets and left P.R.D. modules.

Definition 3.6.1 A double left congruence on a P.R.D. D is an equivalence relation ρ on D such that $x \rho y$ implies that $(a + x) \rho (a + y)$ and $(a.x) \rho (a.y)$ for all $x,y,a \in D$.

Definition 3.6.2 A multiplicative left congruence on a P.R.D. D is an equivalence relation ρ on D such that $x \rho y$ implies that $(a + x) \rho (a + y)$, $(x + a) \rho (y + a)$ and $(a.x) \rho (a.y)$ for all $x,y,a \in D$.

Definition 3.6.3 An additive left congruence on a P.R.D. D is an equivalence relation ρ on D such that $x \rho y$ implies that $(a + x) \rho (a + y)$, $(a.c) \rho (a.y)$ and $(x.a) \rho (y.a)$ for all $x,y,a \in D$.

Definition 3.6.4 A double left C - set of a P.R.D. D is a multiplicative subgroup B of D such that for each $d \in D$, $b \in B$, $(d + 1)^{-1}.(d + b) \in B$.

Definition 3.6.5 A multiplicative left C - set of a P.R.D. D is a multiplicative subgroup B of D such that for each $d \varepsilon D$, $b \varepsilon B$ $(d + 1)^{-1}.(d + b)$, $(1 + d)^{-1}.(b + d) \varepsilon B$.

Definition 3.6.6 An additive left C - set of a P.R.D. D is a multiplicative subgroup B of D such that for each $d \varepsilon D$, $b \varepsilon B$ $d^{-1}.b.d \varepsilon B$ and $(d + 1)^{-1}.(b + d) \varepsilon B$.

Definition 3.6.7 Let D be a P.R.D. A double left D-space is a triple $(M,+,\cdot)$ where $(M,+)$ and $(M,\cdot)$ are left D-spaces such that $d.(d' + m) = d.d' + d.m$ and $1.m = m$ for all $m \varepsilon M$, $d,d' \varepsilon D$.

Definition 3.6.8 Let D be a P.R.D. A left D-semimodule is a triple $(M,+,\cdot)$ where $(M,+)$ is a semigroup and $(M,\cdot)$ is a left D-space such that $d.(n + m) = d.n + d.m$ and $1.m = m$ for all $m,n \varepsilon M$, $d \varepsilon D$.

Definition 3.6.9 Let D be a P.R.D. A left D-module is a triple $(M,+,\cdot)$ where $(M,+)$ is a left D-space and $(M,\cdot)$ is a group.

Remark: For each P.R.D. D,D is a double left D-space, a left D-semimodule and a left D-module.

Now we shall only work with double left congruences. But everything that we define and prove for double left congruences can be similarly defined and proved for multiplicative left congruences and additive left congruences.

Definition 3.6.10 Let D be a P.R.D, M,M' double left D-spaces and $\phi:M \rightarrow M'$

a map. Then ϕ is said to be double left D-equivariant iff $\phi(d + m) = d + \phi(m)$ and $\phi(d.m) = d.\phi(m)$ for all $d \varepsilon D, m \varepsilon M$.

Remarks: 1) If ϕ is a bijectively double left D-equivariant map then ϕ^{-1} is double left D-equivariant. We shall call such a map a double left D-space isomorphism.

2) If ρ is a double left congruence on a P.R.D.D then the set D/ρ of equivalence classes of D can be made into a double left D-space in natural way and the natural projection map $\pi:D \to D/\rho$ is an onto double left D-equivariant map.

3) If ρ is a double left congruence on a P.R.D.D then $[1]_\rho = \{d \varepsilon D | d \rho 1\}$ is a double left C - set of D.

4) If B is a double left C - set of P.R.D.D then $\{(a,b) \varepsilon D \times D | a^{-1}b \varepsilon B\}$ is a double left congruence on D.

Definition 3.6.11 Let D be a P.R.D. A quotient double left D-space is a pair (K,ϕ) where K is a double left D-space and $\phi:D \to M$ is an onto double left D-space equivariant map.

Example. $(D/\rho,\pi)$ is a quotient double left D-space where ρ is a double left congruence on D.

Theorem 3.6.12 Let D be a P.R.D. and (K,ϕ) a double left D-space. Let $\rho = \{(a,b) \varepsilon D \times D | \phi(a) = \phi(b)\}$. Then ρ is a double left congruence on D and there exists a double left D-space isomorphism ψ from D/ρ onto K such that $\psi o \pi = \phi$.

Proof. It is similar to the proof of Theorem 3.5.5.

Definition 3.6.13 Let (K,ϕ) and (K',ϕ') be quotient double left D-spaces. Say that (K,ϕ) is strongly equivalent to (K',ϕ') iff there exists a double left D-space isomorphism $\psi:K \to K'$ such that the following diagram is commutative

$$\begin{tikzcd} & D \arrow[dl, "\phi"'] \arrow[dr, "\phi'"] & \\ K \arrow[rr, "\psi"] & & K' \end{tikzcd}$$

Write this as $(K,\phi) \simeq (K',\phi')$.

Remarks: 1) $\simeq$ is an equivalence relation on the set of quotient double left D-spaces.

2) For each quotient double left D-space (K,ϕ), $(K,\phi) \simeq (D/\rho,\pi)$ where $\rho = \{(a,b) \in D \times D \mid \phi(a) = \phi(b)\}$.

Proposition 3.6.14 If $\phi:D \to D'$ is an onto P.R.D. homomorphism and ρ is a double left congruence on D then $(\phi \times \phi)(\rho)$ is a left double congruence on D'.

Proof. If is similar to the proof of Proposition 3.5.10.

Proposition 3.6.15 If $\phi:D \to D'$ is a P.R.D. homomorphism and ρ' is double left congruence on D' then $(\phi \times \phi)^{-1}(\rho')$ is a double left congruence on D.

Proof. It is standard.

Fix a P.R.D. D, let LB(D) = the set of double left C - sets of D ,

LC(D) = the set of double left congruences on D,

LQ(D) = the set of equivalence
classes of quotient double
left D-space under $\simeq$.

We define natural relations $\subseteq$ on LB(D), LC(D) and LQ(D) as $\subseteq$ on B(D), C(D) and Q(D) in Section 3.5, respectively. Then the proofs that (LB(D),$\subseteq$),(LC(D),$\subseteq$) and (LQ(D),$\subseteq$) are posets are similar to the proofs that (B(D),$\subseteq$) (C(D),$\subseteq$),(C(D),$\subseteq$) and (Q(D),$\subseteq$) are posets, respectively.

Theorem 3.6.16 For each P.R.D. D, the posets LB(D), LC(D) and LQ(D) are isomorphic.

Proof. It is similar to the proof of Theorem 3.5.11 and the isomorphisms have the same form as in Theorem 3.5.11.

Remark: Fix a P.R.D. D, let $B_1, B_2 \in$ LB(D). Then $B_1 \cap B_2$ = g.l.b.$\{B_1, B_2\}$ and the double left C - set of D generated by $B_1 \cup B_2$ = l.u.b. $\{B_1, B_2\}$. Hence LB(D) is a lattice. Therefore LC(D) and LQ(D) are lattices also.

We define contravariant functors LB, LC and LQ from $\mathscr{D}$ to $\mathscr{L}$ as we defined the contravariant functors B,C,Q from $\mathscr{D}$ to $\mathscr{L}$ in Section 3.5, respectively. Then the proof that LB,LC and LQ are naturally equivariant contravariant functors is similar to the proof that B,C and Q are naturally equivariant contravariant functors.

We define covariant functors LB', LC' and LQ' from $\mathscr{D}_o$ to $\mathscr{L}$ as we defined the covariant functors B', C', Q' from $\mathscr{D}_o$ to $\mathscr{L}$ in Section 3.5, respectively. Then the proof that LB', LC' and LQ' are naturally equivariant covariant functors is similar to the proof that B', C' and Q' are naturally equivalent functors.

Definition 3.6.17 Let D be a P.R.D. and B_1, B_2 double left congruence sets of D. Say that B_1 is equivalent to B_2 ($B_1 \sim B_2$) iff there exists a P.R.D. automorphism $\phi : D \to D$ such that $\phi(B_1) = B_2$.

Remark: $\sim$ is an equivalence relation on the set of double left congruence sets of a P.R.D.

Definition 3.6.18 Let D be a P.R.D. and ρ_1, ρ_2 double left congruences on D. Say that ρ_1 is equivalent to ρ_2 ($\rho_1 \sim \rho_2$) iff there exists a P.R.D. automorphism $\phi : D \to D$ such that $(\phi \times \phi)(\rho_1) = \rho_2$.

Remark: $\sim$ is an equivalence relation on the set of double left congruences on a P.R.D.

Definition 3.6.19 Let (K,ϕ) and (K',ϕ') be quotient double left D-spaces. Say that (K,ϕ) is weakly equivalent to (K',ϕ') iff there exist a P.R.D. automorphism $f : D \to D$ and a left double D-space isomorphism $f' : K \to K'$ such that the following diagram is commutative.

$$\begin{tikzcd}
D \arrow[r, "f"] \arrow[d, "\phi"'] & D \arrow[d, "\phi'"] \\
K \arrow[r, "f'"] & K'
\end{tikzcd}$$

Write this as $(K,\phi) \sim (K',\phi')$.

Remarks: 1) $\sim$ is an equivalence relation on the set of quotient double left D-spaces.

2) $(K,\phi) \cong (K',\phi')$ implies that $(K,\phi) \sim (K',\phi')$.

Fix a P.R.D. D, let $LB^*(D)$ = the set of equivalence classes of double left congruence sets of D,

$LC^*(D)$ = the set of equivalence classes of double left congruences on D,

$LQ^*(D)$ = the set of equivalence classes of quotient doutle left D-Spaces under $\sim$.

We define binary relations $\leqslant$ on $LB^*(D)$, $LC^*(D)$ and $LQ^*(D)$ as $\leqslant$ on $B^*(D)$, $C^*(D)$ and $Q^*(D)$ in Section 2.5 respectively. Then the proofs that $(LB^*(D),\leqslant)$, $(LC^*(D),\leqslant)$ and $(LQ^*(D),\leqslant)$ are quasi-ordered sets are similar to the proofs that $(B^*(D),\leqslant)$ $(C^*(D),\leqslant)$ and $(Q^*(D),\leqslant)$ are quasi-ordered sets are quasi-ordered sets, respectively.

Theorem 3.6.20 For each P.R.D. D, the quasi-ordered sets $B^*(D)$, $C^*(D)$ and $Q^*(D)$ are isomorphic.

Proof. It is similar to the proof of Theorem 3.5.17 and the isomorphisms have the same form as in Theorem 3.5.17.

We define covariant functors LB^*, LC^*, and LQ^* from $\mathcal{D}_i$ to $\mathcal{Q}$ as we defined the covariant functors B^*, C^* and Q^* from $\mathcal{D}_i$ to $\mathcal{Q}$ in Section 3.5, respectively. Then the proof that LB^*, LC^* and LQ^* are naturally equivalent covariant functors is similar to the proof that

B^*, C^* and Q^* are naturally equivalent covariant functors.

3.7 Semifields

We shall give the same definition of a semifield as given in [4] without assuming that $+, \cdot$ are commutative.

Definition 3.7.1 A semifield is a triple $(S,+,\cdot)$ where S is a set and $+$ (addition), $\cdot$ (multiplication) are binary operations on S such that

i) $(S,\cdot)$ is a group with zero 0, ie. $(S \setminus \{0\},\cdot)$ is a group and $a.0 = 0 = 0.a$ for all $a \in S$,

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

iii) $x(y + z) = xy + xz$ and $(x + y)z = xz + yz$ for all $x,y,z \in S$.

Remarks: 1) A semifield is an algebraic system.

2) Let $(S,+,\cdot)$ be a semifield. Since $(S \setminus \{0\},\cdot)$ is a group, $|S| \geqslant 2$.

Examples Let $(G,\cdot)$ be a group with zero 0.

1) Define a binary operation $+$ on G by $x + y = 0$ for all $x,y \in G$. Clearly $(G,+,\cdot)$ is a semifield. We call this semifield a null semifield.

2) Define a binary operation $+$ on G by

$$x + y = \begin{cases} 0 & \text{if } x \neq y \\ x & \text{if } x = y \end{cases}$$

Then $(G,+,\cdot)$ is a semifield. We call this semifield an almost null semifield.

3) Define a binary operation + on G by $x + y = y$ for all $x,y \in G$ (or $x + y = x$ for all $x,y \in G$) Clearly $(G,+,\cdot)$ is a semifield.

Definition 3.7.2 Let S,S' be semifields. A semifield homomorphism from S to S' is a map $\phi:S \to S'$ such that for each $x,y \in S$

i) $\phi(x) = 0'$ iff $x = 0$ where $0,0'$ are multiplicative zeroes of S,S' respectively,

ii) $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(x.y) = \phi(x).\phi(y)$.

Remark: A semifield homomorphism is an operation preserving map.

This section will consider the following categories:

1) The category $\mathcal{S}_f$ of semifields and semifield homomorphisms.

2) The category $\mathcal{S}_{f,0}$ of semifields and onto semifield homomorphisms.

3) The category $\mathcal{S}_{f,i}$ of semifields and semifield isomorphisms.

We shall show that $\mathcal{S}_f$ has a congruence set so we shall define naturally equivalent contravariant functors from $\mathcal{S}_f$ to $\mathcal{L}$ by using congruences, C - sets and quotient semifields which are defined below.

Proposition 3.7.3 ρ is a congruence on an object $(S,+,\cdot)$ in $\mathcal{S}_f$ iff ρ is an operation preserving equivalence relation on the semifield

$(S,+,\cdot)$ such that $x \rho 0$ iff $x = 0$ for all $x \varepsilon S$.

Proof. Assume ρ is a congruence on $(S,+,\cdot)$. Then ρ is an operation preserving relation on $(S,+,\cdot)$ such that $(S/\rho,+,\cdot)$ is a semifield. Clearly $0 \rho 0$. Suppose $\exists x \varepsilon S\setminus\{0\}$ such that $x \rho 0$. So $\forall y \varepsilon S \quad y \rho 0$. Then $y \rho z \quad \forall y, z \varepsilon S$. Hence $\rho = S \times S$. So S/ρ has only one element which is a contradiction. Therefore $x \rho 0$ implies that $x = 0$. Hence $x \rho 0$ iff $x = 0$.

The converse is clear . #

Theorem 3.7.4 Let S be a semifield and let 0 denote the zero of S. Then exactly one of the following four cases must occur :

i) $x + 0 = 0 = 0 + x$ for all $x \varepsilon S$,

ii) $x + 0 = x = 0 + x$ for all $x \varepsilon S$,

iii) $x + y = y$ for all $x,y \varepsilon S$,

iv) $x + y = x$ for all $x,y \varepsilon S$,

Proof. Since $1 \neq 0$, if one case occurs then the others do not occur.

1. Note that either $\exists x \varepsilon S\setminus\{0\}$ such that $x + 0 = 0$ or $\forall x \varepsilon S\setminus\{0\} \quad x + 0 \neq 0$.

case 1.1 $\exists x \varepsilon S\setminus\{0\}$ such that $x + 0 = 0$. Let y be an arbitrary element in S. Then $yx^{-1}(x + 0) = yx^{-1}0$ so $y + 0 = 0$. Therefore $\forall y \varepsilon S \quad y + 0 = 0$.

case 1.2 $\forall x \varepsilon S\setminus\{0\} \quad x + 0 \neq 0$. Claim that $0 + 0 = 0$. To prove this, let $z = 0 + 0$. Then $0 = 0.z = 0.(0 + 0) = 0 + 0$. So we have the claim. Let $x \in S \setminus \{0\}$. Let $y = x + 0$ so $y \neq 0$. Then $y + 0 = (x + 0) + 0 = x + (0 + 0) = x + 0 = y$. Hence $\exists\, y \in S\setminus\{0\}$ such that $y + 0 = y$. Let z be an arbitrory element in S. Then $zy^{-1}(y + 0) = zy^{-1}y$ so $z + 0 = z$. Therefore $\forall\, z \in S \quad z + 0 = z$.

2. Note that either $\exists\, x \in S \setminus \{0\}$ such that $0 + x = 0$ or $\forall\, x \in S\setminus\{0\} \quad 0 + x \neq 0$.

case 2.1 $\exists\, x \in S \setminus\{0\}$ such that $a + x = 0$. Similar to case 1.1, we can prove that $\forall\, y \in S \quad 0 + y = 0$.

case 2.2 $\forall\, x \in S\setminus\{0\} \quad 0 + x \neq 0$. Similar to case 1.2, we can prove $\forall\, z \in S \quad 0 + z = z$.

i) If case 1.1 and case 2.1 occur then we have that $x + 0 = 0 = 0 + x \quad \forall\, x \in S$.

ii) If case 1.2 and case 2.2 occur then we have that $x + 0 = x = 0 + x \quad \forall\, x \in S$.

iii) If case 1.1 and case 2.2 occur then we shall prove that $x + y = y \quad \forall\, x,y \in S$. Let $x,y \in S$ then $x + y = (0 + x) + (0 + y) = 0 + (x + 0) + y = 0 + 0 + y = 0 + y = y$.

iv) If case 1.2 and case 2.1 occur then we shall prove that $x + y = x \quad \forall\, x,y \in S$. Let $x,y \in S$ then $x + y = (x + 0) + (y + 0) = x + (0 + y) + 0 = x + 0 + 0 = x + 0 = x$. #

We shall call a semifield satisfying case i an ∞-semifield, a semifield satisfying case ii a 0-semifield, a semifield satisfying case iii a right zero semifield, a semifield satisfying case iv a left zero semifield.

Lemma 3.7.5 Let S be a semigroup. Suppose that there exists an element $1 \varepsilon S$ such that $x.1 = x$ for all $x \varepsilon S$ and for all $x \varepsilon S$ there exists an element $x^{-1} \varepsilon S$ such that $x.x^{-1} = 1$. Then $1.x = x$ for all $x \varepsilon S$ and $x^{-1}x = 1$ for all $x \varepsilon S$, so S is a group.

Proof. Claim that if $y^2 = y$ then $y = 1$. To prove this, let $y^2 = y$ so $y = y^2y^{-1} = 1$. Let $x \varepsilon S$ then $(x^{-1}x)^2 = x^{-1}xx^{-1}x = x^{-1}.1.x = x^{-1}x$. By the claim $x^{-1}x = 1$. We have that $1.x = (xx^{-1}).x = x(x^{-1}x) = x.1 = x$. #

Theorem 3.7.6 Let S be a 0-semifield. If there exists an element x in $S\setminus\{0\}$ such that x has a right additive inverse then every element of S has an additive inverse.

Proof. Let $x \varepsilon S\setminus\{0\}$ be such that x has a right additive inverse. Then $\exists y \varepsilon S$ such that $x + y = 0$. Let z be an arbitrary element in S. Then $z + zx^{-1}y = zx^{-1}(x + y) = zx^{-1}.0 = 0$ therefore z has a right additive inverse. Hence $\forall z \varepsilon S$ z has a right additive inverse. By above Lemma, $\forall z \varepsilon S$ z has an additive inverse. #

By the above theorem we have that if S is a 0-semifield then either every element has an additive inverse in which case S is a skew field or no nonzero element of S has a right (left) additive inverse.

Remarks: 1) For each skew field $(F,+,\cdot)$, Δ is the only congruence on F.

2) Let S be a 0-semifield which is not a skew field. Then for

each $x,y \in S\setminus\{0\}$ $x + y \neq 0$ and $x.y \neq 0$. Therefore $(S\setminus\{0\},+,\cdot)$ is a P.R.D.

3) Let $(S,+,\cdot)$ be a left (right) zero semifield. We can show that

i) If ρ is a congruence on $(S,+,\cdot)$ then $\rho\setminus\{(0,0)\}$ is a congruence on the group $(S\setminus\{0\},\cdot)$.

ii) If ρ is a congruence on the group $(S\setminus\{0\},\cdot)$ then $\rho \cup \{(0,0)\}$ is a congruence on $(S,+,\cdot)$.

<u>Definition 3.7.7</u> Let S be a semifield and 0 multiplicative zero of S. A <u>C - set</u> E of S ($E \triangleleft S$) is a multiplicative subgroup of $(S\setminus\{0\},\cdot)$ such that

i) for each $x \in E$, $a \in S\setminus\{0\}$ $\quad a^{-1}.x.a \in E$,

ii) for each $x \in E$, $z \in S$ $[z + x = 0 \quad \text{iff} \quad z + 1 = 0]$,

iii) for each $x \in E$, $z \in S$ $[x + z = 0 \quad \text{iff} \quad 1 + z = 0]$,

iv) for each $x \in E$, $z \in S$ $[z + 1 \neq 0$ and $1 + z \neq 0$ implies that $(z + 1)^{-1}.(z + x)$, $(1 + z)^{-1}.(x + z) \in E]$.

<u>Remarks</u>: 1) A semifield S is not a C - set of S.

2) For each skew field F, {1} is the only C - set of F.

3) If S is a 0-semifield which is not a skew field then E is a C - set of S iff E is a C - set of the P.R.D. $(S\setminus\{0\},+,\cdot)$.

4) If S is a left (right) zero semifield then E is a C - set of S iff E is a normal subgroup of the group $(S\setminus\{0\},\cdot)$.

Examples 1) Let ρ be a congruence on a semifield $(S,+,\cdot)$. Let $[1]_\rho = \{a \varepsilon S | a \rho 1\}$. We shall show that $[1]_\rho \lhd S$. Clearly $[1]_\rho$ is a multiplicative subgroup of $(S\setminus\{0\},\cdot)$ and $\forall a \varepsilon S\setminus\{0\}$, $x \varepsilon [1]_\rho$ $a^{-1}.x.a \varepsilon [1]_\rho$. Let $x \varepsilon [1]_\rho$ and $z \varepsilon S$. Assume that $z + x = 0$. Since $(z + x)\rho(z + 1), z + 1 = 0$. Assume that $z + 1 = 0$. Since $(z + x)\rho(z + 1)$, $z + x = 0$. Similarly we can prove that $\forall x \varepsilon [1]_\rho$, $z \varepsilon S$ $[x + z = 0 \text{ iff } 1 + z = 0]$. Let $x \varepsilon [1]_\rho$ and $z \varepsilon S$. Assume that $z + 1 \neq 0$ and $1 + z \neq 0$. Since $(z + x)\rho(z + 1)$ and $(x + z)\rho(1 + z)$, $(z + 1)^{-1}.(z + x)$ and $(1 + z)^{-1}. (x + z) \varepsilon [1]_\rho$. Therefore $[1]_\rho \lhd S$.

2) Let E be a C - set of a semifield $(S,+,\cdot)$. Let $\rho = \{(a,b) \varepsilon S \setminus\{0\} \times S\setminus\{0\} | a^{-1}.b \varepsilon E\} \cup \{(0,0)\}$. We shall show that ρ is a congruence on S. Clearly ρ is an equivalence relation on S. If S is not an ∞-semifield then we are done. We may assume that S is an ∞-semifield. Let $(a,b) \varepsilon \rho\setminus\{(0,0)\}$, and $c \varepsilon S$. If $c = 0$ then clearly $(ac,bc),(ca,cb),(a + c,b + c),(c + a,c + b) \varepsilon \rho$ so we are done. Hence we may assume that $c \neq 0$. Clearly (ac,bc), $(ca,cb) \varepsilon \rho$. Let $d = ab^{-1}$, $e = cb^{-1}$. If $d + e = 0$ then $ab^{-1} + cb^{-1} = 0$ and $a + c = 0$. Because $ab^{-1} \varepsilon E$ and $E \lhd S$, $1 + cb^{-1} = 0$ so $b + c = 0$. Hence $(a + c,b + c) \varepsilon \rho$. If $e + d = 0$ then we can show that $(c + a,c + b) \varepsilon \rho$. Hence we may assume that $d + e \neq 0$ and $e + d \neq 0$. So $(b + c)^{-1}.(a + c) = (1 + e)^{-1}.b.b^{-1}(d + e) = (e + e)^{-1}.(d + e) \varepsilon E$. Similarly we can prove that $(e + 1)^{-1}.(e + d) \varepsilon E$. Therefore $(a + c,b + c)$, $(c + d,c + b) \varepsilon \rho$ Thus ρ is a congruence on S.

Definition 3.7.8 A quotient semifield of a semifield S is a pair (K,ϕ) where K is a semifield and $\phi:S \to K$ is an onto semifield homomorphism.

Examples 1) $(S/\rho,\pi)$ is a quotient semifield of a semifield S where ρ is a congruence on S.

2) Let E be a C - set of a semifield S. Let $\rho = \{(a,b) \varepsilon S\setminus\{0\} \times S\setminus\{0\} | a^{-1}.b \varepsilon E\} \cup \{(0,0)\}$ and $S/E = S/\rho$. Then $(S/E,\pi)$ is a quotient semifield of S.

Theorem 3.7.9 Let (K,ϕ) be a quotient semifield of a semifield S and $\rho = \{(a,b) \varepsilon S \times S \mid \phi(a) = \phi(b)\}$. Then ϕ is a congruence on S and there exists an automorphism $\phi:S/\rho \to K$ such that the following diagram is commutative

$$\begin{tikzcd}
 & S \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\
S/\rho \arrow[rr, "\psi"'] & & K
\end{tikzcd}$$

Proof. It is similar to the proof of Theorem 3.5.5.

Definition 3.7.10 Let S,S' be semifields and $\phi:S \to S'$ a homomorphism. Then kernel of ϕ , denoted by ker ϕ, = $\{d \varepsilon S | \phi(d) = 1\}$.

Theorem 3.7.11 Let $\phi:S \to S'$ be an onto semifield homomorphism. Then ker $\phi \triangleleft S$ and there exists a natural isomorphism $\psi:S/\ker\phi \to S'$ such that the following diagram is commutative .

$$\begin{tikzcd}
 & S \arrow[ld, "\pi"'] \arrow[rd, "\phi"] & \\
S/\ker \phi \arrow[rr, "\psi"] & & S'
\end{tikzcd}$$

หอสมุดกลาง สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Proof. First we shall show that $\ker \phi \lhd S$. Because $\phi(0) = 0 \neq 1$, $0 \notin \ker \phi$. Clearly $\ker \phi$ is a multiplicative subgroup of $(S \setminus \{0\}, \cdot)$ and $\forall\, x \, \epsilon \ker \phi,\ a \, \epsilon \, S \setminus \{0\}\quad a^{-1}.x.a \, \epsilon \ker \phi$. Let $x \, \epsilon \ker \phi$ and $z \, \epsilon \, S$. Then $\phi(x) = 1$. Assume that $z + x = 0$ so $\phi(z + 1) = \phi(z) + \phi(1) = \phi(z) + \phi(x) = \phi(z + x) = 0$ therefore $z + 1 = 0$. Assume that $z + 1 = 0$ so $\phi(z + x) = \phi(z) + \phi(x) = \phi(z) + \phi(1) = \phi(z + 1)$ therefore $z + x = 0$. Similarly we can prove that $\forall\, x \, \epsilon \text{ Ker } \phi,\ z \, \epsilon \, S\ [x + z = 0 \text{ iff } z + z = 0]$. Let $x \, \epsilon \ker \phi$ and $z \, \epsilon \, S$. Assume $z + 1 \neq 0$ and $1 + z \neq 0$. Then $\phi((1 + z)^{-1}.(x + z)) = (\phi(1) + \phi(z))^{-1}.(\phi(x) + \phi(z)) = (1 + \phi(z))^{-1}.(1 + \phi(z)) = 1$ hence $(1 + z)^{-1}.(x + z) \, \epsilon \ker \phi$. Similarly we can prove that $(z + 1)^{-1}.(z + x) \, \epsilon \ker \phi$. Hence $\ker \phi \lhd S$.

Define $\psi: S/\ker \phi \to S'$ as follows: given $\alpha \, \epsilon \, S/\ker \phi$ choose $a \, \epsilon \, \alpha$ and then let $\psi(\alpha) = \phi(a)$. Then clearly ψ is an isomorphism such that $\psi o \pi = \phi$. #

We shall call the above theorem the first isomorphism Theorem of semifield Theory.

Definition 3.7.12 Let (K,ϕ) and (K',ϕ') be quotient semifields of a semifield S. Say that (K,ϕ) is strongly equivalent to (K',ϕ') iff there exists an isomorphism $\psi : K \to K'$ such that the following diagram is commutative .

$$\begin{tikzcd} & S \arrow[dl, "\phi"'] \arrow[dr, "\phi'"] & \\ K \arrow[rr, "\psi"'] & & K' \end{tikzcd}$$

Write this as $(K,\phi) \simeq (K',\phi')$.

<u>Remarks</u>: 1) $\simeq$ is an equivalence relation on the set of quotient semifields of a semifield.

2) For each quotient semifield (K,ϕ) of a semifield S, $(K,\phi) \simeq (S/\rho,\pi)$ where $\rho = \{(a,b) \in S \times S \mid \phi(a) = \phi(b)\}$.

3) For each quotient semifield (K,ϕ) of a semifield S. $(K,\phi) \simeq (S/\ker \phi,\pi)$.

<u>Proposition 3.7.13</u> Let S,S' be semifields and $\phi : S \to S'$ an onto semifield homomorphism. If ρ is a congruence on S then $(\phi \times \phi)(\rho)$ is a congruence on S'. If $E \triangleleft S$ then $\phi(E) \triangleleft S'$.

<u>Proof</u>. It is similar to the proof of Proposition 3.5.10.

<u>Proposition 3.7.14</u> Let $\phi : S \to S'$ be a semifield homomorphism. If ρ' is a congruence on S' then $(\phi \times \phi)^{-1}(\rho')$ is a congruence on S. If $E' \triangleleft S'$ then $\phi^{-1}(E') \triangleleft S$.

<u>Proof</u> . It is standard.

Fix a semifield S, let E(S) = the set of C - sets of S,

C(S) = the set of congruences on S,

Q(S) = the set of equivalence
classes of quotient semifields
of S under $\simeq$.

We shall define natural relations $\subseteq$ on E(S), C(S), Q(S) as $\subseteq$ on N(G), C(G), Q(G) in Section 2.3, respectively. Then the proof that $(E(S),\subseteq)$, $(C(S),\subseteq)$, $(Q(S),\subseteq)$ are posets is similar to the proof that $(N(G),\subseteq)$, $(C(G),\subseteq)$, $(Q(G),\subseteq)$ are posets, respectively.

Theorem 3.7.15 For each semifield S, the posets E(S), C(S), Q(S) are isomorphic.

Proof. It is similar to the proofs of Theorem 3.5.11 and the isomorphisms have the same form as in Theorem 3.5.11.

Proposition 3.7.16 Let S be a semifield and E_1, E_2 C - sets of S. Then $E_1.E_2 = \{a_1.a_2 \mid a_1 \varepsilon E_1, a_2 \varepsilon E_2\}$ is the C - set of S generated by $E_1 \cup E_2$.

Proof. First we shall show that $E_1.E_2$ is a C - set of S. Note that $\forall x,y \ \varepsilon\ S[x.y = 0$ implies that $x = 0$ or $y = 0]$. Because $0 \notin E_1$ and $0 \notin E_2$, $0 \notin E_1.E_2$. Let $a,b \ \varepsilon\ E_1.E_2$ then $a = a_1.a_2$, $b = b_1.b_2$ for some $a_1,b_1 \varepsilon\ E_1$, $a_2,b_2 \varepsilon\ E_2$. So $a^{-1}.b = (a_1.a_2)^{-1}.(b_1.b_2) =$ $a_2^{-1}.(a_1^{-1}.b_1).b_2 = (a_2^{-1}.(a_1^{-1}.b_1).a_2).(a_2^{-1}b_2) \ \varepsilon\ E_1.E_2$. Hence $E_1.E_2$ is a multiplicative subgroup of $(S\setminus\{0\},\cdot)$. Clearly $\forall$ a ε $S\setminus\{0\}$, $x \ \varepsilon\ E_1.E_2$

$a^{-1}.x.a \in E_1.E_2$. Let $a \in E_1.E_2$ and $z \in S$. Then $a = a_1.a_2$ for some $a_1 \in E_1, a_2 \in E_2$. Assume that $z + a = 0$ then $a_1^{-1}z + a_2 = 0$ (since $a_1 \neq 0$). Because $E_2 \triangleleft S$ and $a_1^{-1}z + a_2 = 0$, $z + a_1, = a_1(a_1^{-1}z + 1) = a_1.0 = 0$. Since $E_1 \triangleleft S$ and $z + a_1 = 0$, $z + 1 = 0$. Assume that $z + 1 = 0$ then $z + a_1 = 0$. Therefore $a_1^{-1}z + 1 = 0$ then $a_1^{-1}z + a_2 = 0$. So $z + a = a_1(a_1^{-1}z + a_2) = 0$. Similarly we can prove that $\forall x \in E_1.E_2$, $z \in S[x + z = 0$ iff $1 + z = 0]$. Let $a \in E$ and $z \in S$. Then $a = a_1.a_2$ for some $a_1 \in E_1$, $a_2 \in E_2$. Assume that $z + 1 \neq 0$ and $1 + z \neq 0$. Then $a_1(a_1^{-1}.z + a_2) = z + a \neq 0$ and $a_1(a_2 + a_1^{-1}.z) = a + z \neq 0$ so $a_1^{-1}z + a_2 \neq 0$ and $a_2 + a_1^{-1}z \neq 0$. Because $E_2 \triangleleft S$, $(1 + a_1^{-1}z)^{-1}.(a_2 + a_1^{-1}z) \in E_2$. Since $(a_1^{-1} + a_1^{-1}z)^{-1}.(1 + a_1^{-1}z) = (1 + z)^{-1}.(a_1 + z)$ and $E_1 \triangleleft S$, $(a_1^{-1} + a_1^{-1}z)^{-1}.(1 + a_1^{-1}z) \in E_1$. So $(1 + z)^{-1}.(a_1a_2 + z) = (a_1(a_1^{-1} + a_1^{-1}z))^{-1}$ $(a_1(a_2 + a_1^{-1}z)) = (a_1^{-1} + a_1^{-1}z)^{-1}.(a_2 + a_1^{-1}z) = (a_1^{-1} + a_1^{-1}z)^{-1}(1 + a_1^{-1}z)$. $(1 + a_1^{-1}z)^{-1}(a_2 + a_1^{-1}z) \in E_1.E_2$. Hence $(1 + z)^{-1}.(a + z) \in E_1.E_2$. Similarly we can show that $(z + 1)^{-1}.(z + a) \in E_1.E_2$. Therefore $E_1.E_2 \triangleleft S$. Clearly $E_1 \in E_1.E_2$ and $E_2 \in E_1.E_2$. Let E be a C - set containing E_1 and E_2. Since E is a multiplicative subgroup of $(S\setminus\{0\},\cdot)$, $E_1.E_2 \subsetneq E$. Hence $E_1.E_2$ is the C - set of S generated by $E_1 \cup E_2$. #

Proposition 3.7.17 Let S be a semifield and ρ_1,ρ_2 congruences on S. Then $\rho_1.\rho_2 = \{(a_1.a_2,\ b_1.b_2) \mid (a_1,b_1) \in \rho_1,\ (a_2,b_2) \in \rho_2\}$ is the congruence on S generated by $\rho_1 \cup \rho_2$.

Proof. It is similar to the proof of Proposition 3.5.13.

Remark: Fix a semifield S, let $E_1, E_2 \in E(S)$. Then $E_1 \cap E_2 =$ g.l.b.$\{E_1, E_2\}$ and $E_1 . E_2 =$ l.u.b. $\{E_1, E_2\}$ therefore E(S) is a lattice. Let $\rho_1, \rho_2 \in C(S)$. Then $\rho_1 \cap \rho_2 =$ g.l.b. $\{\rho_1, \rho_2\}$ and $\rho_1 . \rho_2 =$ l.u.b. $\{\rho_1, \rho_2\}$. Therefore C(S) is a lattice. Hence Q(S) is a lattice also.

Now we define covariant functors E, C, Q from $\mathcal{S}_f$ to $\mathcal{L}$ as we definedthe covariant functors N, C, Q from $\mathcal{G}$ to $\mathcal{L}$ in Section 2.3, respectively. Then the proof that E, C, Q are naturally equivalent covariant functors is similar to the proof that N , C, Q are naturally equivalent.

Remarks: As a result, we have that C is the congruence functor of $\mathcal{S}_f$, $\mathcal{S}_f$ has a congruence set and C - sets of a semifield are congruence sets with respect to E.

Now we define covariant functor E', C', Q', from $\mathcal{S}_{f,o}$ to $\mathcal{L}$ as we definedthe covariant functors N', C', Q' from $\mathcal{G}_o$ to $\mathcal{L}$ in Section 2.3, respectively. Then the proof that E', C', Q' are naturally equivalent covariant functors is similar to the proof that N', C', Q' are naturally equivalent covariant functors.

Next we shall define naturally equivalent covariant functors from $\mathcal{S}_{f,i}$ to $\mathcal{Q}$ by using equivalence classes of congruences, equivalence classes of C - sets and equivalence classes of quotient semifields which are defined below.

Definition 3.7.18 Let S be a semifield and E_1, E_2 C - sets in S. Say that E_1 is equivalent to E_2 ($E_1 \sim E_2$) iff there exists a semifield automorphism $\phi : S \to S$ such that $\phi(E_1) = E_2$.

Remark: $\sim$ is an equivalence relation on the set of C - sets of a semifield.

Definition 3.7.19 Let ρ_1, ρ_2 be congruences on a semifield S. Say that ρ_1 is equivalent to ρ_2 ($\rho_1 \sim \rho_2$) iff there exists a semifield automorphism $\phi : S \to S$ such that $(\phi \times \phi)(\rho_1) = \rho_2$.

Remark: $\sim$ is an equivalence relation on the set of congruences on a semifield.

Definition 3.7.20 Let (K,ϕ), (K',ϕ') be quotient semifields of a semifield. Say that (K,ϕ) is weakly equivalent to (K',ϕ') iff there exist semifield isomorphisms $f : S \to S$ and $F : K \to K'$ such that the following diagram is commutative

$$\begin{tikzcd}
S \arrow[r, "f"] \arrow[d, "\phi"'] & S \arrow[d, "\phi'"] \\
K \arrow[r, "F"] & K'
\end{tikzcd}$$

Write this as $(K,\phi) \sim (K',\phi')$.

Remarks: 1) $\sim$ is an equivalence relation on the set of quotient semifields of a semifield.

2) $(K,\phi) \simeq (K',\phi')$ implies that $(K,\phi) \sim (K',\phi')$.

Fix a semifield S, let $E^*(S)$ = the set of equivalence classes of C - sets in S under $\sim$,

$C^*(S)$ = the set of equivalence classes of congruences on S under $\sim$,

$Q^*(S)$ = the set of equivalence classes of quotient semifields of S under $\sim$,

We define binary relations $\leqslant$ on $E^*(S)$, $C^*(S)$ $Q^*(S)$ as $\leqslant$ on $N^*(G)$, $C^*(G)$, $Q^*(G)$ in Section 1.3, respectively. Then the proof that $(E^*(S),\leqslant)$ $(C^*(S),\leqslant)$ $(Q^*(S),\leqslant)$ are quasi-ordered sets is similar to $(N^*(G),\leqslant)$, $(C^*(G),\leqslant)$ $(Q^*(G),\leqslant)$ are quasi-ordered sets, respectively.

Theorem 3.7.21 For each semifield S the quasi-ordered sets $E^*(S)$, $C^*(S)$, $Q^*(S)$ are isomorphic.

Proof. It is similar to the proofs of Theorem 3.5.17 and the isomorphisms have the same form as the isomorphisms of Theorem 3.5.17.

Now we define covariant functors E^*, C^*, Q^* from $\mathscr{S}_{f,i}$ to $\mathscr{Q}$ as define the covariant functors N^*, C^*, Q^* from $\mathscr{G}_i$ to $\mathscr{Q}$ in Section 2.3, respectively. Then the proof that E^*, C^*, Q^* are naturally equivalent covariant functors is similar to the proof that N^*, C^*, Q^* are naturally equivalent.

Remark: We can prove that the following subcategories of $\mathscr{S}_f$ have a congruence set as we proved that $\mathscr{S}_f$ has a congruence set :

1) the category of additively commutative semifields and semifield homomorphisms,

2) the category of multiplicatively commutative semifields homomorphisms,

3) the category of commutative semifields and semifield homomorphisms.

Lastly we shall consider some theorems which use C - sets of semifields (congruence sets).

Definition 3.7.22 A subsemifield of a semifield S is a subset of S which is a semifield.

Definition 3.7.23 Let E be a C - set of a semifield S. Then E is said to be a maximal C - set of S iff E is a C - set of S such that $E \subsetneq E'$ implies that $E = E'$.

Definition 3.7.24 Let A be a subsemifield of a semifield S and $A \neq S$. Then A is said to be a maximal subsemifield of S iff A' is a subsemifield of S such that $A \subset A'$ implies that $S = A'$.

Theorem 3.7.25 Let E be a C - set of a semifield S. Then there exists a bijection between the set of C - sets of S containing E and the set of C - sets of S/E and this bijection take maximal C - sets to maximal C - sets.

Proof. It is similar to the proof of Theorem 3.5.23 .

Remark: We can prove that for each C - set E of a semifield S there exists a bijection between the set of subsemifields of S containing E and the set of subsemifields of S/E and this bijection take maximal subsemifields to maximal subsemifields as we proved in Theorem 3.7.25.

Definition 3.7.26 Let S be a semifield. Then S is said to be simple iff S has only one C - set $\{1\}$.

Examples 1) Let G be a simple group. Define binary operations + and $\cdot$ on $G \cup \{0\}$ by $a.0 = 0 = 0.a$ and $a + b = 0$ for all $a,b \ \varepsilon\ G \cup \{0\}$. Then $(G \cup \{0\},+,\cdot)$ is a simple semifield .

2) $\mathbb{Q}_0^+$, $\mathbb{Q}_\infty^+$, $\mathbb{R}_0^+$ and $\mathbb{R}_\infty^+$ are simple semifields.

3) A skew field is simple.

Remark: If E is a maximal C - set of a semifield S then S/E is simple.

Proposition 3.7.27 Let $(S,+,\cdot)$ be a null semifield such that $(S\setminus\{0\},\cdot)$ is not a simple group. Then there exists a nontrivial congruence on S.

Proof. Let N be a nontrivial normal subgroup of $(S\setminus\{0\},\cdot)$. Define $\rho = \{(a,b) \ \varepsilon\ S\setminus\{0\} \times S\setminus\{0\} \mid a^{-1}.b \ \varepsilon\ N\} \cup \{(0,0)\}$. We shall show that ρ is a congruence on S. Clearly ρ is an equivalence relation on S. Let $(a,b) \ \varepsilon\ \rho$ and $c \ \varepsilon\ S$. Because S is a null semifield, $(a + c,b + c) = (0,0) \ \varepsilon\ \rho$ and $(c + a,c + b) = (0,0) \ \varepsilon\ \rho$. If a,b or $c = 0$ then clearly $(a.c,b.c),(c.a,c.b) \ \varepsilon\ \rho$. so we are done. Hence we may assume that $a,b,c \neq 0$. Because $a^{-1}.b \in N$, $(c.s)^{-1}.(c.b) \in N$ and $(a.c)^{-1}.(b.c) \in N$ so $(c.a,c.b)$, $(a.c,b.c) \in \rho$. Hence ρ is a congruence on S. Because $\exists\, n \in N$ such that $n \neq 1$, $(n,1) \in \rho$. Hence ρ is a nontrivial congruence on S. #

Proposition 3.7.28 Let $(S,+,\cdot)$ be an almost null semifield. Then there exists only one congruence Δ on S.

Proof. Let ρ be a congruence on S. We must show that $\rho = \Delta$. Suppose not, so $\exists\,(a,b) \in \rho$ such that $a \neq b$. Then $(a + a)\rho(a + b)$. Therefore $a \rho 0$ which is a contradiction. Thus $\rho = \Delta$. #

Corollary 3.7.29 If S is an almost null semifield then S is simple.

Wedderburn's Theorem says that if F is a finite skew field then F is a field. For a proof see in [3]. In this thesis we shall generalize Wedderburn's Theorem.

Theorem 3.7.30 If S is a finite 0-semifield such that + is commutative then $\cdot$ is commutative ie. S is a commutative semifield.

Proof. Let S be a finite 0-semifield such that + is commutative.

case 1 S is a skew field then by Wedderburn's Theorem, S is a field so $\cdot$ is commutative

case 2 S is not a skew field. Then $(S\setminus\{0\},+,\cdot)$ is a P.R.D. Therefore $S\setminus\{0\}$ is a finite P.R.D. By Theorem 3.5.31, $S\setminus\{0\} \cong D_1 \times D_2$ where $x + y = x\ \forall x, y \in D_1$ and $x + y = y\ \forall x,y \in D_2$. Let $x,y \in D_1$.

Then $x + y = x$. Since + is commutative, $y + x = x + y$ so $y = y + x = x + y = x$. Therefore $D_1 = \{1\}$. Similarly we can show that $D_2 = \{1\}$ Therefore $S \setminus \{0\} \cong \{(1,1)\}$. So $S = \{0,1\}$. Because $0.1 = 1.0 = 0 = 0.0$ and $1.1 = 1$, S is a commutative semifield. #

Remark : Let S be a left (right) zero semifield. Suppose + is commutative. We have that $1 = 1 + 0 = 0 + 1 = 0$ which is a contradiction. Hence + is not commutative.

3.8 Semifield-modules.

In this section we shall work with left congruences on a semifield. But everything that we prove for left congruences can be similarly proved for right congruences also. As in section 3.7, we shall consider the categories $\mathcal{S}_f$, $\mathcal{S}_{f,o}$, $\mathcal{S}_{f,i}$

We shall define naturally equivalent contravariant functors from $\mathcal{S}_f$ to $\mathcal{P}$, naturally equivalent covariant functors from $\mathcal{S}_{f,o}$ to $\mathcal{P}$ and naturally equivalent covariant functors from $\mathcal{S}_{f,i}$ to $\mathcal{Q}$ by using

1) double left congruences, double left C - sets and quotient double left semigroup spaces,

2) multiplicative left congruences, multplicative left C - sets and quotient left semimodules,

3) additive left congruences, additive left C - sets and quotient left semifield modules.

Definition 3.8.1 Let S be a semifield. A double left congruence on S is an equivalence relation ρ on S such that for each $a,x,y \in S$

i) $x \rho 0$ iff $x = 0$,

ii) $x \rho y$ implies that $(a + x)\rho(a + y)$ and $(a.c)\rho(a.y)$.

Definition 3.8.2 Let S be a semifield. A multiplicative left congruence on S is an equivalence relation ρ on S such that for each $a,x,y \in S$.

i) $x \rho 0$ iff $x = 0$,

ii) $x \rho y$ implies that $(a + x)\rho(a + y)$, $(x + a)\rho(y + a)$ and $(a.x)\rho(a.y)$.

Definition 3.8.3 Let S be a semifield. An additive left congruence on S is an equivalence relation ρ on S such that for each $a,x,y \in S$

i) $x \rho 0$ iff $x = 0$,

ii) $x \rho y$ implies that $(a + x)\rho(a + y)$, $(a.x)\rho(a.y)$ and $(x.a)\rho(y.a)$.

Definition 3.8.4 A double left C - set of a semifield S is a multiplicative subgroup E of $(S\setminus\{0\},\cdot)$ such that

i) for each $x \in E$, $z \in S$ $[z + x = 0$ iff $z + 1 = 0]$,

ii) for each $x \in E$, $z \in S$ $[z + 1 \neq 0$ implies that $(z + 1)^{-1}.(a + x) \in E]$.

Definition 3.8.4 A *multiplicative left C - set* of a semifield S is a multiplicative subgroup E of $(S\setminus\{0\},\cdot)$ such that

i) for each $x \in E$, $z \in S$ $[z + x = 0$ iff $z + 1 = 0]$.

ii) for each $x \in E$, $z \in S$ $[x + z = 0$ iff $1 + z = 0]$,

iii) for each $x \in E$, $z \in S$ $[z + 1 \neq 0$ and $1 + z \neq 0$ implies that $(z + 1)^{-1}.(z + x)$, $(1 + z)^{-1}.(x + z) \in E]$

Definition 3.8.5 An *additive left C - set* of a semifield S is a multplicative subgroup E of $(S\setminus\{0\},\cdot)$ such that

i) for each $x \in E$, $z \in S\setminus\{0\}$ $z^{-1}.x.z \in E$,

ii) for each $x \in E$, $z \in S$ $[z + x = 0$ iff $z + 1 = 0]$,

iii) for each $x \in E$, $z \in S$ $[z + 1 \neq 0$ implies that $(z + 1)^{-1}.(z + x) \in E]$.

Definition 3.8.6 Let S be a semifield. A *double left S-space* is a triple $(M,+,\cdot)$ where $(M,+)$ and $(M,\cdot)$ are left S-spaces such that $r\cdot(s + m) = r.s + r.m$, $1.m = m$ for all $r,s \in S$, $m \in M$, and there exists an element m^* in M such that $r.m^* = m^*$ for all $r \in S$, then we shall call m^* the *zero element* of M.

Definition 3.8.7 Let S be a semifield. A *left S-semimodule* is a triple $(M,+,\cdot)$ where $(M,+)$ is a semigroup and $(M,\cdot)$ is a left S-space such that $(a + a').m = a.m + a'.m$, $a.(m + n) = a.m + a.n$ $1.m = m$ for all $a,a' \in S$, $m,n \in M$ and there exists an element m^* in M such that

$a.m^* = m^*$ for all $a \varepsilon S$ then we shall call m^* the zero element of M.

Definition 3.8.8 Let S be a semifield. A left S-module is a triple $(M,+,\cdot)$ where $(M,+)$ is a left S-space and $(M,\cdot)$ is a group with zero.

Remark: For each semifield S, S is a double left S-space, a left S-semimodule and a left S-module.

Now we shall work with double left congruences. But everything that we define and prove for double left congruences can be similarly defined and proved for multiplicative left congruences and additive left congruences.

Definition 3.8.9 Let S be a semifield and M,M' double left S-spaces. Then a map $\phi:M \rightarrow M'$ is said to be double left S-equivariant iff $\phi(r + m) = r + \phi(m),\phi(r.m) = r.\phi(m)$ for all $r \varepsilon S$, $m \varepsilon M$ and $\phi(a) = 0'$ iff $a = 0$ for all $a \varepsilon M$ where $0,0'$ are the zero elements of M,M' respectively.

Remarks: 1) If $\phi:M \rightarrow M'$ is a bijective double left S-equivalent map then ϕ^{-1} is also double left S-equivariant. We shall call such a map a double left S-space isomorphism.

2) If ρ is a double left congruence on a semifield S then the set S/ρ of equivalence classes of S can made into a double left S-space in natural way and the natural projection map $\pi:S \rightarrow S/\rho$ is an onto double left S-equivariant map.

3) If ρ is a double left congruence on a semifield S than $[1]_\rho = \{a \in S | a \rho 1\}$ ia a double left C - set of S.

4) If E is a double left C - set of a semifields S then $\{(a,b) \in S\setminus\{0\} \times S\setminus\{0\} | a^{-1}.b \in E\} \cup \{(0,0)\}$ is a double left congruence on S.

Definition 3.8.10 Let S be a semifield. A quotient double left S-space is a pair (K, ϕ) where K is a double left S-space and $\phi: S \to K$ is an onto double left S-equivariant map.

Example $(S/\rho, \pi)$ is a quotient double left S-space where ρ is a double left congruence on S.

Theorem 3.8.11 Let S be a semifield and $\phi: S \to M$ an onto double left S-S-equivariant map. Let $\rho = \{(a,b) \in S \times S | \phi(a) = \phi(b)\}$. Then ρ is a double left congruence on S and there exists a double left S-space isomorphism ψ from S/ρ to M such that the following diagram is commutative.

$$\begin{tikzcd}
& S \arrow[dl, "\pi"'] \arrow[dr, "\phi"] & \\
S/\rho \arrow[rr, "\psi"] & & M
\end{tikzcd}$$

Proof. It is similar to the proof of Theorem 3.7.9.

Definition 3.8.12 Let (K,ϕ), (K',ϕ') be quotient double left S-space where S is a semifield. Say that (K,ϕ) is strongly equivalent of (K',ϕ') iff there exists a double left S-space isomorphism $\psi: K \to K'$ such that the following diagram is commutative.

$$\begin{tikzcd} & S \arrow[dl, "\phi"'] \arrow[dr, "\phi'"] & \\ K \arrow[rr, "\psi"'] & & K' \end{tikzcd}$$

Write this as $(K,\phi) \simeq (K',\phi')$.

Remarks: 1) $\simeq$ is an equivalence relation on the set of quotient double left S-space.

2) For each quotient double left S-space (K,ϕ), $(K,\phi) \simeq (S/\rho,\pi)$ where $\rho = \{(a,b) \varepsilon\ S \times S \,|\, \phi(a) = \phi(b)\}$.

Proposition 3.8.13 Let S, S' be semifields and $\phi: S \to S'$ an onto semifield homomorphism. If ρ is a double left congruence on S then $(\phi \times \phi)(\rho)$ is a double left congruence on S'. If E is a double left C - set of S then $\phi(E)$ is a double left C - set of S'.

Proposition 3.8.14 Let S, S' be semifields and $\phi: S \to S'$ a semifield homomorphism. If ρ' is a double left congruence on S' then $(\phi \times \phi)^{-1}(\rho')$ is a double left congruence on S'. If E is a double left C - set of S' then $\phi^{-1}(E')$ is a double left C - set of S.

Fix a semifield S, let $LE(S)$ = the set of double left C - sets of S,

$LC(S)$ = the set of double left congruences on S,

LQ(S) = the set of equivalence
classes of quotient double left
S-spaces under $\sim$.

We define natural relations $\subsetneq$ on LE(S), LC(S), LQ(S) as $\subsetneq$ on E(S), C(S), Q(S) in Section 1.3, respectively. Then the proof that (LE(S),$\subsetneq$), (LC(S),$\subsetneq$), (LQ(S),$\subsetneq$) are posets is similar to the proof that (E(S),$\subsetneq$), (C(S),$\subsetneq$) (Q(S),$\subsetneq$) are posets, respectively.

Theorem 3.8.15 For each semifield S, the posets LE(S), LG(S), LQ(S) are isomorphic.

Proof. It is similar to the proof of Theorem 3.7.15 and the isomorphisms are the same form as in Theorem 3.7.15.

We define contravariant functors LE, LC and LQ from $\mathcal{S}_f$ to $\mathcal{L}$ as we defined the contravariant functors E, C and Q from $\mathcal{S}_f$ to $\mathcal{L}$ in Section 3.7, respectively. Then the proof that LE, LC and LQ are naturally equivalent contravariant functors is similar to the proof that E, C and Q are naturally equivalent contravariant functors.

We define covariant functors LE$'$, LC$'$ and LQ$'$ from $\mathcal{S}_{f,o}$ to $\mathcal{P}$ as we defined the covariant functors E$'$, C$'$ and Q$'$ from $\mathcal{S}_{f,o}$ to $\mathcal{L}$ in Section 3.7, respectively. Then the proof that LE$'$, LC$'$ and LQ$'$ are naturally equivalent covariant functors is similar to the proof that E$'$, C$'$ and Q$'$ are naturally equivalent covariant functors.

Definition 3.8.16 Let S be a semifield and E_1,E_2 double left congruence sets in S. Say that E_1 is equivalent to $E_2(E_1 \sim E_2)$ iff there exists a semifield automorphism $\phi:S \to S$ such that $\phi(E_1) = E_2$.

Remark: $\sim$ is an equivalence relation on the set of double left C - sets of S.

Definition 3.8.17 Let ρ_1,ρ_2 be double left congruences on a semifield S. Say that ρ_1 is equivalent to ρ_2 $(\rho_1 \sim \rho_2)$ iff there exists a semifield automorphism $\phi:S \to S$ such that $(\phi \times \phi)(\rho_1) = \rho_2$.

Remark: $\sim$ is an equivalence relation on the set of double left congruences on S.

Definition 3.8.18 Let $(K,\phi),(K',\phi')$ be quotient double left S-spaces . Say that (K,ϕ) is weakly equivalent to (K',ϕ') iff there exist a semifield automorphism $f:S \to S$ and a double left S-space isomorphism $f':K \to K'$ such that the following diagram is commutative

$$\begin{tikzcd}
S \arrow[r, "f"] \arrow[d, "\phi"'] & S \arrow[d, "\phi'"] \\
K \arrow[r, "f'"] & K'
\end{tikzcd}$$

หอสมุดกลาง สถาบันวิทยบริการ
จุฬาลงกรณ์มหาวิทยาลัย

Write this as $(K,\phi) \sim (K',\phi')$.

Remarks: 1) $\sim$ is an equivalence relation on the set of quotient double left S-spaces.

2) $(K,\phi) \simeq (K',\phi')$ implies that $(K,\phi) \sim (K',\phi')$.

Fix a semifield S, let $LE^*(S)$ = the set of equivalence classes of double left C - sets of S,

$LC^*(S)$ = the set of equivalence classes of double left congruences on S,

$LQ^*(S)$ = the set of equivalence classes of quotient double left S-spaces under $\sim$.

We define binary relations $\leq$ on $LE^*(S)$, $LC^*(S)$, $LQ^*(S)$ as $\leq$ on $E^*(S)$, $C^*(S)$, $Q^*(S)$ in Section 3.7. respectively. Then the proof that $(LE^*(S),\leq)$, $(LC^*(S),<)$, $(LQ^*(S),\leq)$ are quasi-ordered sets is similar to $(E^*(S),<)$,$(C^*(S),\leq)$, $(Q^*(S),\leq)$ are quasi-ordered sets, respectively.

Theorem 3.8.19 For each semifield S, the quasi-ordered sets $LE^*(S)$, $LC^*(S)$, $LQ^*(S)$ are isomorphic.

Proof. It is similar to the proof of Theorem 3.7.21, and the isomorphisms have the same form as the isomorphisms of Theorem 3.7.21.

We define covariant functors LE^*, LC^* and LQ^* from $\mathcal{S}_{f,i}$ to $\mathcal{Q}$ as we defined the covariant functors E^*, C^* and Q^* from $\mathcal{S}_{f,i}$ to $\mathcal{Q}$ in Section 3.7, respectively. Then the proof that LE^*, LC^* and LQ^* are naturally equivalent covariant functors is similar to the proof that E^*, C^* and Q^* are naturally equivalent covariant functors.