CHAPTER II

POSITIVE RATIONAL DOMAINS

Definition 2.1. A nonempty set D is said to be a positive rational domain, abbreviated by P.R.D., if there are two binary operations, + (addition) and · (multiplication) defined on it such that :

(i) D is an abelian group with respect to multiplication;

(ii) D is a commutative semigroup with respect to addition;

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

We will denote the multiplicative identity of a P.R.D. by 1.

Example 2.2. $\mathbb{Q}^+$ and $\mathbb{R}^+$ with the usual addition and multiplication are infinite P.R.D.'s.

Example 2.3. Let $D = \{1\}$ and define $1 \cdot 1 = 1$, $1+1 = 1$. Then D is a P.R.D.

Example 2.5. (i) A field is not a P.R.D. since 0 has no inverse.

(ii) If D is a P.R.D., then $D \times D$ is also a P.R.D.

Theorem 2.5. There is no finite P.R.D. of order > 1.

Proof : Suppose that there exists D a finite P.R.D. of order $n > 1$. Since $(D, \cdot)$ is a finite abelian group, D is a finite direct product of finite cyclic groups. Thus $D = D_{n_1} \times D_{n_2} \times \ldots \times D_{n_h}$ for some cyclic groups $D_{n_1}, D_{n_2}, \ldots, D_{n_h}$ of orders $n_1, n_2, \ldots, n_h > 1$ respectively.

Let $x_1, x_2, \ldots, x_h$ be generators of $D_{n_1}, D_{n_2}, \ldots, D_{n_h}$ respectively.

Let $m \in \mathbb{N}$. We define $m1 = 1 + 1 + \ldots + 1$ (m times). Therefore $\{m1\}_{m \in \mathbb{N}} \subseteq D$. Since D is finite, $\exists m, s \in \mathbb{N}$ $m < s$ such that $s1 = m1$. Hence $(s-m)1 + m1 = m1$ and so we have that $\exists\, x, y \in D$ such that $y + x = x$. Therefore $x^{-1}y + 1 = 1$, so $\exists\, z \in D$ such that $z + 1 = 1$ ——————— (*)

(1) Claim that $\forall\, m,\ 1 \leqslant m \leqslant n_1 - 1,\ x_1^m + 1 \neq 1$.

To prove this claim we first prove that $\forall\, m,\ 1 \leqslant m \leqslant n_1 - 1$, if $x_1^m + 1 = 1$, then $x_1^{km} + 1 = 1\ \forall k \in \mathbb{N}$. We will prove this by using induction on $k \in \mathbb{N}$. Let $m \in \{1, 2, \ldots, n_1 - 1\}$ be such that $x_1^m + 1 = 1$. Let $k \in \mathbb{N}$. Assume that $x_1^{km} + 1 = 1$. Hence we have that $x_1^m(x_1^{km} + 1) = x_1^m$, and so $x_1^{(k+1)m} + x_1^m + 1 = x_1^m + 1$. Therefore $x_1^{(k+1)m} + 1 = 1$. By mathematical induction we conclude that $\forall\, m,\ 1 \leqslant m \leqslant n_1 - 1$, if $x_1^m + 1 = 1$, then $x_1^{km} + 1 = 1\ \ \forall k \in \mathbb{N}$. Next, we prove that $\forall\, m,\ 1 \leqslant m \leqslant n_1 - 1$ if $m | n_1$, then $x_1^m + 1 \neq 1$. Suppose that this is not true, then $\exists\, m_o$ $1 \leqslant m_o \leqslant n_1 - 1$ such that $m_o | n_1$ and $x_1^{m_o} + 1 = 1$. Hence $\exists\, k \in \mathbb{N} - \{1\}$ such that $n_1 = m_o k$. Since $k-1 \in \mathbb{N}$, $x_1^{(k-1)m_o} + 1 = 1$. Therefore $x_1^{m_o}(x_1^{(k-1)m_o} + 1) = x_1^{m_o}$ and so $1 + x_1^{m_o} = x_1^{m_o}$. Thus $x_1^{m_o} = 1$ which is a contradiction since $1 \leqslant m_o \leqslant n_1 - 1$. Hence we have that $\forall\, m, 1 \leqslant m \leqslant n_1 - 1$ if $m | n_1$, then $x_1^m + 1 \neq 1$.

Now, we will prove (1). If $n_1 = 2$, then we have that $x_1 + 1 \neq 1$ since $1 | 2$. Suppose that $n_1 > 2$. We will prove (1) by using induction on k $1 \leqslant k \leqslant n_1 - 1$. Again, $x_1 + 1 \neq 1$ since $1 | n_1$. Let $k \in \{2, 3, \ldots, n_1 - 1\}$. Assume that $\forall\, m \in \mathbb{N}, m < k$, $x_1^m + 1 \neq 1$. If $k | n_1$, then we have that $x_1^k + 1 \neq 1$. Suppose that $k \nmid n_1$ and $x_1^k + 1 = 1$. Hence $\exists\, m_o \in \mathbb{N}$ such that $m_o k < n_1 < (m_o + 1)k$. Since $n_1 < (m_o + 1)k < 2n_1$, $x_1^{(m_o + 1)k} = x_1^j$ for some j, $1 \leqslant j \leqslant n_1 - 1$.

<u>Case $j < k$.</u> Then $x_1^{(m_o + 1)k} + 1 = 1$ and so $x_1^j + 1 = 1$ which contradicts the induction hypothesis.

<u>Case $j = k$.</u> Then $(m_o + 1)k \equiv k \bmod (n_1)$. Hence $n_1 | m_o k$ which is a contradiction since $0 < m_o k < n_1$.

<u>Case $j > k$.</u> Then $j = ks + r$ for some $r, s \in \mathbb{N}$ $0 \leqslant r < k$ and $s \leqslant m_o$ since if $s > m_o$, then $m_o k < sk < n_1 < (m_o + 1)k$, a contradiction.

If $r = 0$ and $s = m_o$, then $(m_o + 1)k \equiv m_o k \bmod (n_1)$, so $k \equiv 0 \bmod (n_1)$ and therefore we have that $x_1^k = 1$, a contradiction since $2 \leqslant k \leqslant n_1 - 1$.

If $r = 0$ and $s < m_o$, then $(m_o + 1)k \equiv sk \bmod (n_1)$ and so $(m_o + 1 - s)k \equiv 0 \bmod (n_1)$. Since $x_1^{(m_o - s)k} + 1 = 1$, $x_1^{(m_o - s + 1)k} + x_1^k = x_1^k$. Hence $1 + x_1^k = x_1^k$ and so $1 = x_1^k$ which is a contradiction since $2 \leqslant k \leqslant n_1 - 1$.

If $0 < r < k$ and $s \leqslant m_o$, then $(m_o + 1)k \equiv ks + r \bmod (n_1)$. Hence $(m_o + 1 - s)k \equiv r \bmod (n_1)$. Since $x_1^{(m_o + 1 - s)k} + 1 = 1$, $x_1^r + 1 = 1$ which contradicts the induction hypothesis.

We thus see that all these three cases lead to contradictions. Hence we must have that $x_1^k + 1 \neq 1$. By mathematical induction we have (1).

(2) As in (1), we can prove that $\forall\, j \quad 1 \leqslant j \leqslant h$, $x_j^m + 1 \neq 1$ $\forall\, m$ $1 \leqslant m \leqslant n_j - 1$.

(3) Claim that $\forall\, z \in D - \{1\}$, $z + 1 \neq 1$.

If $(D, \cdot)$ is a cyclic group, then the proof of (1) gives us the claim. Suppose that $(D, \cdot)$ is not a cyclic group, then $h > 1$. Note that if $z = (x_1^{m_1}, x_2^{m_2}, \ldots, x_h^{m_h})$, then $z \in D - \{1\}$ iff $\exists\, i$, $1 \leqslant i \leqslant h$ such that $m_i \not\equiv 0 \bmod (n_i)$. We will prove this claim by induction on the number of the components of z which are not 1. By (2), we can see that if z has exactly one component which is not 1, then $z + 1 \neq 1$. Let $k \in \{2, 3, \ldots, h\}$.

Assume that $y + 1 \neq 1$ for all $y \in D - \{1\}$ having the property that the number of components of y which are not 1 is less than k. Suppose that $\exists\ z_o = (x_1^{m_1}, x_2^{m_2}, \ldots, x_h^{m_h}) \in D - \{1\}$ having k components which are not 1 and $z_o + 1 = 1$. We may assume that $0 \leq m_1 \leq n_1 - 1$, $0 \leq m_2 \leq n_2 - 1, \ldots,$ $0 \leq m_h \leq n_h - 1$. We may rearrage the indices if necessary so that $x_1^{m_1}, x_2^{m_2}, \ldots, x_k^{m_k}$ are those k components of z_o which are not 1. Hence $1 \leq m_1 \leq n_1 - 1$, $1 \leq m_2 \leq n_2 - 1, \ldots, 1 \leq m_k \leq n_k - 1$ and $m_j = 0\ \forall\ j$ such that $k + 1 \leq j \leq h$. From now on we shall assume that D has the decomposition just described.

Let $M = \{ z \in D \mid z$ has k components which are not 1 and $z + 1 = 1\}$. Let $N = \{ z \in M \mid \forall\ j,\ k + 1 \leq j \leq h,\ m_j \equiv 0 \bmod (n_j)\}$. $N \neq \emptyset$ since $z_o \in N$. Let $m_o = \min. \{ m \mid 1 \leq m \leq n_k - 1$ such that $\exists\ z \in N$ and the k^{th} component of z is $x_k^m \}$.

Then $\exists\ z_1 = (x_1^{m_1}, x_2^{m_2}, \ldots, x_{k-1}^{m_{k-1}}, x_k^{m_o}, 1, \ldots, 1) \in N$ where $1 \leq m_1 \leq n_1 - 1$, $1 \leq m_2 \leq n_2 - 1, \ldots, 1 \leq m_{k-1} \leq n_{k-1} - 1$ and $1 \leq m_o \leq n_k - 1$.

(**) Claim that $\forall\ s \in \mathbb{N}$, $z_1^s + 1 = 1$.

Since $z_1 \in M$, $z_1 + 1 = 1$. Let $s \in \mathbb{N}$. Assume that $z_1^s + 1 = 1$. Hence $z_1(z_1^s + 1) = z_1$, so we have that $z_1^{s+1} + z_1 + 1 = z_1 + 1$. Thus $z_1^{s+1} + 1 = 1$ and by mathematical induction we have (**).

Now, consider m_o. There are two cases, either $m_o \mid n_k$ or $m_o \nmid n_k$.

Assume that $m_o \mid n_k$. Then $n_k = jm_o$ for some $j \in \mathbb{N} - \{1\}$. Suppose that $\forall\ i,\ 1 \leq i \leq k - 1$, $jm_i \equiv 0 \bmod (n_i)$. Therefore $z_1^j = 1$. By (**), $z_1^{j-1} + 1 = 1$, so $z_1(z_1^{j-1} + 1) = z_1$. Hence $1 + z_1 = z_1$ and so $z_1 = 1$ which is a contradiction. Therefore $\exists\ i_o,\ 1 \leq i_o \leq k-1$ such that $jm_{i_o} \not\equiv 0 \bmod (n_{i_o})$. Again by (**), we have that $z_1^j + 1 = 1$ which implies that $(x_1^{jm_1}, x_2^{jm_2}, \ldots, x_{i_o-1}^{jm_{i_o}-1}, x_{i_o}^{jm_{i_o}}, x_{i_o+1}^{jm_{i_o}+1}, \ldots, x_{k-1}^{jm_{k-1}}, 1, \ldots, 1)+1=1$

which contradicts the induction hypothesis since $x_{i_o}^{jm_{i_o}} \neq 1$. Therefore

$m_o \nmid n_k$. Thus we have that $\exists\, s \in \mathbb{N}$ such that

$sm_o < n_k < (s+1)m_o < 2n_k$. Hence $x_k^{(s+1)m_o} = x_k^j$ for some j, $1 \leqslant j \leqslant n_k - 1$.

<u>Case 1.</u> Assume that $j < m_o$. Suppose that $\exists\ i_o$, $1 \leqslant i_o \leqslant k-1$ such that $(s+1)m_{i_o} \equiv 0 \bmod (n_{i_o})$. By (**), $z_1^{s+1} + 1 = 1$ which implies that

$(x_1^{(s+1)m_1}, x_2^{(s+1)m_2}, \ldots, x_{i_o-1}^{(s+1)m_{i_o}-1}, 1, x_{i_o+1}^{(s+1)m_{i_o}+1}, \ldots, x_{k-1}^{(s+1)m_k-1},$

$x_k^j, 1, \ldots, 1) + 1 = 1$, which contradicts the induction hypothesis. Therefore we have that $\forall\ i$, $1 \leqslant i \leqslant k-1$, $(s+1)m_i \not\equiv 0 \bmod (n_i)$. Since $z_1^{s+1} + 1 = 1$, $(x_1^{(s+1)m_1}, x_2^{(s+1)m_2}, \ldots, x_{k-1}^{(s+1)m_{k-1}}, x_k^j, 1, \ldots, 1) + 1 = 1$ which contradicts the choice of m_o.

<u>Case 2.</u> Assume that $j = m_o$. Then $(s+1)m_o \equiv m_o \bmod (n_k)$ and so $n_k \mid sm_o$, a contradiction since $0 < sm_o < n_k$.

<u>Case 3.</u> Assume that $j > m_o$. Then $j = r_1 m_o + r_2$ for some $r_1, r_2 \in \mathbb{N}$ $0 \leqslant r_2 < m_o$ and $r_1 \leqslant s$ since if $r_1 > s$ then $sm_o < r_1 m_o < n_k < (s+1)m_o$, which is a contradiction.

(3.1) <u>Case $r_1 = s$ and $r_2 = 0$.</u> Then $(s+1)m_o \equiv sm_o \bmod (n_k)$. Hence $m_o \equiv 0 \bmod (n_k)$ and we have that $x_k^{m_o} = 1$ which is a contradiction.

(3.2) <u>Case $r_1 < s$ and $r_2 = 0$.</u> Then $(s+1)m_o \equiv r_1 m_o \bmod (n_k)$, and so $(s+1-r_1)m_o \equiv 0 \bmod (n_k)$. Suppose that $\forall\ i$, $1 \leqslant i \leqslant k-1$, $(s+1-r_1)m_i \equiv 0 \bmod (n_i)$. Therefore $z_1^{s+1-r} = 1$. By (**) $z_1^{s-r_1} + 1 = 1$, so $z_1(z_1^{s-r_1} + 1) = z_1$. Hence $1 + z_1 = z_1$. Therefore we have that $1 = z_1$, a contradiction. So $\exists\ i_o$, $1 \leqslant i_o \leqslant k-1$, such that $(s+1-r_1)m_{i_o} \not\equiv 0 \bmod (n_{i_o})$.

Again by (**), $z_1^{s+1-r_1} + 1 = 1$, so

$$(x_1^{(s+1-r_1)m_1}, x_2^{(s+1-r_1)m_2}, \ldots, x_{i_o-1}^{(s+1-r_1)m_{i_o-1}}, x_{i_o}^{(s+1-r_1)m_{i_o}}, x_{i_o+1}^{(s+1-r_1)m_{i_o+1}},$$

$\ldots, x_{k-1}^{(s+1-r_1)m_{k-1}}, 1, \ldots, 1) + 1 = 1$, which contradicts the induction hypothesis since $x_{i_o}^{(s+1-r_1)m_{i_o}} \neq 1$.

(3.3) <u>Case $r_1 < s$ and $0 < r_2 < m_o$</u>. Then $(s+1)m_o \equiv r_1 m_o + r_2 \mod (n_k)$, and so $(s+1-r_1)m_o \equiv r_2 \mod (n_k)$. Suppose that $\exists\, i_o,\ 1 \leqslant i_o \leqslant k-1$, such that $(s+1-r_1)m_{i_o} \equiv 0 \mod (n_{i_o})$. By (**) $z_1^{s+1-r_1} + 1 = 1$, so

$$(x_1^{(s+1-r_1)m_1}, x_2^{(s+1-r_1)m_2}, \ldots, x_{i_o-1}^{(s+1-r_1)m_{i_o-1}}, 1, x_{i_o+1}^{(s+1-r_1)m_{i_o+1}}, \ldots,$$

$x_{k-1}^{(s+1-r_1)m_{k-1}}, x_k^{r_2}, 1, \ldots, 1) + 1 = 1$, which contradicts the induction hypothesis. Therefore $\forall\, i,\ 1 \leqslant i \leqslant k-1,\ (s+1-r_1)m_i \not\equiv 0 \mod (n_i)$ and we have that

$$(x_1^{(s+1-r_1)m_1}, x_2^{(s+1-r_1)m_2}, \ldots, x_{k-1}^{(s+1-r_1)m_{k-1}}, x_k^{r_2}, 1, \ldots, 1) + 1 = 1$$

which contradicts the choice of m_o.

(3.4) <u>Case $r_1 = s$ and $0 < r_2 < m_o$</u>. Then $(s+1)m_o \equiv sm_o + r_2 \mod (n_k)$, and so $m_o \equiv r_2 \mod (n_k)$. Hence $x_k^{m_o} = x_k^{r_2}$ which is a contradiction since $0 < r_2 < m_o < n_k - 1$.

We thus see that cases 1, 2 and 3 lead to contradictions. Hence we must have that $\forall\ z \in D - \{1\}$ having k components which are not 1, $z + 1 \neq 1$. By induction we have (3) i.e. $\forall\ z \in D - \{1\}$, $z + 1 \neq 1$. Since $\exists\ z \in D$ such that $z + 1 = 1$ by (*), we must then have that $1 + 1 = 1$.

From (1), we have that $(x_1, 1, \ldots, 1) + 1 = y$ for some $y \in D - \{1\}$. Hence $(x_1, 1, \ldots, 1) + 1 + 1 = y + 1$. Since $1 + 1 = 1$, we get that $y = (x_1, 1, \ldots, 1) + 1 = (x_1, 1, \ldots, 1) + 1 + 1 = y + 1$. Thus $1 = 1 + y^{-1}$ and $y^{-1} \neq 1$ since $y \neq 1$. This contradicts (3). Hence such a D cannot exist and we have the theorem. #

Remark 2.7. Let $(D, \cdot)$ be an abelian group. If we define + on D by $x + y = x \quad \forall\, x, y \in D$, then $(D, +)$ is a non-commutative semigroup. Since $x(y + z) = xy = xy + xz$, D satisfies all the axioms of P.R.D. except + is not commutative.

In particular, we see that if the condition of + being commutative was dropped, then we can have a set D of finite order > 1 which satisfies the axioms of a P.R.D.

In fact, even if $(D, \cdot)$ is not abelian then $\cdot$ distributes over the + defined above on both sides so we could get a P.R.D. of finite order > 1 which has non-abelian multiplication, if we drop the condition that + be commutative.

Corollary 2.7. If S is a finite semiring of order > 1, then S cannot be multiplicatively cancellative.

Proof : Suppose there exists S a finite semiring of order $n > 1$ such that S is multiplicatively cancellative. Let $x \in S$. Define $f_x : S \to S$ by $f_x(y) = xy \ \forall y \in S$. Let $y_1, y_2 \in S$ be such that $f_x(y_1) = f_x(y_2)$. Then $xy_1 = xy_2$ and so $y_1 = y_2$. Hence f_x is one-to-one. Since S is finite, f_x is onto. $\exists\, e \in S$ such that $f_x(e) = x$, so $xe = ex = x$. Let $y \in S$. Then

$xy = (xe)y = x(ey)$, so $y = ey = ye$ and hence e is the multiplicative identity. $\exists\, y^{-1} \in S$ such that $f_y(y^{-1}) = e$. Hence $yy^{-1} = y^{-1}y = e$. Thus we have that $(S, \cdot)$ is an abelian group and so S is a finite P.R.D. of order > 1, contradicting Theorem 2.5. #

Remark 2.8. $\mathbb{N}$ is a semiring which is multiplicatively cancellative.

For a P.R.D. of order 1 we see that 1 is also its additive identity and additive zero but in a P.R.D. of infinite order we cannot have this.

Proposition 2.9. If D is an infinite P.R.D. then D cannot contain any additive identity.

Proof : Suppose D has an additive identity e. Hence $e + x = x$ $\forall x \in D$. so $1 + e^{-1}x = e^{-1}x$ $\forall x \in D$. Since $(D, \cdot)$ is a group, $\{e^{-1}x\}_{x \in D} = D$. Therefore $1 + z = z$ $\forall z \in D$, so 1 is also the additive identity. Hence $1 = e$. Let $x \in D - \{1\}$. Then $1 + x = x$, so $x^{-1} + 1 = 1$. Since $x^{-1} + 1 = x^{-1}$, $x^{-1} = 1$. Hence $x = 1$, a contradiction. #

Proposition 2.10. If D is an infinite P.R.D. then D cannot contain any additive zero.

Proof : Suppose D has an additive zero 0, Hence $0 + x = 0$ $\forall x \in D$, so $1 + 0^{-1}x = 1$ $\forall x \in D$. Since $\{0^{-1}x\}_{x \in D} = D$, 1 is also the additive zero. Thus $0 = 1$. Let $x \in D - \{1\}$. Then $1 + x = 1$ and so $x^{-1} + 1 = x^{-1}$. Since $x^{-1} + 1 = 1$, $x^{-1} = 1$. Hence $x = 1$, a contradiction. #

Theorem 2.11. If S is a semiring then S can be embedded into a P.R.D. iff S is multiplicatively cancellative.

Proof : Assume that S is multiplicatively cancellative. Define a relation $\sim$ on $S \times S$ by $(x, y) \sim (x', y')$ iff $xy' = x'y$ $\forall x, y, x', y' \in S$. Clearly $\sim$ is reflexive and symmetric. Let $(a, b), (c, d), (e, f) \in S \times S$ be such that $(a, b) \sim (c, d)$ and $(c, d) \sim (e, f)$. Then $ad = cb$ and $cf = ed$, so $adf = cbf$ and $cfb = edb$. Hence $adf = edb$. Since S is multiplicatively cancellative, we get that $af = eb$. Therefore $(a, b) \sim (e, f)$, so $\sim$ is transitive and $\sim$ is an equivalence relation.

Let $\alpha, \beta \in \frac{S \times S}{\sim}$. Define + and $\cdot$ on $\frac{S \times S}{\sim}$ in the following way :

Choose $(a, b) \in \alpha$ and $(c, d) \in \beta$ and let $\alpha + \beta = [(ad + bc, bd)]$ and $\alpha\beta = [(ac, bd)]$. To show + and $\cdot$ are well-defined, let $(a', b') \in \alpha$ and $(c', d') \in \beta$. Then $ab' = a'b$ and $cd' = c'd$. Hence $ab'd' = a'bd'$ and $cb'd' = c'b'd$, so $adb'd' = a'dbd'$ and $bcb'd' = bc'b'd$. Therefore $adb'd' + bcb'd' = a'd'bd + b'c'bd$, and $(ad + bc)b'd' = (a'd' + b'c')bd$. Thus $(ad + bc, bd) \sim (a'd' + b'c', b'd')$, so + is well-defined. Since $acb'd' = a'bcd'$ and $a'bcd' = a'c'bd$, $acb'd' = a'c'bd$. Hence $(ac, bd) \sim (a'c', b'd')$ and $\cdot$ is well-defined.

Claim that $(\frac{S \times S}{\sim}, +, \cdot)$ is a P.R.D.

Let $a \in S$. Let $\alpha \in \frac{S \times S}{\sim}$. Choose $(c, d) \in \alpha$. Then $[(a, a)]\alpha = [(ac, ad)] = [(c, d)] = \alpha$ so $[(a, a)]$ is the multiplicative identity, also $[(d, c)]\alpha = [(cd, cd)] = [(a, a)]$ so every element has a multiplicative inverse. Clearly $\cdot$ is commutative and associative. Thus $(\frac{S \times S}{\sim}, \cdot)$ is an abelian group, and clearly $(\frac{S \times S}{\sim}, +)$ is a commutative semigroup.

Let $\alpha, \beta, \gamma \in \frac{S \times S}{\sim}$. Choose $(a, b) \in \alpha$, $(c, d) \in \beta$ and $(e, f) \in \gamma$.

Then $\alpha(\beta + \gamma) = [(a(cf + de), b(df))]$

$$= [(acf + ade, bdf)]$$

$$= [(acf + ade, bdf)][(b, b)]$$

$$= [(acbf + aebd, adbf)]$$

$$= [(ac, bd)] + [(ae, bf)]$$

$$= \alpha\beta + \alpha\gamma.$$

Therefore $\underset{\sim}{S \times S}$ is a P.R.D.

Let $a \in S$. Define $f : S \longrightarrow \underset{\sim}{S \times S}$ by $f(r) = [(ra, a)]\ \forall r \in S$. Let $x, y \in S$. Then $f(x + y) = [(xa + ya, a)] = [(xa + ya, a)][(a, a)]$ $= [(xa^2 + ya^2, a^2)] = [(xa, a)] + [(ya, a)] = f(x) + f(y)$ and $f(xy) = [(xya, a)] = [(xya, a)][(a, a)] = [(xya^2, a^2)] =$ $[(xa, a)][(ya, a)] = f(x)f(y)$. Therefore f is a homomorphism.

Let $x, y \in S$ be such that $f(x) = f(y)$. Then $[(xa, a)] = [(ya, a)]$. Hence $xa^2 = ya^2$ and so $x = y$. Thus f is one-to-one and so we can embed S into $\underset{\sim}{S \times S}$.

Conversely, assume that S can be embedded into D which is a P.R.D. Let $x, y, z \in S$ be such that $xy = xz$. Hence $x^{-1}xy = x^{-1}xz$, so $y = z$. Thus S is multiplicatively cancellative. #

Remark 2.12. In the above theorem if S has a multiplicative identity 1 then we can embed S into $\underset{\sim}{S \times S}$ in a canonical way by defining $f(r) = [(r, 1)]$.

Proposition 2.13. If S is a semiring with multiplicative cancellation, then $\underset{\sim}{S \times S}$ is the smallest P.R.D. containing S up to isomorphism i.e. every P.R.D. containing S has a sub P.R.D. isomorphic to $\underset{\sim}{S \times S}$.

Proof: Let D be a P.R.D. such that $S \subseteq D$.

Define $\theta : \underset{\sim}{\underline{D \times D}} \longrightarrow D$ in the following way :

Let $\alpha \in \underset{\sim}{\underline{D \times D}}$. Choose $(a, b) \in \alpha$ and let $\theta(\alpha) = ab^{-1}$. To show θ is well-defined, let $(a', b') \in \alpha$. Then $ab' = a'b$. Hence $ab^{-1} = a'b'^{-1}$ and θ is well-defined.

Let $\alpha, \beta \in \underset{\sim}{\underline{D \times D}}$. Choose $(a, b) \in \alpha$, $(c, d) \in \beta$. Then $\theta(\alpha + \beta) = (ad + bc)(bd)^{-1} = ab^{-1} + cd^{-1} = \theta(\alpha) + \theta(\beta)$ and $\theta(\alpha\beta) = (ac)(bd)^{-1} = (ab^{-1})(cd^{-1}) = \theta(\alpha)\,\theta(\beta)$. Hence θ is a homomorphism.

Let $\alpha, \beta \in \underset{\sim}{\underline{D \times D}}$ be such that $\theta(\alpha) = \theta(\beta)$. Choose $(a, b) \in \alpha$ and $(c, d) \in \beta$. Then $ab^{-1} = cd^{-1}$ and so $ad = bc$. Hence $\alpha = [(a, b)] = [(c, d)] = \beta$ and θ is one-to-one.

Let $x \in D$. Then $\theta([(x, 1)]) = x$ and θ is onto. Therefore we have $\underset{\sim}{\underline{D \times D}} \cong D$.

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

Theorem 2.14. If D is an infinite P.R.D., then the smallest sub-P.R.D. of D is either isomorphic to $\mathbb{Q}^+$ with usual addition and multiplication or $\{1\}$.

Proof : Since the intersection of sub-P.R.D.'s is a sub-P.R.D., we have that the smallest sub-P.R.D. of a P.R.D. exists and is the intersection of all of its sub-P.R.D.'s. Let D' be the smallest sub-P.R.D. of D. Let $n \in \mathbb{N}$. Then define $n1 = 1 + 1 + \ldots + 1$ (n times), so we have that $\{n1\}_{n \in \mathbb{N}} \subseteq D'$

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

Note that $\mathbb{N}$ with the usual addition and multiplication is a multiplicatively cancellative semiring and $(\underline{\mathbb{N} \times \mathbb{N}}_{\sim}, +, \cdot) \cong (\mathbb{Q}^+, +, \cdot)$

Define $\theta : \mathbb{N} \longrightarrow D$ by $\theta(n) = n1 \quad \forall n \in \mathbb{N}$. Let $n_1, n_2 \in \mathbb{N}$. Then $\theta(n_1 + n_2) = (n_1 + n_2)1 = n_1 1 + n_2 1 = \theta(n_1) + \theta(n_2)$ and $\theta(n_1 n_2) = (n_1 n_2)1 = (n_1 1)(n_2 1) = \theta(n_1)\theta(n_2)$. Thus θ is a homomorphism. Clearly θ is one-to-one, so $\theta(\mathbb{N}) \cong \mathbb{N}$ and $\theta(\mathbb{N})$ is also a multiplicatively cancellative semiring contained in D. Therefore by Proposition 2.13 $\underline{\theta(\mathbb{N}) \times \theta(\mathbb{N})}_{\sim}$ is the smallest sub-P.R.D. of D containing $\theta(\mathbb{N})$ up to isomorphism. Since $\theta(1) \in D'$, $n1 \in D' \ \forall n \in \mathbb{N}$. Hence $\theta(\mathbb{N}) \subseteq D'$, so up to isomorphism we can consider that $\underline{\theta(\mathbb{N}) \times \theta(\mathbb{N})}_{\sim} \subseteq D'$. Since D' is the smallest sub-P.R.D., up to isomorphism we can consider that $D' \subseteq \underline{\theta(\mathbb{N}) \times \theta(\mathbb{N})}_{\sim}$. Therefore $D' \cong \underline{\theta(\mathbb{N}) \times \theta(\mathbb{N})}_{\sim}$.

Let $f : \underline{\mathbb{N} \times \mathbb{N}}_{\sim} \longrightarrow \underline{\theta(\mathbb{N}) \times \theta(\mathbb{N})}_{\sim}$ be defined in the following way : Let $\alpha \in \underline{\mathbb{N} \times \mathbb{N}}_{\sim}$. Choose $(m, n) \in \alpha$ and let $f(\alpha) = [(\theta(m), \theta(n))]$. It is clear that f is well-defined and is an isomorphism. Thus $D' \cong \underline{\theta(\mathbb{N}) \times \theta(\mathbb{N})}_{\sim} \cong \underline{\mathbb{N} \times \mathbb{N}}_{\sim} \cong \mathbb{Q}^+$.

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

Let $m_o = \min.\{m \in \mathbb{N} \mid \exists n \in \mathbb{N} \quad n > m$ and $m1 = n1\}$ and let $n_o = \min.\{n \in \mathbb{N} \mid n > m_o$ and $m_o 1 = n1\}$.

Claim that $m_o = 1$ and $n_o = 2$.

Suppose that $m_o \neq 1$ or $n_o \neq 2$. Hence $m_o > 1$ or $n_o > 2$. If $m_o > 1$ then $n_o > 2$. Thus in both cases we have that $n_o - 1 \geqslant 2$ and $\forall m \in \mathbb{N}$ $m1 \in \{n1\}_{1 \leqslant n \leqslant n_o - 1}$. Let $B = \{n1\}_{1 \leqslant n \leqslant n_o - 1}$ and $C = \{(n1)(m1)^{-1}\}_{n1,\ m1 \in B}$. Then C is a finite set with cardinality > 1 and $1 = 1 \cdot 1 \in C$. Let $(n_1 1)(m_1 1)^{-1}$, $(n_2 1)(m_2 1)^{-1} \in C$. Then

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

And

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

Since $(m_1 1)(n_1 1)^{-1} \in C$ and $((n_1 1)(m_1 1)^{-1})((m_1 1)(n_1 1)^{-1}) = 1$, we have that $\forall\ x \in C,\ x^{-1} \in C$. Therefore C is a finite sub-P.R.D. of D with cardinality > 1, which contradicts Theorem 2.5. Hence the claim is true and we have $1 + 1 = 1$. Therefore $\{1\} = D'$. #

Example 2.15. $\mathbb{Q}^+$ with the usual multiplication and + defined by $x + y = \min.\{x, y\}$ $\forall\ x, y \in \mathbb{Q}^+$ is a P.R.D. with $\{1\}$ as its smallest sub-P.R.D.

Remark 2.16. $\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle|\ a, c \in \mathbb{Q}^+, b \in \mathbb{Q} \right\}$ satisfies all the axioms of a P.R.D. except that $\cdot$ is not commutative.