

\mathcal{P} -Cryptogroups

Miyuki YAMADA

Department of Mathematics, Shimane University, Matsue, Japan
(Received September 7, 1988)

A semigroup which is a band of groups is called a cryptogroup (see [4]). Let P be a C -set in a cryptogroup S . Then, $S(P)$ is \mathcal{P} -regular (see [11]). In this case, we simply say that $S(P)$ is a \mathcal{P} -cryptogroup. In this paper, the structure of \mathcal{P} -cryptogroups is investigated.

§1. Introduction

Let S be a regular semigroup, and E_S the set of idempotents of S . Let P be a subset of E_S such that $P \cap L \neq \square$ and $P \cap R \neq \square$ for every \mathcal{L} -class L and \mathcal{R} -class R of S (where \mathcal{L} and \mathcal{R} are Green's L - and R -relations respectively). If the pair (S, P) of S and P satisfies

$$(C.1) \quad (1) \quad P^2 \subset E_S, \\ (2) \quad qPq \subset P \quad \text{for } q \in P,$$

then we say that $S(P)$ is *weakly \mathcal{P} -regular*. If (S, P) further satisfies

$$(3) \quad \text{for any } x \in S, \text{ there exists } x^* \in V(x) \text{ (where } V(x) \text{ denotes the set of all inverses of } x \text{) such that } xP^1x^*, x^*P^1x \subset P \text{ (where } P^1 \text{ is the adjunction of } 1 \text{ to } P),$$

then $S(P)$ is called *\mathcal{P} -regular*. In this case, x^* above is called a *\mathcal{P} -inverse* of x , and the set of all \mathcal{P} -inverses of x is denoted by $V_{\mathcal{P}}(x)$.

If $S(P)$ is \mathcal{P} -regular and if $V_{\mathcal{P}}(q) \subset P$ for every $q \in P$, then $S(P)$ is called *strongly \mathcal{P} -regular*.

In a regular semigroup S , a subset P of E_S is called a *full subset* of E_S if $P \cap L \neq \square$ and $P \cap R \neq \square$ for every \mathcal{L} -class L and \mathcal{R} -class R of S . Further, a full subset P of E_S is called *left [right] minimal* if $P \cap L$ [$P \cap R$] consists of a single element for every \mathcal{L} -class L [\mathcal{R} -class R] of S . A full subset P of E_S is called a *C -set* in S if it satisfies (1)–(3) of (C.1).

For example, if S is a regular semigroup then $S(E_S)$ is \mathcal{P} -regular if and only if S is orthodox. As another example, if S is a regular semigroup with special involution $\#$ (that is, a regular $*$ -semigroup having $\#$ as its special involution; see [8]) and if Q is the set of all projections of S , then $S(Q)$ is \mathcal{P} -regular and Q is a both left and right minimal full subset of E_S . Conversely, if $S(Q)$ is a \mathcal{P} -regular semigroup and if Q is a both left and right minimal full subset of E_S , then every element x of S has a unique \mathcal{P} -inverse x^* , and S becomes a regular $*$ -semigroup having Q as its projections under the special involution $\#$.

defined by " $x^* = (\text{the } \mathcal{P}\text{-inverse of } x)$ ". Hereafter, such a regular $*$ -semigroup having $\#$ and Q as its special involution and the projections respectively is denoted by $S(Q; \#)$. From the examples above, it is easy to see that the class of \mathcal{P} -regular semigroups contains both the class of orthodox semigroups and that of regular $*$ -semigroups. The following shows a part of the connection between orthodox semigroups, inverse semigroups, regular $*$ -semigroups and strongly \mathcal{P} -regular semigroups:

THEOREM 1.1. *Let $S(P)$ be a \mathcal{P} -regular semigroup. Then:*

- (1) $P = E_S$ if and only if P is closed with respect to the multiplication. Hence, in this case S is orthodox.
- (2) $S(P)$ is strongly \mathcal{P} -regular if and only if $pq \in P$ implies $qp \in P$ for every $p, q \in P$.
- (3) $S(P)$ is a regular $*$ -semigroup having P as its projections if and only if $pq \in P$ implies $qp \in P$ and $pq = qp$ for $p, q \in P$.
- (4) $S(P)$ is an inverse semigroup if and only if $pq = qp$ for $p, q \in P$.

PROOF. (1) Obvious. (2): The "if" part: Let $p \in P$, and $q \in V_{\mathcal{P}}(P)$. Let $pq = u$ and $qp = v$. Then, $u, v \in P$. Since $uv \in E_S$, $uv \mathcal{R} u$ and $uv \mathcal{L} v$, we have $p = uv$. Similarly, $vu = q$. Since $uv \in P$, it follows that $vu \in P$. Hence, $q \in P$, that is, $S(P)$ is strongly \mathcal{P} -regular. The "only if" part: Let $qp \in P$ for $p, q \in P$. Then, every \mathcal{P} -inverse of pq is contained in P . Hence, $qp \in P$ since qp is a \mathcal{P} -inverse of pq .

(3): The "if" part: We need only to show that P is a p -system (see [8]). Suppose that $p \mathcal{L} q$ for $p, q \in P$. Then, $pq = p \in P$. Therefore, $pq = qp$. Hence, $p = q$. Thus, each of $L \cap P$ and $R \cap P$ consists of a single element for every \mathcal{L} -class L and \mathcal{R} -class R . This implies that P is a p -system in S . (4): The "if" part: Let $p, q \in P$. Since $pqp \in P$, $pqp = ppq = pq \in P$. Therefore, $E_S = P^2 \subset P$, that is, $P = E_S$. Thus, $ef = fe$ for $e, f \in E_S$. That is, $S(P)$ is an inverse semigroup.

The "only if" part: For $p, q \in P$, $pq = pqp \in P$. Thus, $P^2 \subset P$, and hence $E_S = P$ by (1). Since $S(P)$ is an inverse semigroup, $pq = qp$ for $p, q \in E_S = P$.

Further, we have the following:

THEOREM 1.2. *Let $S(P)$ be a \mathcal{P} -regular semigroup. Then, $S(P)$ is strongly \mathcal{P} -regular if and only if $p, q, h \in P$ and $q \mathcal{L} h \mathcal{R} p$ imply that there exists $u \in P$ such that $p \mathcal{L} u \mathcal{R} q$.*

PROOF. The "if" part: Let $p \in P$, and p^* a \mathcal{P} -inverse of p . Let $pp^* = q$ and $p^*p = h$. Then, $q, h \in P$ and $q \mathcal{R} p \mathcal{L} h$. Hence, there exists $u \in P$ such that $q \mathcal{L} u \mathcal{R} h$. Now, $qh = p$ and $hq = u$. Since $p^* = hq = u \in P$, $S(P)$ is strongly \mathcal{P} -regular. The "only if" part: Let $p, q, h \in P$, and $q \mathcal{L} h \mathcal{R} p$. There exists $u \in V(h)$ such that $p \mathcal{L} u \mathcal{R} q$. Now, $hu = p$ and $uh = q$. Since $pq = h$ and $qp = u$ and since $pq \in P$, it follows that $qp \in P$. Then, $u \in P$.

The basic properties of a \mathcal{P} -regular semigroup and the structures of some special \mathcal{P} -regular semigroups have been studied in the previous papers [11] and [12]. A regular semigroup is called a *cryptogroup* if it is a band of groups (see [4]). In this paper, we shall investigate the structure of \mathcal{P} -regular cryptogroups (abbrev., \mathcal{P} -cryptogroups).

§2. Fundamental properties

A completely regular semigroup S is uniquely decomposed into a semilattice A of completely simple subsemigroups $\{S_\lambda: \lambda \in A\}$. This decomposition is called *the structure decomposition* of S , and is denoted by $S \sim \Sigma\{S_\lambda: \lambda \in A\}$. In this case A is unique up to isomorphism, and is called *the structure semilattice* of S .

It has been shown in [6] that an orthodox cryptogroup S is isomorphic to the spined product (hence, of course a subdirect product) of E_S and a Clifford semigroup C (see [6]). That is, there exists a Clifford semigroup C whose structure semilattice A is the same as that of E_S , such that S is isomorphic to the spined product $E_S \triangleright_{\lambda} C$ of E_S and C . That is, let $E_S \sim \Sigma\{E_\lambda: \lambda \in A\}$ and $C \sim \Sigma\{C_\lambda: \lambda \in A\}$ be the structure decompositions of E_S and C . Then,

$E_S \triangleright_{\lambda} C = \Sigma\{E_\lambda \times C_\lambda \text{ (direct product): } \lambda \in A\}$ (where Σ means disjoint sum), and the multiplication is given by

$$(e, a) (f, b) = (ef, ab),$$

and $S \cong E_S \triangleright_{\lambda} C$.

It is obvious that any \mathcal{P} -regular semigroup is weakly \mathcal{P} -regular. Conversely,

LEMMA 2.1. *For a cryptogroup S , $S(P)$ is \mathcal{P} -regular if and only if it is weakly \mathcal{P} -regular.*

PROOF. The “only if” part is obvious. The “if” part: Let $S(P)$ be a band A of groups $\{G_\lambda: \lambda \in A\}$. Of course, each G_λ is an \mathcal{H} -class (where \mathcal{H} denotes Green’s H -relation) of $S(P)$. Let e_λ be the identity of G_λ . Let $x \in H_{e_\lambda}$ (the \mathcal{H} -class containing e_λ ; hence $H_{e_\lambda} = G_\lambda$). Then, there exist p, q such that $pq = e_\lambda$. There exists $x^* \in V(x) \cap H_{qp}$. Now, $xx^* = p$ and $x^*x = q$. For any $h \in P$, $(xhx^*)^2 = xhx^*$. There exist G_τ, G_δ such that $h \in G_\tau$ and $x^* \in G_\delta$. Then, $xhx^* \in G_{\lambda\tau\delta}$, and $pqhqp \in G_{\lambda\tau\delta}$. Hence, $xhx^* = pqhqp \in P$.

Similarly, $x^*hx \in P$. Thus, $x^* \in V_\mathcal{P}(x)$. Therefore, $S(P)$ is \mathcal{P} -regular.

Thus, for cryptogroups, weakly \mathcal{P} -regularity and \mathcal{P} -regularity are just the same. It is well-known that a regular semigroup is an inverse semigroup if and only if every element has a unique inverse. Similarly, the following is interest as a characterization of a regular $*$ -semigroup:

THEOREM 2.2. *A \mathcal{P} -regular semigroup $S(P)$ is a regular $*$ -semigroup $S(P; \#)$ if and only if every element x of $S(P)$ has a unique \mathcal{P} -inverse.*

PROOF. The “only if” part: Suppose that $S(P)$ is a regular $*$ -semigroup $S(P; \#)$. Then, it is easy to see that x^* is a unique \mathcal{P} -inverse of x for any element $x \in S(P)$ (see [8]). The “if” part: Assume that every element x of the \mathcal{P} -regular semigroup $S(P)$ has a unique \mathcal{P} -inverse x^* . Suppose that a certain \mathcal{L} -class L contains two different elements p, q of P . Since $pq = p$ and $qp = q$, we have $pPq = pqPqp \subset pPp \subset P$ and $qPp = qpPpq \subset qPq \subset P$. Since $q \in V(P)$, q is a \mathcal{P} -inverse of p , and hence $p = q$. This is a contradiction. Thus, each \mathcal{L} -class contains a unique element of P . Similarly, each \mathcal{R} -class contains a unique element of P . Therefore, P is a both left and right minimal full

subset of E_S , and accordingly $S(P)$ becomes a regular $*$ -semigroup $S(P; \#)$.

§3. Completely simple \mathcal{P} -regular semigroups

First, we have:

THEOREM 3.1. *Let B be a rectangular band, and P a full subset of B . Then, P is a C -set in B , and accordingly $B(P)$ is \mathcal{P} -regular.*

PROOF. Since $qPq = \{q\} \subset P$ for $q \in P$, $B(P)$ is weakly \mathcal{P} -regular. Since B is of course a cryptogroup, it is also \mathcal{P} -regular.

COROLLARY. *if B is a square band (see [8]), and P a both left and right minimal full subset of B . Then, $B(P)$ is \mathcal{P} -regular, and it becomes a regular $*$ -semigroup $B(P; \#)$ under the special involution $\#$ defined by $x^\# =$ (the \mathcal{P} -inverse of x).*

Next, we shall investigate the completely simple (weakly) \mathcal{P} -regular semigroups. Let S be a completely simple semigroup. Then we can assume that S is a Rees $I \times J$ matrix semigroup over a group G with sandwich matrix Q ; that is, $S = M(G; I, J; Q)$ (see [1]). Let $Q = [p_{ji}]$ ($j \in J, i \in I$).

LEMMA 3.2. *For a completely simple semigroup $S = M(G; I, J; Q)$ and for idempotents $[p_{ji}^{-1}]_{ij}, [p_{sk}^{-1}]_{ks}$, the following (1), (2) are equivalent:*

- (1) $[p_{ji}^{-1}]_{ij}[p_{sk}^{-1}]_{ks} \in E_S$ and $[p_{sk}^{-1}]_{ks}[p_{ji}^{-1}]_{ij} \in E_S$.
- (2) $[p_{ji}^{-1}]_{ij}[p_{sk}^{-1}]_{ks}[p_{ji}^{-1}]_{ij} = [p_{ji}^{-1}]_{ij}$.

PROOF. (1) \Rightarrow (2): It is obvious that $[p_{sk}^{-1}]_{ks}[p_{ji}^{-1}]_{ij}$ is an inverse of $[p_{ji}^{-1}]_{ij}[p_{sk}^{-1}]_{ks}$. Hence, $[p_{ji}^{-1}]_{ij}[p_{sk}^{-1}]_{ks}[p_{sk}^{-1}]_{ks}[p_{ji}^{-1}]_{ij} = [p_{ji}^{-1}]_{ij}[p_{sk}^{-1}]_{ks}[p_{ji}^{-1}]_{ij} \in E_S$. Then, we have $[p_{ji}^{-1}]_{ij}[p_{sk}^{-1}]_{ks}[p_{ji}^{-1}]_{ij} = [p_{ji}^{-1}]_{ij}$. (2) \Rightarrow (1): Obvious.

By the result above, we have:

LEMMA 3.3. *Let S be a completely simple semigroup, and P a full subset of E_S . Then, the following (1) and (2) are equivalent:*

- (1) $P^2 \subset E_S$.
- (2) For any $q \in P$, $qPq = \{q\}$.

Further, $S(P)$ is \mathcal{P} -regular if and only if it satisfies one of (1) and (2).

PROOF. The first part follows from Lemma 3.2. It is obvious that if $S(P)$ is \mathcal{P} -regular then P satisfies (1) and (2). Conversely, suppose that P satisfies (1) or (2). Then, $S(P)$ is weakly \mathcal{P} -regular. Since S is a cryptogroup, $S(P)$ is \mathcal{P} -regular.

Suppose that P is a C -set in $S = M(G; I, J; Q)$. Let $T = \{(i, j) \in I \times J : [p_{ji}^{-1}]_{ij} \in P\}$. Then, of course

- (C.3) (1) for any $i \in I$, there exists $j \in J$ such that $(i, j) \in T$, and
 (2) for any $j \in J$, there exists $i \in I$ such that $(i, j) \in T$.

Since P is a C -set, $[p_{ji}^{-1}]_{ij}[p_{sk}^{-1}]_{ks} = [p_{si}^{-1}]_{is}$ for $(i, j), (k, s) \in T$. Hence, $p_{ji}^{-1} p_{jk}^{-1} p_{sk}^{-1} = p_{si}^{-1}$, that is, $p_{ji}^{-1} p_{jk} = p_{si}^{-1} p_{sk}$.

Thus, $Q = [p_{uv}]$ satisfies the following:

- (C.4) $p_{ji}^{-1} p_{jk} = p_{si}^{-1} p_{sk}$ for any $(i, j), (k, s) \in T$.

Conversely, suppose that T is a subset of $I \times J$ such that it satisfies (C.3). In this case, if $Q = [p_{uv}]$ satisfies (C.4), then $S(P)$ is weakly \mathcal{P} -regular, and hence \mathcal{P} -regular, with respect to $P = \{[p_{ji}^{-1}]_{ij}; (i, j) \in T\}$.

First, it is obvious that P is a full subset of E_S . For any $[p_{ji}^{-1}]_{ij}, [p_{sk}^{-1}]_{ks} \in P$, $[p_{ji}^{-1}]_{ij}[p_{sk}^{-1}]_{ks} = [p_{ji}^{-1} p_{jk}^{-1} p_{sk}^{-1}]_{is} = [p_{si}^{-1}]_{is}$ (by (C.4)) $\in E_S$. Hence, it follows from Lemma 3.3 that $S(P)$ is weakly \mathcal{P} -regular, and accordingly \mathcal{P} -regular. Thus, we have:

THEOREM 3.4. *Let $S = M(G; I, J; Q)$ be a completely simple semigroup, and $Q = [p_{uv}]$. Let T be a subset of $I \times J$ such that*

- (1) T satisfies (C.3), and
 (2) $P = \{[p_{ji}^{-1}]_{ij}; (i, j) \in T\}$ satisfies (C.4),

then $S(P)$ is \mathcal{P} -regular. Further, every completely simple \mathcal{P} -regular semigroup is constructed in this fashion.

Let $S(P)$ be a \mathcal{P} -regular semigroup. Let T be a regular subsemigroup of S , and put $U = P \cap T$. Then, $T(U)$ is called a \mathcal{P} -regular subsemigroup of $S(P)$ if $T(U)$ is \mathcal{P} -regular. Let $S_1(P_1)$ and $S_2(P_2)$ be \mathcal{P} -regular semigroups, and $f: S_1(P_1) \rightarrow S_2(P_2)$ a homomorphism. Then, f is called a \mathcal{P} -homomorphism if $P_1 f = S_1 f \cap P_2$. Let $S(P)$ be a \mathcal{P} -regular semigroup, and τ a congruence on $S(P)$. Let $x\tau = \bar{x}$ for $x \in S$, and $\bar{X} = \{\bar{x}; x \in X\}$ for a subset X of S . Then, $\bar{S}(\bar{P})$ is a \mathcal{P} -regular semigroup, which we call the factor \mathcal{P} -regular semigroup of $S(P)$ mod τ and denote by $S(P)/(\tau)_{\mathcal{P}}$. Hereafter, this congruence τ is especially called a \mathcal{P} -congruence. Hence, a congruence and a \mathcal{P} -congruence are essentially the same. A bijective \mathcal{P} -homomorphism is called a \mathcal{P} -isomorphism. Hereafter, a \mathcal{P} -regular band is simply called a \mathcal{P} -band. Let $E(P), S(Q)$ be a rectangular \mathcal{P} -band and a completely simple \mathcal{P} -regular semigroup, and $E(P) \times S(Q) = T(U)$ the direct product of $E(P)$ and $S(Q)$, where $U = \{(p, q); p \in P \text{ and } q \in Q\}$. Then, $T(U)$ is \mathcal{P} -regular. This $T(U)$ is called a \mathcal{P} -direct product of $E(P)$ and $S(Q)$ (for the general case, see §5). Let V be a subdirect product of E and S . Let $(e, x) \in V$. Then, there exists $(f, x^{-1}) \in V$, where x^{-1} is the group inverse of x and $f \in E$. Then $(e, x)(f, x^{-1}) = (ef, h)$, where $h = xx^{-1}$. Similarly, $(f, x^{-1})(e, x) = (fe, h)$. Hence, $(ef, h)(f, x^{-1})(fe, h) = (e, x^{-1}) \in V$. Hence, V is a completely simple semigroup. Let $K = \{(p, q) \in V; p \in P \text{ and } q \in Q\}$. If $V(K)$ is \mathcal{P} -regular, then $V(K)$ is a \mathcal{P} -regular subsemigroup of $E(P) \times_{\mathcal{P}} S(Q) = T(U)$, where $E(P) \times_{\mathcal{P}} S(Q)$ denotes the \mathcal{P} -direct product of $E(P)$ and $S(Q)$. This $V(K)$

is called a \mathcal{P} -subdirect product of $E(P)$ and $S(Q)$.

We shall show later the following: Any completely simple \mathcal{P} -regular semigroup $S(U)$ is \mathcal{P} -isomorphic to a \mathcal{P} -subdirect product of a rectangular \mathcal{P} -band $E(P)$ and a completely simple $*$ -semigroup $T(Q; \#)$. Conversely, a \mathcal{P} -subdirect product $S(U)$ of a rectangular \mathcal{P} -band $E(P)$ and a completely simple $*$ -semigroup $T(Q; \#)$ is a completely simple \mathcal{P} -regular semigroup.

EXAMPLES. 1. Let $S = M(G; I, J; Q)$ be a completely simple semigroup such that $Q = [p_{ji}]$, where $p_{ji} = 1$ for all $(j, i) \in J \times I$. Then, $E_S = \{[1]_{ij}: (i, j) \in I \times J\}$. Let T be a subset of $I \times J$, and assume that T satisfies (C.3). Then, $P = \{[1]_{ij}: (i, j) \in T\}$ is a C -set in S , and $S(P)$ is \mathcal{P} -regular. In particular, $S(E_S)$ is \mathcal{P} -regular and is orthodox.

2. Let S be a completely simple semigroup: $S = M(G; I, J; Q)$. Let T be a subset of $I \times J$, and assume that T satisfies (C.3). Further, assume that $Q = [p_{uv}]$ satisfies $p_{ji} = 1$ for $(i, j) \in T$ and $p_{si} = p_{jk}^{-1}$ for $(i, j), (k, s) \in T$. Put $P = \{[1]_{ij}: (i, j) \in T\}$. Then, $S(P)$ is \mathcal{P} -regular. In particular, consider the case where $I = J$ and $p_{ii} = 1$ for all $(i, i) \in I \times I$ and $p_{it} = p_{it}^{-1}$ for all $(i, t) \in I \times I$. Let $T = I \times I$, and $P = \{[1]_{ii}: (i, i) \in T\}$. Then, T satisfies (C.3) and $S(P)$ is \mathcal{P} -regular. In fact, in this case $S(P)$ is a regular $*$ -semigroup $S(P; \#)$. Further, it has been shown in [5] that every completely simple regular $*$ -semigroup is constructed in this fashion.

§4. \mathcal{P} -Bands

Let B be a band, and $B \sim \Sigma\{B_\lambda: \lambda \in A\}$ the structure decomposition of B . Let $P \subset B$. If $B(P)$ is \mathcal{P} -regular, then $B_\lambda(P_\lambda)$, where $P_\lambda = B_\lambda \cap P$, is also \mathcal{P} -regular, that is, P_λ is a full subset of B_λ . Conversely, let P_λ be a full subset of B_λ for all $\lambda \in A$. Then, $B_\lambda(P_\lambda)$ is \mathcal{P} -regular, but $P = \Sigma\{P_\lambda: \lambda \in A\}$ is not necessarily a C -set in B , and hence $B(P)$ is not necessarily \mathcal{P} -regular. However, we can construct the least C -set Q_p containing P as follows:

Let $p_1, p_2, \dots, p_n \in P$, and consider the element $p_1 p_2 \cdots p_{n-1} p_n p_{n-1} \cdots p_2 p_1$. Let Q_p be all these elements, that is, $Q_p = \{p_1 p_2 \cdots p_{n-1} p_n p_{n-1} \cdots p_2 p_1 \mid (n \text{ arbitrary}): p_i \in P \text{ for all } i = 1, 2, \dots, n\}$. Then, clearly $q Q_p q \subset Q_p$ for any $q \in Q_p$. Hence, Q_p is a C -set in B and $Q_p \supset P$. It is obvious that any C -set (in B) containing P contains Q_p . Therefore, Q_p is the least C -set containing P . Of course, if P itself is a C -set in B , then $Q_p = P$. Hence, we have:

THEOREM 4.1. *Let B be a band, and P a full subset of B .*

Let $Q_p = \{p_1 p_2 \cdots p_{n-1} p_n p_{n-1} \cdots p_2 p_1 \mid (n \text{ arbitrary}): p_i \in P \text{ for } i = 1, 2, \dots, n\}$. Then, Q_p is the least C -set containing P , and $B(Q_p)$ is \mathcal{P} -regular. Further, every \mathcal{P} -band is constructed in this fashion.

Consider special kinds of bands, in particular the class of regular bands and that of normal bands. Let B be a regular band, and define multiplication \circ in B as follows:

$$(C.5) \quad a \circ b = aba \quad \text{for } a, b \in B.$$

Then, $B(\circ)$ is also a band. Let P be a full subset of B (not of $B(\circ)$). Then, it is easy to see that $pPp \subset P$ if and only if $P(\circ)$ is a subband of $B(\circ)$. Hence, P is a C -set in B if and only if $P(\circ)$ is a subband of $B(\circ)$.

Therefore, we have:

THEOREM 4.2. *Let B be a regular band, and P a full subset of B . Then, P is a C -set in B if and only if $P(\circ)$ is a subband of $B(\circ)$.*

Next, let B be a normal band. It is well-known that B is a strong semilattice A of rectangular bands $\{B_\lambda: \lambda \in A\}$. That is, there exists a transitive system $\{\phi_\beta^\alpha: \alpha \geq \beta, \alpha, \beta \in A\}$ of homomorphisms $\phi_\beta^\alpha: B_\alpha \rightarrow B_\beta$ such that the product of $a \in B_\lambda$ and $b \in B_\delta$ is given by $ab = (a\phi_{\lambda\delta}^\lambda)(b\phi_{\lambda\delta}^\delta)$ (see [10]). In this case, denote B by $B = \mathcal{S}(B_\lambda; A; \phi_\beta^\alpha)$. Then we have:

THEOREM 4.3. *Let P be a full subset of a normal band $B = \mathcal{S}(B_\lambda; A; \phi_\beta^\alpha)$. Let $P \cap B_\lambda = P_\lambda$ for each $\lambda \in A$. Then, $B(P)$ is \mathcal{P} -regular if and only if $P_\alpha \phi_\beta^\alpha \subset P_\beta$ for $\alpha, \beta \in A$ with $\alpha \geq \beta$.*

PROOF. The “if” part: Obvious. The “only if” part: Let $p \in P_\alpha$ and $\alpha \geq \beta$. Since $B(P)$ is \mathcal{P} -regular, $pP_\beta p \subset P_\beta$. Hence, $pqp = (p\phi_\beta^\alpha)q(p\phi_\beta^\alpha) = p\phi_\beta^\alpha \subset P_\beta$ for $q \in P_\beta$.

§5. \mathcal{P} -Cryptogroups

Let $S(P)$ and $V(Q)$ be \mathcal{P} -regular semigroups. Consider the direct product W of S and V ; that is, $W = S \times V$. Let $K = \{(p, q) \in S \times V: p \in P \text{ and } q \in Q\}$. Then, $W(K)$ is \mathcal{P} -regular. This $W(K)$ is called the \mathcal{P} -direct product of $S(P)$ and $V(Q)$, and denoted by $S(P) \times_{\mathcal{P}} V(Q)$. Let $T(P_T)$ be a \mathcal{P} -regular subsemigroup of $W(K) = S(P) \times_{\mathcal{P}} V(Q)$, where $P_T = T \cap K$. If the first and second projections of $T(P_T)$ to $S(P)$ and $V(Q)$ are surjective \mathcal{P} -homomorphisms, then $T(P_T)$ is called a \mathcal{P} -subdirect product of $S(P)$ and $V(Q)$. Now, we consider the special case where $S(P)$ and $V(Q)$ are \mathcal{P} -cryptogroups.

Let $A(P)$ and $B(Q)$ be \mathcal{P} -cryptogroups, and $A \sim \Sigma\{A_\lambda: \lambda \in A\}$ and $B \sim \Sigma\{B_\lambda: \lambda \in A\}$ be the structure decompositions of A and B respectively, and put $P_\lambda = P \cap A_\lambda$ and $Q_\lambda = Q \cap B_\lambda$ for $\lambda \in A$ (we assume that A and B have the same structure semilattice A). Then, each $A_\lambda(P_\lambda)$ [$B_\lambda(Q_\lambda)$] is \mathcal{P} -regular. Let $S(U) = \Sigma\{A_\lambda(P_\lambda) \times_{\mathcal{P}} B_\lambda(Q_\lambda): \lambda \in A\}$, where $U = \Sigma\{P_\lambda \times Q_\lambda$ (cartesian product): $\lambda \in A\}$. Then, of course $S(U)$ is also a cryptogroup under the multiplication $(a, b)(c, d) = (ac, bd)$. Now, let $(e, f) \in P_\lambda \times Q_\lambda$ and $(h, t) \in P_\delta \times Q_\delta$. Then, it is easy to see that $(e, f)(h, t) \in E_S$ and $(e, f)(h, t)(e, f) \in U$. Hence, $S(U)$ is weakly \mathcal{P} -regular, and accordingly \mathcal{P} -regular. This $S(U)$ is called \mathcal{P} -spined product of $A(P)$ and $B(Q)$, and denoted by $A(P) \times_{\mathcal{P}}^{\#} B(Q)$. Now, let $T(V)$ be a \mathcal{P} -regular subsemigroup of $A(P) \times_{\mathcal{P}}^{\#} B(Q)$ such that

- (C.6) (1) the first and second projections of $S(U) = A(P) \times_{\mathcal{P}}^{\#} B(Q)$ are surjective \mathcal{P} -homomorphisms of $T(V)$ onto $A(P)$ and $B(Q)$ respectively, and
 (2) $(a, b) \in T(V)$ implies $(a^{-1}, b^{-1}) \in T(V)$, where a^{-1}, b^{-1} are the group inverses of a, b respectively,

then $T(V)$ is called a \mathcal{P} -subspined product of $A(P)$ and $B(Q)$, and denoted by $A(P) \times_{\mathcal{P}} B(Q)$, etc.

Now, let $S(P)$ be a \mathcal{P} -cryptogroup, and $S \sim \Sigma\{S_\lambda: \lambda \in A\}$ the structure decomposition of S . Let $S_\lambda \cap P = P_\lambda$ for each $\lambda \in A$. Then, $S_\lambda(P_\lambda)$ is a completely simple \mathcal{P} -regular semigroup. Now, $S(P)$ is a band of groups $\{G_\gamma: \gamma \in \Gamma\}$, where Γ is a band and each G_γ is an \mathcal{H} -class (where \mathcal{H} is Green's H -relation). Let $\Gamma \sim \Sigma\{\Gamma_\lambda: \lambda \in A\}$ the structure decomposition of Γ . Let ν be the least strong \mathcal{P} -congruence on $S(P)$. This is given as follows (see [11]): Let ν be the transitive closure of the relation ν° defined by $\nu^\circ = \{(a, b) \in S \times S: V_\nu(a) \cap V_\nu(b) \neq \emptyset\}$. Then, it follows from [12] that ν is the least strong \mathcal{P} -congruence on $S(P)$ which makes $S(P)$ to a regular $*$ -semigroup $S(P; \#) = S(P)/(\nu)_\nu$, where $x\nu = \tilde{x}$ and $\tilde{X} = \{\tilde{x}: x \in X\}$ for any subset X of $S(P)$. Now, $\tilde{S}(\tilde{P}) = \bigcup\{\tilde{G}_\gamma: \gamma \in \Gamma\}$. Further, it follows from [11] that $x \nu y$ implies $x, y \in S_\lambda$ for some $\lambda \in A$. Since a homomorphic image of a completely simple semigroup is completely simple (see [3]), S_λ/ν is completely simple. Therefore, $\tilde{S}(\tilde{P})$ has the structure decomposition $\tilde{S}(\tilde{P}) \sim \Sigma\{\tilde{S}_\lambda(\tilde{P}_\lambda): \lambda \in A\}$, and each $\tilde{S}_\lambda(\tilde{P}_\lambda)$ is a completely simple $*$ -semigroup $\tilde{S}(\tilde{P}_\lambda; \#)$. Since $\tilde{S}(\tilde{P}) = \bigcup\{\tilde{G}_\gamma: \gamma \in \Gamma\}$, $\tilde{S}(\tilde{P})$ is also a band of groups. Hence, $\tilde{S}(\tilde{P}; \#)$ is a $*$ -cryptogroup (that is, a regular $*$ -semigroup which is a cryptogroup). Next, define ρ on $S(P)$ as follows: $x \rho y$ if and only if $x, y \in G_\gamma$ for some $\gamma \in \Gamma$. Let e_γ be the identity of G_γ . Let $x\rho = \bar{x}$ and $\bar{X} = \{\bar{x}: x \in X\}$ for $X \subset S(P)$. Then, it is easy to see that $\bar{S}(\bar{P}) = S(P)/(\rho)_\nu$ is a \mathcal{P} -band, and $\bar{e}_\gamma \bar{e}_\delta = \bar{e}_{\gamma\delta}$. Hence, $\bar{S}(\bar{P}) = \{\bar{e}_\gamma: \gamma \in \Gamma\}$ is isomorphic to Γ . Now, let $x, y \in S_\lambda(P_\lambda)$ and assume that $x(\rho \cap \nu)y$. Then, $x, y \in G_\delta$ for some $\delta \in \Gamma$. Since $xy^{-1} \nu yy^{-1}$, we have $xy^{-1} = e_\delta$, and hence $x = y$. Therefore, $f: S(P) \rightarrow \bar{S}(\bar{P}) \times_{\mathcal{P}} \tilde{S}(\tilde{P}; \#)$ defined by $xf = (\bar{x}, \tilde{x})$ is a \mathcal{P} -isomorphism of $S(P)$ to $S(P)f = \{(\bar{x}, \tilde{x}): x \in S(P)\} \subset \bar{S}(\bar{P}) \times_{\mathcal{P}} \tilde{S}(\tilde{P}; \#)$. Let $S(P)f = T(Q)$, where $Q = \{(\bar{p}, \tilde{p}): p \in P\}$. Then, it is easy to see that $T(Q)$ is a \mathcal{P} -regular subsemigroup of $\bar{S}(\bar{P}) \times_{\mathcal{P}} \tilde{S}(\tilde{P}; \#)$ and is a \mathcal{P} -subspined product of $\bar{S}(\bar{P})$ and $\tilde{S}(\tilde{P}; \#)$. Conversely, let $E(P)$ be a \mathcal{P} -band, and $T(Q; \#)$ a $*$ -cryptogroup. Then, $T(Q; \#)$ is a band Γ of groups $\{T_\gamma: \gamma \in \Gamma\}$. Assume that $E(P)$ and $T(Q; \#)$ have the same structure semilattice A , and $E \sim \Sigma\{E_\lambda: \lambda \in A\}$ and $T \sim \Sigma\{T_\lambda: \lambda \in A\}$ the structure decompositions of E and T respectively, and put $P_\lambda = E_\lambda \cap P$ and $Q_\lambda = Q \cap T_\lambda$ for each $\lambda \in A$. Let $S(U)$ be a \mathcal{P} -subspined product of $E(P)$ and $T(Q; \#)$; that is, $S(U) = E(P) \times_{\mathcal{P}} T(Q; \#)$. Then, $S(U)$ is of course a \mathcal{P} -regular semigroup. For any $e \in E(P)$, there exists $a \in S(U)$ such that $(e, x) = a$ for some $x \in T_\gamma$. Now, let $S_{e,\gamma} = \{(e, x) \in E \times T_\gamma: (e, x) \in S(U)\}$. Let $(e, x), (e, y) \in S_{e,\gamma}$. Then, $(e, x)(e, y) = (e, xy) \in S(U)$. Hence, $(e, x)(e, y) \in S_{e,\gamma}$. Further, e, x have group inverses $e^{-1} = e$ and x^{-1} in E and T_γ respectively. Therefore, $(e, x^{-1}) \in S(U) \cap S_{e,\gamma}$. Thus, $S_{e,\gamma}$ is a group. Hence, $S(U) = \Sigma\{S_{e,\gamma}: e \in E \text{ and } \gamma \in \Gamma\}$ such that $S_{e,\gamma} \neq \emptyset$. Further, for $(e, a) \in S_{e,\gamma}$ and $(f, b) \in S_{f,\delta}$, $(e, a)(f, b) = (ef, ab) \in S_{ef,\gamma\delta}$, that is, $S_{e,\gamma}S_{f,\delta} \subset S_{ef,\gamma\delta}$. Therefore, $S(U)$ is a band of the groups $\{S_{e,\gamma}: e \in E \text{ and } \gamma \in \Gamma \text{ such that } S_{e,\gamma} \neq \emptyset\}$. Thus, $S(U)$ is a \mathcal{P} -cryptogroup.

By the result above, we have:

THEOREM 5.1. *Every \mathcal{P} -cryptogroup is \mathcal{P} -isomorphic to a \mathcal{P} -subspined product $S(U)$*

of a \mathcal{P} -band $E(P)$ and a $*$ -cryptogroup $T(Q; \#)$. Conversely, any \mathcal{P} -subspined product $S(U)$ of a \mathcal{P} -band $E(P)$ and a $*$ -cryptogroup $T(Q; \#)$ is a \mathcal{P} -cryptogroup.

The structure of $*$ -cryptogroups has been clarified in [9]. The theorem above is a generalization of the structure theorem (Theorem 4, [6]) for strictly inversive semigroups (that is, orthodox cryptogroups) to the class of \mathcal{P} -regular cryptogroups. In fact: Let S be an orthodox cryptogroup, and $S \sim \Sigma\{S_\lambda: \lambda \in A\}$ the structure decomposition of S . Then, E_S has the structure decomposition $E_S \sim \Sigma\{E_\lambda: \lambda \in A\}$, where $E_\lambda = S_\lambda \cap E_S$. Further, $S(E_S)$ and $S_\lambda(E_\lambda)$ are \mathcal{P} -regular. Now let $x\rho = \bar{x}$ and $xv = \tilde{x}$ for $x \in S$, and $\bar{X} = \{\bar{x}: x \in X\}$ and $\tilde{X} = \{\tilde{x}: x \in X\}$ for $X \subset S$. Then, $\bar{S}(E_S) = S(E_S)/(\rho)_\mathcal{P}$ is isomorphic to the band E_S . On the other hand, the least strong \mathcal{P} -congruence ν on $S(E_S)$ is the least inverse semigroup congruence on S (see [2], [7]), and hence $\tilde{S}(E_S) = S(E_S)/(\nu)_\mathcal{P}$ is a Clifford semigroup. Further, each $\tilde{S}_\lambda(E_\lambda)$ is a group. Let $T = \{(\bar{x}, \tilde{x}): x \in S\}$. Then, it follows from the result above that S is isomorphic to $T = \bar{S}(E_S) \times_A \tilde{S}(E_S)$. Now, let $T_\lambda = \{(\bar{x}, \tilde{x}): x \in S_\lambda\}$ for $\lambda \in A$. Let $(\bar{x}, \tilde{y}) \in \bar{S}_\lambda \times \tilde{S}_\lambda$. Then, $(\bar{x}, \tilde{y}) = (xx^{-1}yxx^{-1}, xx^{-1}yxx^{-1}) \in T_\lambda$. Therefore, $T_\lambda = \bar{S}_\lambda \times \tilde{S}_\lambda$. Hence, T is the spined product $\bar{S} \times_A \tilde{S}$ of \bar{S} and \tilde{S} . Now, $\bar{S} \cong E_S$. Therefore, S is isomorphic to the spined product of E_S and the Clifford semigroup \tilde{S} . This is just the structure theorem for strictly inversive semigroups given by [6].

As a special case of the theorem above, if $S(P)$ is a completely simple \mathcal{P} -regular semigroup, then the structure semilattice of S consists of a single element. Therefore, we have the following as a corollary to Theorem 5.1:

COROLLARY. *A completely simple \mathcal{P} -regular semigroup $S(P)$ is \mathcal{P} -isomorphic to a \mathcal{P} -subdirect product of a rectangular \mathcal{P} -band $E(Q)$ and a completely simple $*$ -semigroup $T(K; \#)$. Conversely, a \mathcal{P} -subdirect product $S(P)$ of a rectangular \mathcal{P} -band $E(Q)$ and a completely simple $*$ -semigroup $T(K; \#)$ is a completely simple \mathcal{P} -regular semigroup.*

§6. Strongly \mathcal{P} -regular cryptogroups

Let B be a band, and P a C -set in B . Then, $B(P)$ is \mathcal{P} -regular. Let ν be the least strong \mathcal{P} -congruence on $B(P)$. Then, $\tilde{B}(\tilde{P}) = B(P)/(\nu)_\mathcal{P}$ is the regular $*$ -semigroup having \tilde{P} as the projections, where $\tilde{x} = xv$ and $\tilde{X} = \{\tilde{x}: x \in X\}$ for $X \subset B$. Let $Q_p = \{e \in B: \tilde{e} = \tilde{q} \text{ for some } q \in P\}$.

Then,

LEMMA 6.1. *$B(Q_p)$ is strongly \mathcal{P} -regular.*

PROOF. Let $e \in Q_p$. Then, there exists $q \in P$ such that $\tilde{q} = \tilde{e}$. Hence, $q \nu e$, and $q \in P$. Let $f \in V_\mathcal{P}(e)$ in $B(Q_p)$. Then, $\tilde{e}\tilde{f}\tilde{e} \in \tilde{Q}_p = \tilde{P}$ and similary $\tilde{f}\tilde{P}\tilde{e} \in \tilde{P}$. Further, $\tilde{f} \in V(\tilde{e})$. Hence, $\tilde{f} \in V_\mathcal{P}(\tilde{e})$ in $\tilde{B}(\tilde{P})$. Since $\tilde{B}(\tilde{P})$ is a regular $*$ -semigroup, a \mathcal{P} -inverse of \tilde{e} ($= \tilde{q}$) is unique, and hence $\tilde{f} = \tilde{q} = \tilde{e}$. Therefore, $f \in Q_p$. Further, $e\tilde{Q}_p e = \tilde{e}\tilde{P}\tilde{e} = \tilde{q}\tilde{P}\tilde{q} \subset \tilde{P}$, and accordingly $eQ_p e \subset Q_p$. Thus, Q_p is a C -set. Therefore, $B(Q_p)$ is strongly \mathcal{P} -regular.

Conversely,

LEMMA 6.2. *Let $B(U)$ be a strongly \mathcal{P} -regular semigroup, and ν the least strong \mathcal{P} -congruence on $B(U)$. Let $\tilde{B}(\tilde{U}) = B(U)/(\nu)_{\mathcal{P}}$ where $x\nu = \tilde{x}$ and $\tilde{X} = \{\tilde{x} : x \in X\}$ for $X \subset B$. Then, $U = \{x \in B : \tilde{x} = \tilde{u} \text{ for some } u \in U\}$.*

PROOF. This follows from [11].

Thus, we have:

THEOREM 6.3. *Let B be a band, and P a C -set in B . Let ν be the least strong \mathcal{P} -congruence on the \mathcal{P} -band $B(P)$. Let $x\nu = \tilde{x}$ and $\tilde{X} = \{\tilde{x} : x \in X\}$ for $X \subset B$. Let $Q_p = \{x \in B : \tilde{x} = \tilde{q} \text{ for some } q \in P\}$.*

Then, $B(Q_p)$ is strongly \mathcal{P} -regular. Every C -set U such that $B(U)$ is strongly \mathcal{P} -regular is obtained in this fashion.

Next, let S be a cryptogroup. Assume that $S(P)$ is strongly \mathcal{P} -regular. In this case, each \mathcal{H} -class is a group. Of course, S is a band Γ of groups $\{G_\gamma : \gamma \in \Gamma\}$. Let e_γ be the identity of G_γ for each $\gamma \in \Gamma$. Then, $S(P)/(\mathcal{H})_{\mathcal{P}} = \bar{S}(\bar{P})$, where $x\mathcal{H} = \bar{x}$ and $\bar{X} = \{\bar{x} : x \in X\}$ for $X \subset S$, is isomorphic to Γ ; an isomorphism g is given by $\bar{x}g = \gamma$ if $x \in G_\gamma$. Let $A = \{\bar{p}g : p \in P\}$. Then, clearly $\Gamma(A)$ is \mathcal{P} -isomorphic to $\bar{S}(\bar{P})$. Now, let $\bar{p}\mathcal{L}\bar{u}\mathcal{R}\bar{q}$, where $p, u, q \in P$. Since $S(P)$ is strongly \mathcal{P} -regular, $\bar{p}\bar{u} = \bar{p}$ and $\bar{u}\bar{p} = \bar{u}$. Hence, $pu \mathcal{H} p$ and $up \mathcal{H} u$, and accordingly $p\mathcal{L}u$. Similarly, $u \mathcal{R}q$. Hence, there exists $v \in P$ such that $p \mathcal{R}v \mathcal{L}q$. Therefore, $\bar{p} \mathcal{R} \bar{v} \mathcal{L} \bar{q}$. Similarly, $\bar{p} \mathcal{R} \bar{u} \mathcal{L} \bar{q}$ implies that $\bar{p} \mathcal{L} \bar{v} \mathcal{R} \bar{q}$ for some $v \in P$. Thus, $\bar{S}(\bar{P})$ is strongly \mathcal{P} -regular, and hence $\Gamma(A)$ is strongly \mathcal{P} -regular.

From the results above, we easily obtain the following:

THEOREM 6.4. *Let $S(P)$ be a strongly \mathcal{P} -regular semigroup. Then, $S(P)$ is \mathcal{P} -isomorphic to a \mathcal{P} -subspined product of a strongly \mathcal{P} -regular band $T(Q)$ and a $*$ -cryptogroup $W(U; \#)$.*

References

- [1] Clifford, A. H. and Preston, G. B.: The algebraic theory of semigroups, Vol 1, Amer. Math. Soc., Providence, R. I., 1961.
- [2] Hall, T. E.: On regular semigroups whose idempotents form a subsemigroup, Bull. Australian Math. Soc. 1 (1969), 195–208.
- [3] Howie, J. M.: An introduction to semigroup theory, Academic Press, London, 1976.
- [4] Pastijn, F. J. and Petrich, M.: Regular semigroups as extensions, Research Notes in Mathematics 136, Pitman Advanced Publishing Program, Boston, 1985.
- [5] Reilly, N. R.: A class of regular $*$ -semigroups, Semigroup Forum 18 (1979), 385–386.
- [6] Yamada, M.: Strictly inversive semigroups, Bull. Shimane Univ. 13 (1964), 128–138.
- [7] —: On a regular semigroup in which the idempotents form a band, Pacific J. Math. 33 (1970), 261–272.
- [8] —: P -systems in regular semigroups, Semigroup Forum 24 (1982), 173–187.
- [9] —: Construction of a certain class of regular semigroups with special involution, The 1984 Marquette Conference on Semigroups, Marquette Univ., Wisconsin, 1985, 229–240.

- [10] Yamada, M. and Kimura, N.: Note on idempotent semigroups, II, Proc. Japan Acad. **34** (1958), 110–112.
- [11] Yamada, M. and Sen, M. K.: On P -regular semigroups, Proc. of the 11th Symposium on Semigroups, Ritsumeikan Univ., 1988, 3–11.
- [12] —: \mathcal{P} -regularity in semigroups, Mem. Fac. Sci., Shimane Univ. **21** (1987), 47–54.