Publ. Math. Debrecen
73/3-4 (2008), 281–298

The existence of an associate subgroup in normal cryptogroups

By MARIO PETRICH (Brač)

Abstract. Let S be a semigroup. If $a, x \in S$ are such that $a = axa$, then x is an associate of a. A subgroup G of S is an associate subgroup of S if it contains exactly one associate of each element of S. Representing a normal cryptogroup S as a strong semilattice of Rees matrix semigroups, we give necessary and sufficient conditions on S in order for S to have an associate subgroup. Having an associate subgroup is equivalent to admitting a unary operation satisfying three simple axioms. We prove that every maximal subgroup of S is an associate subgroup if and only if S is completely simple. A counterexample shows that the unary semigroups corresponding to two different associate subgroups of (completely simple) S need not be isomorphic. Normal cryptogroups having an associate subgroup are characterized in several ways in the main result of the paper.

1. Introduction and summary

The concept of an associate subgroup was introduced by Blyth, Giraldes and Smith in [1] as a generalization of a notion introduced by Blyth and McFadden in [3]. Let S be a semigroup. For $a, x \in S$ such that $a = axa$, the element x is an *associate* of a. Consider the following condition on a subsemigroup T of S: T contains exactly one associate of every element of S. It is proved in [1] that T must be a maximal subgroup, say G, of S. In such a case, G is termed an *associate subgroup* of S. When S is orthodox and G is also the group of units of S, a structure theorem is proved in [3] for S in terms of a semidirect product of the band of idempotents of S and G. This result is generalized in [1] to the case

Mathematics Subject Classification: 20M10.
Key words and phrases: normal cryptogroup, completely simple semigroup, $*$-semigroup, Rees matrix semigroup, pure, $\mathcal{H}$-surjective, associate subgroup, zenith.

when S is orthodox and has a middle unit. In its turn, this result was generalized by Blyth and Martins in [2] to regular semigroups with a medial idempotent, where e is medial if for any product of idempotents a we have $a = aea$. Even this case does not include such familiar examples as completely simple semigroups.

The situation explained above suggests at least two directions of investigation: either to try to generalize the last of these results or to start from a familiar class of regular semigroups and single out those that admit an associate subgroup. The first option is enhanced by the attractive construction in the structure theorem in [2], whereas the second seems promising if the class in question has a substantial structure theorem. This work is devoted to the second approach for normal cryptogroups (completely regular semigroups S in which $\mathcal{H}$ is a congruence and $S/\mathcal{H}$ is a normal band). In the constellation of manifold choices of classes of regular semigroups, those with an associate subgroup seem to offer a promising case in terms of structure theory.

An associate subgroup of S induces a unary operation so we refer to it as a $*$-semigroup below.

Section 2 consists of a short list of terminology and notation. The general case of $*$-semigroups takes up Section 3 with several lemmas to be used later. The centerpiece of this section is a reformulation of a result in [2] and [4]. Completely simple semigroups are treated in Section 4 with a remarkable result: they are precisely all semigroups in which every maximal subgroup is associate. Section 5 is auxiliary treating certain concepts to be used later. The case of general normal cryptogroups is the subject of Section 6. In particular, it contains several characterizations of normal cryptogroups which admit an associate subgroup including one of them in terms of a subdirect product of a normal band and a completely simple semigroup; these are our main results.

2. Terminology and notation

As a general reference, we recommend the book [6]. In addition, or for emphasis, we now list a few frequently used concepts and notation.

Throughout the paper S denotes an arbitrary semigroup unless specified otherwise. For elements $s, t \in S$, t is an *associate* of s if $s = sts$; if also s is an associate of t, that is $t = tst$ then s and t are *inverses* of each other. Denote by $A(s)$ the set of all associates and by $V(s)$ the set of all inverses of s. A subsemigroup T of S is an *associate subsemigroup* of S if for every $s \in S$, $T \cap A(s)$ contains exactly one element.

We denote by $E(S)$ the set of all idempotents of S, $C(S)$ (the core of S) the subsemigroup of S generated by $E(S)$, $G(S)$ the set of all group elements (completely regular elements) of S, $\mathcal{A}(S)$ the automorphism group of S. For $s \in S$, H_s denotes the $\mathcal{H}$-class of s and if H_s is a group, then s^0 stands for its identity.

The semigroup S is a normal cryptogroup (a normal band of groups) if S is completely regular, that is $S = G(S)$, Green's relation $\mathcal{H}$ is a congruence, that is S is a cryptogroup, and $S/\mathcal{H}$ is a normal band, that is satisfies the identity $axya = ayxa$.

3. Generalities

The following result is essentially known, but we summarize in it the seminal features of an associate subgroup starting with the more general concept of an associate subsemigroup.

Theorem 3.1. *Let T be an associate subsemigroup of a semigroup S.*

(i) *T is a maximal subgroup of S.*

(ii) *The identity z of T is a maximal idempotent of S.*

(iii) *For every $s \in S$, define s^* by the requirement*

$$A(s) \cap T = \{s^*\}. \tag{1}$$

The unary operation $s \to s^*$ satisfies the following axioms:

(A1) $s = ss^*s$,

(A2) $s^*s^{**} = t^{**}t^*$,

(A3) $s = st^*s \implies s^* = t^*$.

In particular, $z = s^*s^{**}$ for all $s \in S$ and for $S^* = \{s^* \mid s \in S\}$, we have $S^* = T$.

Conversely, let S be a semigroup with a unary operation $*$ satisfying axioms (A1)–(A3). *Let $z = s^*s^{**}$ for any $s \in S$. Then H_z is an associate subgroup of S with identity z, and for every $s \in S$, relation* (1) *holds.*

Proof. *Direct part.*

(i) This is the content of ([1],Theorem 2).

(ii) Let $e \in E(S)$ be such that $e \geq z$. Then

$$z = ze = zee^*e = ze^*e = e^*e = e^*ze = e^*z = e^*$$

whence

$$e = ee^*e = eze = z,$$

and z is maximal.

(iii) Let $s, t \in S$. Then $s = ss^*s$ and axiom (A1) holds. Since $s^*, s^{**}, t^*, t^{**} \in H_z$, and by (A1) we have $s^*s^{**}, t^{**}t^* \in E(S)$, we get $s^*s^{**} = t^{**}t^*$ and axiom (A2) holds. If $s = st^*s$, then $t^* \in A(s) \cap H_z = \{s^*\}$ so that axiom (A3) holds as well. The remaining assertions now follow without difficulty.

Converse. The definition of z is justified by axiom (A2). For any $s \in S$, this axiom also implies that

$$z \in s^*S \cap Ss^*, \quad s^* = zs^* = s^*z \in zS \cap Sz$$

and thus $s^* \mathcal{H} z$, that is $s^* \in H_z$. Since $s^* \in A(s)$ by axiom (A1), we get $s^* \in A(s) \cap H_z$.

Let $t \in A(s) \cap H_z$. Then $t \in A(s)$ implies that $s = sts$ and $t \in H_z$ yields $t^* = t^{-1}$ in view of (A1). But then $t = t^{**}$ so that $s = s(t^*)^*s$ and axiom (A3) gives $s^* = (t^*)^* = t$. Therefore $A(s) \cap H_z = \{s^*\}$ which proves that H_z is an associate subgroup of S and relation (1) holds. □

The above theorem is essentially a variant of ([4], Theorem 3.1). It appears convenient to introduce the following

Definition 3.2. If z is an idempotent of a semigroup S and H_z is an associate subgroup of S, call z an *associate idempotent* and the *zenith* of the $*$-operation induced by H_z. By a *$*$-operation* we will mean that axioms (A1)–(A3) are satisfied, in which case S is a *$*$-semigroup.* For brevity we will speak of $*$-bands, normal $*$-cryptogroups, etc.

Lemma 3.3. *Let S and T be $*$-semigroups and $\chi : S \to T$ be a multiplicative homomorphism. Then χ respects the $*$-operations if and only if it respects their zeniths.*

Proof. Let z and w be the zeniths of S and T, respectively.

Direct part. For any $s \in S$, we have

$$z\chi = (s^*s^{**})\chi = (s\chi)^*(s\chi)^{**} = w.$$

Converse. For any $s \in S$, we get $s\chi = (s\chi)(s^*\chi)(s\chi)$ where $s^* \mathcal{H} z$ which implies that $s^*\chi \mathcal{H} z\chi = w$. But then $s^*\chi \in A(s\chi) \cap H_w = \{(s\chi)^*\}$ and thus $s^*\chi = (s\chi)^*$. □

It is of some interest to compare two associate subgroups of the same semigroup.

Proposition 3.4. *Any two associate idempotents of a semigroup S are $\mathcal{D}$-equivalent.*

Proof. Let z and w be associate idempotents of S. Denote by $*$ and $^-$ the corresponding $*$-operations on S relative to z and w, respectively. Then $z = z\overline{z}z$ and $w = ww^*w$, where $\overline{z} \in H_w$ and $w^* \in H_z$. In particular, $\overline{z} = wu$ for some $u \in S$. It follows that $z = zwuz \in zwS$, and trivially $zw \in zS$ so that $z \mathcal{R} zw$. Similarly $w \mathcal{L} zw$ and thus $z \mathcal{R} zw \mathcal{L} w$ so that $z \mathcal{D} w$. □

In particular, any two associate subgroups of S are isomorphic. Also, by Theorem 3.1(ii), in a monoid, its identity is the only possible associate idempotent.

It will be convenient to use the following notation. If S is a $*$-semigroup and $s \in S$, let

$$s^+ = s(ss)^*s.$$

We will need the following result.

Lemma 3.5. *The following conditions on an element a of a semigroup S are equivalent.*

(i) *s is completely regular.*

(ii) *s is contained in a subgroup of S.*

(iii) *$s \in s^2S \cap Ss^2$.*

Proof. See ([6], Proposition II.1.3). □

We will often use the following lemma without express mention.

Lemma 3.6. *Let S be a $*$-semigroup. Then*

$$G(S) = \{s \in S \mid s = ss^+ = s^+s\}.$$

Proof. If $s \in G(S)$, then by Lemma 3.5 we have $s = s^2x = ys^2$ for some $x, y \in S$ and thus

$$s = s^2x = ss(ss)^*ssx = ss(ss)^*s = ss^+$$

and dually $s = s^+s$. Conversely, $s = ss^+ \in s^2S$ and $s = s^+s \in Ss^2$ which by the same reference yields $s \in G(S)$. □

Another result will be needed.

Lemma 3.7. *A semigroup S is completely regular if and only if for every $s \in S$, we have $s \in s^2Ss$.*

Proof. This is the dual of a part of ([6], Theorem II.1.4). □

Corollary 3.8. *Let S be a $*$-semigroup. Then S is completely regular if and only if $s = ss^+$ (equivalently $s = s^+s$) for every $s \in S$.*

Proof. The direct part follows from Lemma 3.6. For the converse, assume that $s = ss^+$ for all $s \in S$. Then $s \in s^2Ss$ and Lemma 3.7 implies that S is completely regular. The statement in the parentheses follows dually. □

4. Completely simple semigroups

From the development of the concept of an associate subgroup one gets the impression that the motivation for it was the desire that, in the original setting, the group of units of an orthodox semigroup and its band of idempotents determine the structure of the entire semigroup [3]. The first generalization substitutes the identity element by a middle unit [1]. The second generalization further weakens these hypotheses [2]. In each of these cases, the authors arrive at a lucid structure theorem. The main result in this section points in a different direction: the concept of an associate subgroup can be regarded as a generalization of completely simple semigroups.

In the preceding section we established the relationship of semigroups with an associate subgroup and a class of unary semigroups which we dubbed $*$-semigroups. We tackle here the problem of necessary and sufficient conditions on an abstract semigroup S in order for S to have all its maximal subgroups associate.

Theorem 4.1. *The following conditions on a semigroup S are equivalent.*

(i) *S is regular and every maximal subgroup of S is an associate subgroup.*

(ii) *S is completely simple.*

(iii) *S admits a unary operation $s \to s^*$ satisfying axiom $s = (st)(st)^*s$.*

In such a case, S admits a unary operation making it a $*$-semigroup.

Proof. (i) $\Longrightarrow$ (ii). By Theorem 3.1(ii), every idempotent of S is maximal. But then all idempotents of the regular semigroup S are primitive and thus S is completely simple.

(ii) $\Longrightarrow$ (i). We may set $S = \mathcal{M}(I, G, \Lambda; P)$. Fix

$$H_{j\mu} = \{(j, h, \mu) \mid h \in G\}.$$

For any $(i, g, \lambda) \in S$, the equation

$$(i, g, \lambda) = (i, g, \lambda)(j, h, \mu)(i, g, \lambda) = (i, gp_{\lambda j}hp_{\mu i}g, \lambda)$$

has a unique solution $(j, p_{\lambda j}^{-1}g^{-1}p_{\mu i}^{-1}, \mu)$. Therefore $H_{j\mu}$ is an associate subgroup of S.

(ii) $\Longrightarrow$ (iii). We may set $S = \mathcal{M}(I, G, \Lambda; P)$ where P is normalized at 1. For every $s = (i, g, \lambda) \in S$, let $s^* = (1, g^{-1}, 1)$. Straightforward verification will show that that the given identity is satisfied.

(iii) $\Longrightarrow$ (ii). Setting $s = t$ in the given identity, by Lemma 3.7 we conclude that S is completely regular. The given identity also implies that $s \in StS$ for any $s, t \in S$ and thus S is simple. Therefore S is completely simple.

Simple verification will show that s^* defined in (ii) $\Longrightarrow$ (iii) above satisfies axioms (A1)–(A3). □

It is part (iii) which locates the completely simple case among $*$-semigroups. The theorem shows that completely simple semigroups form a variety in the context of $*$-semigroups.

As a consequence of Proposition 3.4, any two associate subgroups of a semigroup S are isomorphic. This follows trivially from Theorem 4.1 for completely simple semigroups. It seems natural to ask whether the $*$-semigroups resulting from two associate subgroups are $*$-isomorphic. We will see below that this fails even for completely simple semigroups.

Let $I = \Lambda = \{1, 2\}$, G be a group and $P = \left[\begin{smallmatrix} e & e \\ e & q \end{smallmatrix}\right]$ where e is the identity of G and q will be specified later. Let χ be an automorphism of the semigroup $S = \mathcal{M}(I, G, \Lambda; P)$. Recall from ([6], Section III.3) that

$$\chi : \mathcal{M}(I, G, \Lambda; P) \longrightarrow \mathcal{M}(J, H, M; Q)$$

is a homomorphism if there exist mappings

$$\varphi : I \to J, \quad \psi : \Lambda \to M, \quad u : I \to H, \quad v : \Lambda \to H$$

and a homomorphism $\omega : G \to H$ such that $p_{\lambda i}\omega = v_\lambda q_{\lambda\psi, i\varphi} u_i$ and

$$(i, g, \lambda)\chi = (i\varphi, u_i(g\omega)v_\lambda, \lambda\psi) \quad (i \in I,\ g \in G,\ \lambda \in \Lambda).$$

Recall that $(\varphi, u, \omega, v, \psi)$ is called an h-quintuple. In this case, φ and ψ are permutations of the set $\{1, 2\}$, ω is an automorphism of G, and $u : i \to u_i$ and $v : \lambda \to v_\lambda$ are functions from $\{1, 2\}$ to G.

Suppose that the $*$-semigroups induced by the maximal (i.e. associate) subgroups H_{11} and H_{12} are $*$-isomorphic. By Lemma 3.3, there is an automorphism χ of S such that $(1, e, 1)\chi = (1, e, 2)$. In the above notation $\varphi = (1)$ and $\psi = (12)$ so that the condition on these parameters has the form

$$p_{\lambda i}\omega = v_\lambda p_{\lambda\psi, i} u_i \qquad (i, \lambda \in \{1, 2\}).$$

For special values of i and λ, we get

$$\begin{aligned}
&\lambda = i = 1 : e = v_1 u_1, \\
&\lambda = 2, i = 1 : e = v_2 u_1, \\
&\lambda = 1, i = 2 : e = v_1 q u_2, \\
&\lambda = i = 2 : q\omega = v_2 u_2.
\end{aligned}$$

From the first two equations, we obtain $v_1 = v_2$, from the third $u_2 = q^{-1}v_1^{-1}$ and using this in the fourth yields

$$q\omega = v_1 q^{-1} v_1^{-1}.$$

Letting $\pi_g : x \to g^{-1}xg$ ($x \in G$) for any $g \in G$, we obtain

$$q\omega\pi_{v_1} = (v_1 q^{-1} v_1^{-1})\pi_{v_1} = q^{-1},$$

where $\omega\pi_{v_1} \in \mathcal{A}(G)$. Letting $\tau = \omega\pi_{v_1}$, our hypothesis implies the existence of an automorphism τ of G and an element q of G such that $q\tau = q^{-1}$.

Mr. Peter Campbell then of the University of St. Andrews, Scotland, has kindly provided examples of groups G in which there exists an element q such that $q\tau \neq q^{-1}$ for all automorphisms τ of G. For this q in our sandwich matrix the $*$-semigroups induced by H_{11} and H_{12} are not $*$-isomorphic.

In detail, some of his findings are: "the group of smallest order with this property has 20 elements with the presentation $\langle s, t \mid s^5 = 1,\ t^4 = 1,\ st = ts^2\rangle$ or equally $\langle s, t \mid s^2tsts^{-1}t = 1,\ t^2 = 1\rangle$. A list of permutation generators is $[(1, 2, 4, 5, 3), (2, 4, 3, 5)]$. When considering it as a permutation group the calculations suggest that any of the ten 4-cycles in the group e.g. $(2, 5, 3, 4)$, $(1, 3, 2, 4)$ etc. satisfy this property. There were also groups of order 21 and 27 satisfying this property".

Any smaller format of sandwich matrix would be 1×1, 1×2, 1×3, 2×1, 3×1 giving a rectangular group. There are no counterexamples among rectangular groups. Hence the smallest example of a completely simple semigroup with nonisomorphic $*$-semigroups is of order $4 \times 20 = 80$.

5. Purity, injectivity and surjectivity

We review here some concepts. They will be used subsequently. We then briefly establish certain relationships among some of them.

The setting is: S and T are regular semigroups and $\chi : S \to T$ is a homomorphism. We denote by $\overline{\chi}$ the congruence on S induced by χ. The homomorphism χ is

pure	if $a \in S,\ a\chi \in E(T),$ then $a \in E(S)$,
$\mathcal{H}$*-injective*	if $a, b \in S,\ a\,\mathcal{H}\,b, a\chi = b\chi,$ then $a = b$,
$\mathcal{H}$*-surjective*	if $a \in S,\ b \in T, a\chi\,\mathcal{H}\,b$ implies the existence of $x \in S$ such that $x\,\mathcal{H}\,a, x\chi = b$.

The first concept was introduced in [5]; the last one is new. Recall that the natural partial order is defined by

$$a \leq b \text{ if } a = eb = bf \quad \text{for some } e, f \in E(S).$$

Lemma 5.1. *Let $\chi : S \to T$ be a homomorphism of regular semigroups.*

(i) *If S and T are completely regular, then χ is pure if and only if it is $\mathcal{H}$-injective.*

(ii) *Let $S = \mathcal{M}(I, G, \Lambda; P)$, $T = \mathcal{M}(J, H, M; Q)$ and $\chi = \chi(\varphi, u, \omega, v, \psi)$. Then*

 (a) *χ is $\mathcal{H}$-injective if and only if ω is ($\mathcal{H}$-)injective.*

 (b) *χ is $\mathcal{H}$-surjective if and only if ω is ($\mathcal{H}$-)surjective.*

Proof. (i) Assume that χ is pure and $a\,\mathcal{H}\,b$, $a\chi = b\chi$. Then $a\,\overline{\chi}\,b$ whence $ab^{-1}\,\overline{\chi}\,b^0$ so that $(ab^{-1})\chi = b^0\chi \in E(T)$. By hypothesis, $ab^{-1} \in E(S)$. But then $a\,\mathcal{H}\,b$ implies $a = b$. Thus χ is $\mathcal{H}$-injective.

Conversely, suppose that χ is $\mathcal{H}$-injective and let $a\chi = f \in E(T)$. Then $a^0\chi = (a\chi)^0 = f^0 = f$ and hence $a\chi = a^0\chi$. Since $a\,\mathcal{H}\,a^0$, the hypothesis implies that $a = a^0$. Hence χ is pure.

(ii)(a) Assume that χ is $\mathcal{H}$-injective and $g\omega = 1$. For any $i \in I$, $\lambda \in \Lambda$, we get $(i, g, \lambda)\chi = (i, 1, \lambda)\chi$. Now $(i, g, \lambda)\ \mathcal{H}\ (i, 1, \lambda)$ by hypothesis implies that $(i, g, \lambda) = (i, 1, \lambda)$ so that $g = 1$. Hence ω is injective.

Conversely, suppose that ω is injective and $(i, g, \lambda)\chi = (i, h, \lambda)\chi$. Hence $g\omega = h\omega$ which by hypothesis yields $g = h$, and thus $(i, g, \lambda) = (i, h, \lambda)$. Therefore χ is $\mathcal{H}$-injective.

(b) Assume that χ is $\mathcal{H}$-surjective and let $h \in H$. Let $a = (i, g, \lambda) \in S$ be arbitrary. For $b = (i\varphi, u_i h v_\lambda, \lambda\psi)$ we have $a\chi\ \mathcal{H}\ b$. By hypothesis, there exists $x = (i, t, \lambda)$ such that $x\chi = b$ whence $u_i(t\omega)v_\lambda = u_i h v_\lambda$ and thus $t\omega = h$.

Conversely, suppose that ω is surjective and let $a = (i, g, \lambda) \in S$ and $b = (j, h, \mu) \in T$ be such that $a\chi \,\mathcal{H}\, b$. Then $i\varphi = j$ and $\lambda\psi = \mu$. For $x\omega = u_i^{-1} h v_\lambda^{-1}$ and $c = (i, x, \lambda)$, we have $c \,\mathcal{H}\, a$ and $c\chi = b$. Therefore χ is $\mathcal{H}$-surjective. $\square$

A regular semigroup S is

pure	if $e \in E(S),\ a \in S,\ e \leq a \implies a \in E(S)$,
$\mathcal{H}$-surjective	if $a \geq b,\ b \,\mathcal{H}\, c$ implies the existence of x such that $x \,\mathcal{H}\, a,\ x \geq c$.

The first concept was introduced in [5]; the second one is known as the link property.

Lemma 5.2. *Let S and T be disjoint completely simple semigroups and V be an ideal extension of T by S^0 determined by a homomorphism $\chi : S \to T$.*

(i) *V is pure if and only if χ is pure.*

(ii) *V is $\mathcal{H}$-surjective if and only if χ is $\mathcal{H}$-surjective.*

Proof. (i) This is a special case of ([5], Corollary 3.5).
(ii) Straightforward. $\square$

In this context, the concept of $\mathcal{H}$-minorization in completely regular semigroups could be termed *$\mathcal{H}$-injectivity.*

6. Normal cryptogroups

We now address the problem: which normal cryptogroups have an associate subgroup? Equivalently, which ones contain an associate idempotent or admit the structure of a $*$-semigroup? This problem for completely simple semigroups had an easy solution in Section 4. Here the situation is more complex, but as we will see presently, still manageable. We will represent our semigroup as a strong semilattice of Rees matrix semigroups, and the needed structure homomorphisms in terms of h-quintuples. All of these parameters will come into play pointing as to possible complications if we want to consider more general semigroups. We will obtain several characterizations of normal cryptogroups with an associate subgroup one of which is as a subdirect product of a normal band and a completely simple semigroup. We will construct such subdirect products. We shall use freely Theorem 3.1 to simultaneously consider associate subgroups or $*$-operations.

We will consistently represent a normal cryptogroup S in the form $[Y; S_\alpha, \chi_{\alpha,\beta}]$. Another result will be needed.

Lemma 6.1. *Let S be a semigroup. Then $S \cong [Y; S_\alpha, \chi_{\alpha,\beta}]$ where S_α is completely simple for every $\alpha \in Y$ and $\chi_{\alpha,\beta}$ is pure for all $\alpha \geq \beta$ if and only if S is a subdirect product of a normal band and a completely simple semigroup.*

Proof. See ([6], Theorem IV.3.3). □

Theorem 6.2. *Let $S = [Y; S_\alpha, \chi_{\alpha,\beta}]$ be a normal cryptogroup, where*

$$S_\alpha = \mathcal{M}(I_\alpha, G_\alpha, \Lambda_\alpha; P^\alpha) \qquad (\alpha \in Y),$$
$$\chi_{\alpha,\beta} = \chi(\varphi_{\alpha,\beta}, u^{\alpha,\beta}, \omega_{\alpha,\beta}, v^{\alpha,\beta}, \psi_{\alpha,\beta}) \qquad (\alpha \geq \beta).$$

Then the following statements are equivalent.

(i) *S has an associate subgroup.*

(ii) *Y has an identity element ϵ and all $\omega_{\epsilon,\alpha}$ are isomorphisms.*

(iii) *Y is a monoid and all $\omega_{\alpha,\beta}$ are isomorphisms.*

(iv) *$S/\mathcal{D}$ is a monoid and S is pure and $\mathcal{H}$-surjective.*

(v) *S is an $\mathcal{H}$-surjective subdirect product of a normal band B such that $B/\mathcal{D}$ is a monoid and a completely simple semigroup M.*

In such a case, G is an associate subgroup of S if and only if G is a maximal subgroup of S_ϵ. If $G = H_{k\nu}$ and $(i, g, \lambda) \in S_\alpha$, then

$$(i, g, \lambda)^* = (k, (v_\nu^{\epsilon,\alpha} p^\alpha_{\nu\psi_{\epsilon,\alpha},i} g p^\alpha_{\lambda,k\varphi_{\epsilon,\alpha}} u_k^{\epsilon,\alpha})^{-1} \omega^{-1}_{\epsilon,\alpha}, \nu).$$

Moreover, for every $\alpha \in Y$ and $e \in E(S_\alpha)$, H_e is an associate subgroup of S_α, $\cup_{\beta \leq \alpha} S_\beta$ and $\cup_{f \leq e} H_f$.

Proof. (i) $\Longrightarrow$ (ii). Let $z = (k, p^{-1}_{\nu k}, \nu) \in S_\epsilon$ be an associate idempotent of S. Axiom (A1) implies that ϵ is the identity of Y. Let $s = (i, g, \lambda) \in S_\alpha$. Then $s^* = (k, h, \nu)$ for some $h \in G_\epsilon$. First note that

$$ss^* = (s\chi_{\alpha,\alpha\epsilon})(s^*\chi_{\epsilon,\alpha\epsilon}) = (s\chi_{\alpha,\alpha})(s^*\chi_{\epsilon,\alpha}) = s(s^*\chi_{\epsilon,\alpha}).$$

Omitting sub- and superscripts, we get by axiom (A1)

$$\begin{aligned}(i, g, \lambda) &= (i, g, \lambda)(k, h, \nu)(i, g, \lambda) = (i, g, \lambda)(k\varphi, u_k(h\omega)v_\nu, \nu\psi)(i, g, \lambda)\\ &= (i, g p_{\lambda,k\varphi} u_k (h\omega) v_\nu p_{\nu\psi,i} g, \lambda)\end{aligned}$$

whence $h\omega = (v_\nu p_{\nu\psi,i} g p_{\lambda,k\varphi} u_k)^{-1}$. Now given $t \in G_\alpha$, let $g = (p_{\lambda,k\varphi} u_k t v_\nu p_{\nu\psi,i})^{-1}$. By the above, for this g there exists a unique $h \in G_\epsilon$ such that $h\omega = t$. Therefore $\omega_{\epsilon,\alpha}$ is an isomorphism of G_ϵ onto G_α.

(ii) $\Longrightarrow$ (iii). First let $\alpha \geq \beta \geq \gamma$ in Y. We simplify the notation by writing

$$\chi_{\alpha,\beta} = \chi(\varphi, u, \omega, v, \psi),\ \chi_{\beta,\gamma} = \chi(\varphi', u', \omega', v', \psi'),\ \chi_{\alpha,\gamma} = \chi(\varphi'', u'', \omega'', v'', \psi'').$$

For any $(i, g, \lambda) \in S_\alpha$, we obtain

$$\begin{aligned}(i, g, \lambda)\chi_{\alpha,\beta}\chi_{\beta,\gamma} &= (i\varphi\varphi', u'_{i\varphi}(u_i\omega')(g\omega\omega')(v_\lambda\omega')v'_{\lambda\psi}, \lambda\psi\psi'),\\ (i, g, \lambda)\chi_{\alpha,\gamma} &= (i\varphi'', u''_i(g\omega'')v''_\lambda, \lambda\psi'')\end{aligned}$$

and thus

$$u'_{i\varphi}(u_i\omega')(g\omega\omega')(v_\lambda\omega')v'_{\lambda\psi} = u''_i(g\omega'')v''_\lambda. \tag{2}$$

For g the identity of G_α, this yields

$$u'_{i\varphi}(u_i\omega')(v_\lambda\omega')v'_{\lambda\psi} = u''_i v''_\lambda$$

whence

$$(u''_i)^{-1}u'_{i\varphi}(u_i\omega') = v''_\lambda(v'_{\lambda\psi})^{-1}(v_\lambda\omega')^{-1}.$$

The left hand side depends only on i and the right hand side only on λ. Hence both sides are equal to some constant c. It follows that

$$u''_i c = u'_{i\varphi}(u_i\omega'), \quad c^{-1}v''_\lambda = (v_\lambda\omega')v'_{\lambda\psi}$$

which together with (2) yields

$$u''_i c(g\omega\omega')c^{-1}v''_\lambda = u''_i(g\omega'')v''_\lambda.$$

After cancelation, we obtain $g\omega\omega' = (g\omega'')\pi_c$ where π_c is the inner automorphism $t \to c^{-1}tc$ of G_γ induced by c. Therefore $\omega\omega' = \omega''\pi_c$. In the special case $\epsilon \geq \alpha \geq \beta$, we get $\omega_{\epsilon,\alpha}\omega_{\alpha,\beta} = \omega_{\epsilon,\beta}\pi_c$ whence $\omega_{\alpha,\beta} = \omega_{\epsilon,\alpha}^{-1}\omega_{\epsilon,\beta}\pi_c$. Since the mapping on the right hand side of this equation is an isomorphism, $\omega_{\alpha,\beta}$ is an isomorphism as well.

(iii) $\Longrightarrow$ (iv). By Lemma 5.1, each $\chi_{\alpha,\beta}$ is pure. Since each S_α is (trivially) pure, ([5], Proposition 3.4) implies that S is pure. By Lemma 5.1, each $\chi_{\alpha,\beta}$ is $\mathcal{H}$-surjective. Since for $a \in S_\alpha$, $b \in S_\beta$, $a \geq b$ if and only if $\alpha \geq \beta$ and $b = a\chi_{\alpha,\beta}$, and $\mathcal{H}\mid_{S_\alpha} = \mathcal{H}_{S_\alpha}$, $\mathcal{H}$-surjectivity of all $\chi_{\alpha,\beta}$ implies $\mathcal{H}$-surjectivity of S itself.

(iv) $\Longrightarrow$ (v). As above, in the opposite direction, purity of S implies purity of all $\chi_{\alpha,\beta}$. Now Lemma 6.1 implies that S is a subdirect product of a normal band B and a completely simple semigroup M. Here B is a homomorphic image of S, hence $S/\mathcal{D}$ being a monoid implies that also $B/\mathcal{D}$ is a monoid.

(v) $\Longrightarrow$ (i). Let z be an element of the $\mathcal{D}$-class of B corresponding to the identity of $B/\mathcal{D}$. Then $(z, c) \in S$ for some $c \in M$. Let $g \in H_c$. Then $(x, g) \in S$

for some $x \in B$. Since S is completely regular, we have $(x, g)^0 = (x, g^0) \in S$ where $g^0 = c^0$. Next

$$\begin{aligned} (zxz, g^0) &= (z, c^0)(x, g^0)(z, c^0) \in S, \\ (zxz, g) &= (z, c^0)(x, g)(z, c^0) \in S, \end{aligned}$$

so

$$\begin{tikzcd} (z, g^0) \arrow[d, no head] & \mathcal{H} & (z, g) \arrow[d, no head, dashed] \\ (zxz, g^0) & \mathcal{H} & (zxz, g) \end{tikzcd}$$

and by $\mathcal{H}$-surjectivity, we get $(z, g) \in S$. Thus $\{z\} \times H_c \subseteq S$. Now $\{z\}$ is an associate subgroup of B and H_c is an associate subgroup of M, see Theorem 4.1. Expressing this in terms of $*$-operations, in view of the coordinatewise multiplication it shows that $\{z\} \times H_c$ is an associate subgroup of S.

Let G be an associate subgroup of S. By Theorem 3.1(ii), its identity e is a maximal idempotent of S so that $G \subseteq S_\epsilon$, where ϵ is the identity of Y. By the same reference, G is a maximal subgroup of S and thus a maximal subgroup of S_ϵ.

Conversely, let G be a maximal subgroup of S_ϵ. Then $G = H_{k\nu}$ for some $k \in I_\epsilon$ and $\nu \in \Lambda_\epsilon$ in the usual notation. For $(i, g, \lambda) \in S_\alpha$, it remains to show that the equation

$$(i, g, \lambda) = (i, g, \lambda)(k, h, \nu)(i, g, \lambda)$$

has a unique solution for $h \in G_\epsilon$ as indicated in the statement of the theorem. We simplify the notation and calculate

$$\begin{aligned} (i, g, \lambda)(k, h, \nu)(i, g, \lambda) &= (i, g, \lambda)[(k, h, \nu)\chi](i, g, \lambda) \\ &= (i, g, \lambda)(k\varphi, u_k(h\omega)v_\nu, \nu\psi)(i, g, \lambda) \\ &= (i, gp_{\lambda, k\varphi}u_k(h\omega)v_\nu p_{\nu\psi, i}g, \lambda) = (i, g, \lambda) \\ &\Longleftrightarrow gp_{\lambda, k\varphi}u_k(h\omega)v_\nu p_{\nu\psi, i}g = g \\ &\Longleftrightarrow p_{\lambda, k\varphi}u_k(h\omega)v_\nu p_{\nu\psi, i} = g^{-1} \\ &\Longleftrightarrow u_k^{-1}p_{\lambda, k\varphi}^{-1}g^{-1}p_{\nu\psi, i}^{-1}v_\nu^{-1} = h\omega \\ &\Longleftrightarrow h = (u_k^{-1}p_{\lambda, k\varphi}^{-1}g^{-1}p_{\nu\psi, i}^{-1}v_\nu^{-1})\omega^{-1}. \end{aligned}$$

This proves the first two additional assertions of the theorem. These statements imply the final claims of the theorem since all three semigroups stated satisfy part (ii) of the theorem. $\square$

Corollary 6.3. *Any two maximal subgroups of a normal $*$-cryptogroup are isomorphic.*

Another result will be useful.

Lemma 6.4. *On $S = [Y; S_\alpha, \chi_{\alpha,\beta}]$ where S_α is completely simple for every $\alpha \in Y$, define a relation θ_S by: for $a \in S_\alpha$ and $b \in S_\beta$, let*

$$a \; \theta_S \; b \Longleftrightarrow a\chi_{\alpha,\gamma} = b\chi_{\beta,\gamma} \quad \text{for some } \gamma \leq \alpha\beta.$$

Then θ_S is the least completely simple congruence on S.

Proof. See ([6], Lemma IV.3.2). □

We will need the next lemma only for the band case but prove it in full generality.

Lemma 6.5. *Let $S = [Y; S_\alpha, \chi_{\alpha,\beta}]$ be a normal $*$-cryptogroup. Then θ_S preserves the $*$-operation.*

Proof. Let $s = (i, g, \lambda) \in S_\alpha$ and $t = (j, h, \mu) \in S_\beta$ and assume that for some $\gamma \leq \alpha\beta$, we have $s\chi_{\alpha,\gamma} = t\chi_{\beta,\gamma}$. We apply Theorem 6.2. In particular, Y has an identity ϵ, so that the zenith $z = (k, p_{\nu k}^{-1}, \nu)$ of S is an element of S_ϵ. Further notation:

$$\chi_{\epsilon,\alpha} = \chi(\varphi, u, \omega, v, \psi), \qquad \chi_{\epsilon,\beta} = \chi(\varphi', u', \omega', v', \psi'),$$
$$\chi_{\alpha,\gamma} = \chi(\varphi'', u'', \omega'', v'', \psi''), \qquad \chi_{\beta,\gamma} = \chi(\varphi''', u''', \omega''', v''', \psi''').$$

The hypothesis implies

$$(i\varphi'', u_i''(g\omega'')v_\lambda'', \lambda\psi'') = (j\varphi''', u_j'''(h\omega''')v_\mu''', \mu\psi''')$$

so that

$$i\varphi'' = j\varphi''', \quad u_i''(g\omega'')v_\lambda'' = u_j'''(h\omega''')v_\mu''', \quad \lambda\psi'' = \mu\psi'''. \tag{3}$$

Next

$$\begin{aligned} s^*\chi_{\epsilon,\gamma} &= (k, (v_\nu p_{\nu\psi,i} g p_{\lambda,k\varphi} u_k)^{-1}\omega^{-1}, \nu)\chi_{\epsilon,\alpha}\chi_{\alpha,\gamma} \\ &= (k\varphi, p_{\lambda,k\varphi}^{-1} g^{-1} p_{\nu\psi,i}^{-1}, \nu\psi)\chi_{\alpha,\gamma} \\ &= (k\varphi\varphi'', u_{k\varphi}''(p_{\lambda,k\varphi}^{-1} g^{-1} p_{\nu\psi,i}^{-1})\omega'' v_{\nu\psi}'', \nu\psi\psi''). \end{aligned} \tag{4}$$

and analogously

$$t^*\chi_{\epsilon,\gamma} = (k\varphi'\varphi''', u_{k\varphi'}'''(p_{\mu,k\varphi'}^{-1} h^{-1} p_{\nu\psi',j}^{-1})\omega''' v_{\nu\psi'}''', \nu\psi'\psi'''). \tag{5}$$

Since $s^* \mathcal{H} t^*$ and $\chi_{\epsilon,\gamma}$ preserves $\mathcal{H}$-classes, we get

$$k\varphi\varphi'' = k\varphi'\varphi''', \quad \nu\psi\psi'' = \nu\psi'\psi''' \tag{6}$$

Using the condition in the definition of an h-quintuple, we obtain

$$\begin{aligned} u''_{k\varphi}(p^{-1}_{\lambda,k\varphi}g^{-1}p^{-1}_{\nu\psi,i})\omega''v''_{\nu\psi} &= u''_{k\varphi}(p_{\lambda,k\varphi}\omega'')^{-1}(g\omega'')^{-1}(p_{\nu\psi,i}\omega'')^{-1}v''_{\nu\psi} \\ &= u''_{k\varphi}(v''_{\lambda}p_{\lambda\psi'',k\varphi\varphi''}u''_{k\psi})^{-1}(g\omega'')^{-1}(v''_{\nu\psi}p_{\nu\psi\psi'',i\varphi''}u''_{i})^{-1}v''_{\nu\psi} \\ &= p^{-1}_{\lambda\psi'',k\varphi\varphi''}\big[(v''_{\lambda})^{-1}(g\omega'')^{-1}(u''_{i})^{-1}\big]p^{-1}_{\nu\psi\psi'',i\varphi''}, \end{aligned} \tag{7}$$

and similarly

$$\begin{aligned} &u'''_{k\varphi'}(p^{-1}_{\mu,k\varphi'}h^{-1}p^{-1}_{\nu\psi,j})\omega'''v_{\nu\psi'} \\ &= p^{-1}_{\mu\psi''',k\varphi'\varphi'''}[(v'''_{\mu})^{-1}(h\omega''')^{-1}(u'''_{j})^{-1}]p^{-1}_{\nu\psi'\psi''',j\varphi'''}. \end{aligned} \tag{8}$$

The first and the third entries of (4) and (5) are equal by (6). The second entries of (4) and (5) equal (7) and (8), respectively. The latter two are equal in view of (3) and (6). Therefore (4) and (5) are equal which proves that θ_S preserves the $*$-operation. □

Lemma 6.6. *The congruence θ_S in Lemma 6.4 admits the following equivalent formulation:*

$$a\ \theta_S\ b \Longleftrightarrow a \geq c,\ b \geq c \quad \text{for some } c \in S.$$

Proof. This follows from the fact that for $a \in S_\alpha$ and $b \in S_\beta$,

$$a \geq b \Longleftrightarrow \alpha \geq \beta \quad \text{and} \quad a\chi_{\alpha,\beta} = b.$$ □

Lemma 6.7. *A regular subsemigroup of a completely regular semigroup is itself completely regular.*

Proof. See ([6], Lemma II.3.7). □

Next we give a construction of subdirect products which occur in Theorem 6.2(v). We denote by $\mathcal{N}B^*$, $\mathcal{R}B^*$ and $\mathcal{C}S^*$ the classes of $*$-semigroups which are normal bands, rectangular bands and completely simple semigroups, respectively. By a $*$-band we mean a band which is a $*$-semigroup.

Theorem 6.8. *Let* $B = [Y; B_\alpha, \chi_{\alpha,\beta}] \in \mathcal{NB}^*$ *with* z *as its zenith. Then* $\theta = \theta_B$ *is a* $*$*-congruence on* B *and* $B/\theta \in \mathcal{RB}^*$*. Let* $M \in \mathcal{CS}^*$ *and* A *be a subdirect product of* B/θ *and* M *as* $*$*-semigroups. Define*

$$S = \{(x, a) \in B \times M \mid (x\theta, a) \in A\},$$
$$(x, a)^* = (z, a^*) \qquad ((x, a) \in S).$$

Then S *is* $\mathcal{H}$*-surjective and a subdirect product of* B *and* M *as* $*$*-semigroups.*

Conversely, every $\mathcal{H}$*-surjective* $*$*-semigroup* S *which is a subdirect product of a normal* $*$*-band and a completely simple* $*$*-semigroup is* $*$*-isomorphic to one constructed above.*

Proof. *Direct part.* That θ is a $*$-congruence on B follows from Lemmas 6.4 and 6.5. Hence $B/\theta \in \mathcal{RB}^*$. Clearly $z\theta$ is the zenith of B/θ. Since A is a subdirect product of B/θ and M as $*$-semigroups, S is closed under both multiplication and unary operation and is a subdirect product of B and M under multiplication. In $B/\theta \times M$, the unary operation is by coordinates, so $(x\theta, a)^* = (z\theta, a^*)$. The above definition of $(x, a)^*$ now yields that S is also a subdirect product of B and M as $*$-semigroups.

Let $(x, a), (y, b), (u, c) \in S$ be such that $(x, a) \geq (y, b)\ \mathcal{H}\ (u, c)$. Then $a \geq b$ and thus $a = b$ since $M \in \mathcal{CS}^*$ and $y\ \mathcal{H}\ u$ whence $y = u$ since $B \in \mathcal{NB}^*$. Also $x \geq y$ and $b\ \mathcal{H}\ c$. The former implies that $x\theta = y\theta$. From

$$(x\theta, a), (y\theta, b), (u\theta, c) \in A$$

we deduce that $(x\theta, c) \in A$ and thus $(x, c) \in S$. Furthermore, $(u, c) \leq (x, c)\ \mathcal{H}\ (x, a)$ and S is $\mathcal{H}$-surjective.

Converse. We assume that $S \subseteq B \times M$ is a subdirect product and is $\mathcal{H}$-surjective. For every $x \in B$, let

$$M_x = \{a \in M \mid (x, a) \in S\}.$$

Since B is a band and S is a subdirect product, for every $x \in B$, M_x is a subsemigroup of M, $M_x M_y \subseteq M_{xy}$, $\bigcup_{x\in B} M_x = M$, $a^* \in M_z$ for all $a \in M$. For any $s \in S$, by Corollary 3.8, we have

$$s = ss^+ = ss(ss)^* s^+ s = s[s(ss)^* s(ss)^* s]s$$

and thus for any $(x, a) \in S$, we obtain

$$\begin{aligned}(x, a) &= (x, a)[(x, a)(z, (aa)^*)(x, a)(z, (aa)^*)(x, a)](x, a)\\ &= (x, a)(x, a(aa)^* a(aa)^* a)(x, a)\end{aligned}$$

which implies that M_x is regular. By Lemma 6.7, we conclude that M_x is completely regular and thus also completely simple. Therefore the mapping $x \to M_x$ maps B into the partially ordered set $\mathcal{S}(M)$ of completely simple subsemigroups of M.

Assume now that for $x, y \in B$ we have $x \geq y$ and $a \in M_x$. Then $(y, b) \in S$ for some $b \in M$ and

$$((x,a)(y,b)(x,a))^0 = (xyx, aba)^0 = (y, (aba)^0) = (y, a^0)$$

so that $(y, a^0) \in S$ and thus $(y, a) = (x, a)(y, a^0) \in S$. Therefore $a \in M_y$ which proves

$$x \geq y \implies M_x \subseteq M_y. \tag{9}$$

By hypothesis, S is $\mathcal{H}$-surjective, that is, given $(x, a) \geq (y, b)\ \mathcal{H}\ (u, c)$ in S there exists $(v, d) \in S$ such that $(x, a)\ \mathcal{H}\ (v, d) \geq (u, c)$. Since B is a band and M is completely simple, this implies that $x = v$, $y = u$, $a = b$, $c = d$, $x \geq y$, and thus $(x, a), (y, a), (y, c) \in S$ implies $(x, c) \in S$, that is

$$a \in M_x \cap M_y, \quad c \in M_y \implies c \in M_x,$$

and finally

$$x \geq y, \quad M_x \cap M_y \neq \emptyset \implies M_y \subseteq M_x. \tag{10}$$

By (9), we have $M_x \cap M_y = M_x$, and by hypothesis $M_x \neq \emptyset$ so that $M_x \cap M_y \neq \emptyset$. This together with (10) implies

$$x \geq y \implies M_y \subseteq M_x$$

which in conjunction with (9) yields

$$x \geq y \implies M_y = M_x.$$

By Lemma 6.6 this implies that

$$x\ \theta\ y \implies M_x = M_y.$$

We have arrived at the diagram

$$\begin{tikzcd} B \arrow[r] \arrow[d] & \mathcal{S}(M) \\ B/\theta \arrow[ur, dashed] & \end{tikzcd} \qquad \begin{tikzcd} x \arrow[r] \arrow[d] & M_x \\ x\theta \arrow[ur, dashed] & \end{tikzcd}$$

and hence at a function $B/\theta \to \mathcal{S}(M)$ where $B/\theta \in \mathcal{RB}^*$. This function determines a subdirect product A of B/θ and M which bears the relationship to S as in the direct part of the theorem. $\square$

Acknowledgement. The author is indebted to the referees for careful reading of the paper.

References

[1] T. S. Blyth, E. Giraldes and M. P. O. M. Smith, Associate subgroups of orthodox semigroups, *Glasgow Math. J.* **36** (1994), 163–171.

[2] T. S. Blyth and P. M. Martins, On associate subgroups of regular semigroups, *Comm. Algebra* **25** (1997), 2147–2156.

[3] T. S. Blyth and R. McFadden, Unit orthodox semigroups, *Glasgow Math. J.* **24** (1983), 39–42.

[4] P. M. Martins and M. Petrich, Unary semigroups with an associate subgroup, *Comm. Algebra* **36** (2008), 1999–2013.

[5] M. Petrich, A condition on the natural order for regular semigroups, *Comm. Algebra* **30** (2002), 517–542.

[6] M. Petrich and N. R. Reilly, Completely Regular Semigroups, *Wiley*, *New York*, 1999.

MARIO PETRICH
21420, BOL, BRAČ
CROATIA

(Received June 4, 2007; revised June 25, 2008)