Spined Product Decompositions of Orthocryptogroups

Akihiro Yamamura

Abstract A semigroup is said to be an internal spined product of its subsemigroups if it is naturally isomorphic to an external spined product of the subsemigroups. We shall show that internal spined products can be identified with external spined products in the class of orthocryptogroups. On the other hand, two concepts are not equivalent in general as we give examples of external spined products that admit no internal spined product decomposition. Further, we examine internal spined product of orthocryptogroups. Using a lattice theoretic method, we obtain a unique decomposition theorem similar to the Krull–Schmidt theorem in group theory. We also study completely reducible orthocryptogroups in which any normal sub-orthocryptogroup is a spined factor. We show that such an orthocryptogroup is an internal spined product of simple sub-orthocryptogroups.

Keywords Orthocryptogroups · Spined products · Krull–Schmidt theorem · Ore theorem

1 Introduction

An external spined product gives a convenient way to construct a new semigroup from old ones. It plays an important role in the structure theory of regular semigroups. Suppose S_1 and S_2 are semigroups. Let $\phi_1 : S_1 \to Q$ and $\phi_2 : S_2 \to Q$ be epimorphisms. The *external spined product* of S_1 and S_2 over Q with respect to ϕ_1 and ϕ_2 is defined to be the set of pairs (s_1, s_2) satisfying $\phi_1(s_1) = \phi_2(s_2)$. Obviously, an external spined product forms a subsemigroup of the external direct product $S_1 \times S_2$. We denote the external spined product by $S_1 \bowtie_Q S_2$. An external spined product is called just a *spined product* in the literature of semigroup theory. An external spined product of more than two factors is defined similarly. If Γ is the largest semilattice homomorphic image of S_1 and S_2, respectively, and both ϕ_1 and ϕ_2 are the natural

A. Yamamura (✉)
Department of Mathematical Science and Electrical-Electric-Computer Engineering,
Akita University, 1-1, Tegata-Gakuenmachi, Akita, Japan
e-mail: yamamura@ie.akita-u.ac.jp

S.T. Rizvi et al. (eds.), *Algebra and its Applications*, Springer Proceedings
in Mathematics & Statistics 174, DOI 10.1007/978-981-10-1651-6_2

homomorphisms, then the external spined product can be formed over Γ. Similarly, if Green's $\mathcal{H}$-relation of S_1 and S_2 are congruences and $B = S_1/\mathcal{H} = S_2/\mathcal{H}$, then the external spined product with respect to $\mathcal{H}$ can be formed over B.

A semigroup is called *cryptic* if Green's $\mathcal{H}$-relation is a congruence. A cryptic completely regular semigroup is called a *cryptogroup*. An *orthodox semigroup* is a regular semigroup in which the set of idempotents forms a subsemigroup and an *orthocryptogroup* is an orthodox cryptogroup. It was first studied by Yamada and called a *strictly inversive semigroup* in [7]. He showed that an external spined product of a Clifford semigroup and a band with respect to the structure decomposition is an orthocryptogroup, and conversely, every orthocryptogroup S is isomorphic to an external spined product $C \bowtie_\Gamma E(S)$ of the largest Clifford semigroup homomorphic image C and the band $E(S)$ of idempotents of S over the structure semilattice Γ.

The group inverse of an element a in a completely regular semigroup is denoted by a^{-1}. The identity element of the subgroup of a completely regular semigroup containing an element a is denoted by a^0, that is, $a^0 = aa^{-1} = a^{-1}a$. It is known (see [5]) that a completely regular semigroup satisfies the equation

$$(xy)^{-1} = (xy)^0 y^{-1} (yx)^0 x^{-1} (xy)^0 \tag{1.1}$$

and an orthocryptogroup satisfies the equation

$$(xy)^0 = x^0 y^0. \tag{1.2}$$

Therefore an orthocryptogroup satisfies the equation

$$(xy)^{-1} = x^0 y^{-1} x^{-1} y^0. \tag{1.3}$$

The equational class of completely regular semigroups defined by (1.3) includes the variety of orthocryptogroups but does not coincide [9].

The least band congruence of an orthocryptogroup S is Green's $\mathcal{H}$-relation and so S has the $\mathcal{H}$-decomposition $\bigcup_{e \in E(S)} S(e)$, where $S(e)$ is the maximal subgroup containing the idempotent e and $E(S)$ is the band of idempotents of S. Note that $E(S)$ is isomorphic to the largest band image of S and $E(S) \cong S/\mathcal{H}$.

A nonempty subset of an orthocryptogroup S is called a *sub-orthocryptogroup* if it forms an orthocryptogroup under the multiplication of S, that is, a nonempty subset is a sub-orthocryptogroup if and only if it is closed under taking an inverse and multiplication.

Suppose S is an orthocryptogroup and ϕ is the natural homomorphism of S onto the largest band image B, that is, $B \cong S/\mathcal{H}$. A sub-orthocryptogroup H of S is called *full* if $E(H) = E(S)$. If S has the $\mathcal{H}$-decomposition $\bigcup_{e \in E(S)} S(e)$, then H has the $\mathcal{H}$-decomposition $\bigcup_{e \in E(S)} H(e)$. The following lemma is obvious because an orthocryptogroup is isomorphic to an external spined product of a Clifford semigroup and a band, however, we give a direct proof.

Lemma 1.1 *Let $H_1, H_2, \ldots, H_n$ be full sub-orthocryptogroups of S. Suppose $s_1 \in H_1(e_1)$, $s_2 \in H_2(e_2)$, ..., $s_n \in H_n(e_n)$ for $e_1, e_2, \ldots, e_n \in E(S)$. Then there exists $s_1' \in H_1(e)$, $s_2' \in H_2(e)$, ..., $s_n' \in H_n(e)$ such that $s_1 s_2 \ldots s_n = s_1' s_2' \ldots s_n'$, where $e = e_1 e_2 \ldots e_n$.*

Proof Note that $s_1 = s_1 e_1$ because $s_1 \in S(e_1)$ and e_1 is the identity element of $S(e_1)$. Likewise, $s_2 \ldots s_n = e_2 \ldots e_n s_2 \ldots s_n$ because $s_2 \ldots s_n \in S(e_2 \ldots e_n)$ and $e_2 \ldots e_n$ is the identity element of $S(e_2 \ldots e_n)$. Then $s_1 s_2 \ldots s_n = s_1 e_1 e_2 \ldots e_n s_2 \ldots s_n = s_1(e_1 e_2 \ldots e_n)(e_1 e_2 \ldots e_n) s_2 \ldots s_n = s_1 e_2 \ldots e_n e_1 s_2 \ldots s_n$. Likewise we have $s_1 e_2 \ldots e_n e_1 s_2 s_3 \ldots s_n = s_1 e_2 \ldots e_n e_1 s_2 e_3 \ldots e_n e_1 e_2 s_3 \ldots s_n$ and similarly $s_1 s_2 \ldots s_n = (s_1 e_2 \ldots e_n)(e_1 s_2 e_3 \ldots e_n)(e_1 e_2 s_3 e_4 \ldots e_n) \ldots (e_1 \ldots e_{n-1} s_n)$. Now we set $s_i' = e_1 e_2 \ldots e_{i-1} s_i e_{i+1} \ldots e_n$. Then $s_1 s_2 \ldots s_n = s_1' s_2' \ldots s_n'$ and $s_i' \in H_i(e)$ for every $i = 1, 2, \ldots, n$. □

2 Internal Spined Products

Let S be a semigroup and ϕ a homomorphism of S onto Q. Suppose H_1 and H_2 are subsemigroups of S such that $\phi(H_1) = \phi(H_2) = Q$. If the external spined product $H_1 \bowtie_Q H_2$ over Q with respect to $\phi|_{H_1}$ and $\phi|_{H_2}$ is isomorphic to S under the mapping $(h_1, h_2) \mapsto h_1 h_2$ where $(h_1, h_2) \in H_1 \bowtie_Q H_2$, then S is said to be the *internal spined product* of H_1 and H_2 over Q. In such a case we denote $S = H_1 \bowtie_Q H_2$. Similarly, we can define an internal spined product $H_1 \bowtie_Q H_2 \bowtie_Q \ldots \bowtie_Q H_n$ of finitely many subsemigroups.

By the definition, every internal spined product is always isomorphic to an external spined product of its subsemigroups. On the other hand, an external spined product does not always admit an internal spined product decomposition as we shall see next. We note that an external direct product of groups always admits an internal direct product decomposition of its subgroups.

Example 1 A band is said to be *normal* (*left normal*, *right normal*, resp.) if it satisfies the equation $xyzx = xzyx$ ($xyz = xzy$, $yzx = zyx$, resp.). Let B be a band defined on the set $\{e, f, a, b, c, d\}$ with the following multiplication Table 1.

Table 1 Multiplication table of B

	e	f	a	b	c	d
e	e	b	a	b	a	b
f	c	f	c	d	c	d
a	a	b	a	b	a	b
b	a	b	a	b	a	b
c	c	d	c	d	c	d
d	c	d	c	d	c	d

Table 2 Multiplication table of L

	l_1	l_2	l_3	l_4
l_1	l_1	l_3	l_3	l_3
l_2	l_4	l_2	l_4	l_4
l_3	l_3	l_3	l_3	l_3
l_4	l_4	l_4	l_4	l_4

Table 3 Multiplication table of R

	r_1	r_2	r_3	r_4
r_1	r_1	r_4	r_3	r_4
r_2	r_3	r_2	r_3	r_4
r_3	r_3	r_4	r_3	r_4
r_4	r_3	r_4	r_3	r_4

Clearly, $\{e\}$, $\{f\}$, and $\{a, b, c, d\}$ are $\mathcal{D}$-classes of B, which are rectangular bands, and B is a strong semilattice of them. Note that a band is normal if it is a strong semilattice of rectangular bands [6]. Therefore, B is normal and has the structure decomposition $B = \{e\} \cup \{f\} \cup \{a, b, c, d\}$. It is well known that a normal band is an external spined product of a left normal band and a right normal band [6]. It is easy to see B is isomorphic to an external spined product of four element left normal band $L = \{l_1, l_2, l_3, l_4\}$ and a four element right normal band $R = \{r_1, r_2, r_3, r_4\}$ over the structure semilattice $\Gamma = \{\alpha, \beta, 0\}$ that is the three element non-chain semilattice (Tables 2 and 3).

Note that L and R have the structure decomposition $L = \{l_1\} \cup \{l_2\} \cup \{l_3, l_4\}$ and $R = \{r_1\} \cup \{r_2\} \cup \{r_3, r_4\}$, respectively. Then $L \bowtie_\Gamma R$ is isomorphic to B under the mapping; $(l_1, r_1) \mapsto e$, $(l_2, r_2) \mapsto f$, $(l_3, r_3) \mapsto a$, $(l_3, r_4) \mapsto b$, $(l_4, r_3) \mapsto c$, $(l_4, r_4) \mapsto d$.

On the other hand, it is easy to verify that there is no proper subsemigroup of B whose largest semilattice homomorphic image is Γ. It follows that there is no subsemigroups B_1 and B_2 of B so that B is the internal spined product $B_1 \bowtie_\Gamma B_2$. Therefore, B admits no internal spined product with respect to the structure decomposition even though B is an external spined product.

Example 2 Next we consider a spined product of completely simple semigroups. Let S_1 be the two element right zero semigroup. Note that S_1 can be considered as the Rees matrix semigroup $\mathcal{M}(G_1; I, \Lambda; P)$, where G_1 is the trivial group, $I = \{1\}$, $\Lambda = \{1, 2\}$, and the sandwich matrix P is defined by $\begin{pmatrix} p_{11} \\ p_{21} \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

Next let S_2 be a Rees matrix semigroup $\mathcal{M}(G_2; I, \Lambda; Q)$, where $G_2 = \{1, g, g^2\}$ is the cyclic group of order three, $I = \{1\}$, $\Lambda = \{1, 2\}$, and the sandwich matrix Q is defined by $\begin{pmatrix} q_{11} \\ q_{21} \end{pmatrix} = \begin{pmatrix} g \\ 1 \end{pmatrix}$. Note that S_2 is not a rectangular group because the set of idempotents does not form a subsemigroup. Clearly both $S_1/\mathcal{H}$ and $S_2/\mathcal{H}$ are the two element right zero semigroup B. Then the external spined product $S_1 \bowtie_B S_2$ over B can be considered as the Rees matrix semigroup $\mathcal{M}(G_1 \times G_2; I, \Lambda; R)$, where the sandwich matrix R is defined by $\begin{pmatrix} r_{11} \\ r_{21} \end{pmatrix} = \begin{pmatrix} (1, g) \\ (1, 1) \end{pmatrix}$. It is easy to see that S is isomorphic to S_2. On the other hand, there exists no subsemigroup isomorphic to S_1 because $\mathcal{M}(G_1 \times G_2; I, \Lambda; R)$ does not contain the two element right zero semigroup. Therefore, $S_1 \bowtie_B S_2$ admits no internal spined product with respect to $\mathcal{H}$.

3 Internal Spined Products of Orthocryptogroups

Suppose S is an orthocryptogroup and ϕ is the natural homomorphism of S onto the largest band image B, that is, $B \cong S/\mathcal{H}$. Let $H_1, H_2, \ldots, H_n$ be full sub-orthocryptogroups of S. They have the same largest band image B and so we can consider the external spined product over B. Recall that if S is isomorphic to the external spined product $H_1 \bowtie_B H_2 \bowtie_B \ldots \bowtie_B H_n$ under the mapping $(s_1, s_2, \ldots, s_n) \mapsto s_1 s_2 \ldots s_n$, then S is said to be the internal spined product of $H_1, H_2, \ldots, H_n$.

Lemma 3.1 *If S is the internal spined product of full sub-orthocryptogroups $H_1, H_2, \ldots, H_n$, then the following conditions hold.*

(A1) Elements of $H_i(e)$ and $H_j(e)$ $(i \neq j)$ commute for every $e \in E(S)$.
(A2) For $e \in E(S)$ every element s of $S(e)$ is expressed uniquely as $s = s_1 s_2 \ldots s_n$, where $s_i \in H_i(e)$.

Conversely, if full sub-orthocryptogroups $H_1, H_2, \ldots, H_n$ satisfy (A1) and (A2), then S is the internal spined product $H_1 \bowtie_B H_2 \bowtie_B \ldots \bowtie_B H_n$.

Proof If $S = H_1 \bowtie_B H_2 \bowtie_B \ldots \bowtie_B H_n$, then clearly (A1) and (A2) are satisfied. We now suppose (A1) and (A2) hold for full sub-orthocryptogroups $H_1, H_2, \ldots, H_n$. Define a mapping ψ of the external spined product $H_1 \bowtie_B H_2 \bowtie_B \ldots \bowtie_B H_n$ into S by $\psi(s_1, s_2, \ldots, s_n) = s_1 s_2 \ldots s_n$. We shall show that ψ is an isomorphism onto S. Take two elements $(s_1, s_2, \ldots, s_n)$ and $(t_1, t_2, \ldots, t_n)$ of $H_1 \bowtie_B H_2 \bowtie_B \ldots \bowtie_B H_n$. Suppose that $s_1 \in H_1(e), s_2 \in H_2(e), \ldots, s_n \in H_n(e)$ and $t_1 \in H_1(f), t_2 \in H_2(f), \ldots, t_n \in H_n(f)$. Let $h = ef$. Then we have $\psi((s_1, s_2, \ldots, s_n)(t_1, t_2, \ldots, t_n)) = \psi(s_1 t_1, s_2 t_2, \ldots, s_n t_n) = s_1 t_1 s_2 t_2 s_3 t_3 \ldots s_n t_n = s_1 h t_1 s_2 h t_2 s_3 t_3 \ldots s_n t_n = s_1 s_2 h h t_1 t_2 s_3 t_3 \ldots s_n t_n = s_1 s_2 t_1 t_2 s_3 t_3 \ldots s_n t_n$ since elements of $H_i(h)$ and $H_j(h)$ commute by (A1). Similarly we can show $s_1 s_2 t_1 t_2 s_3 t_3 \ldots s_n t_n = s_1 s_2 \ldots s_n t_1 t_2 \ldots t_n = \psi(s_1, s_2, \ldots, s_n)\psi(t_1, t_2, \ldots, t_n)$. Next, suppose that $\psi(s_1, s_2, \ldots, s_n) = \psi(t_1, t_2, \ldots, t_n)$, where $s_1 \in H_1(e), s_2 \in H_2(e), \ldots, s_n \in H_n(e)$ and $t_1 \in H_1(f)$,

$t_2 \in H_2(f), \ldots, t_n \in H_n(f)$. We have $s_1 s_2 \ldots s_n = t_1 t_2 \ldots t_n$. Then we have $e = f$ and (A2) implies $(s_1, s_2, \ldots, s_n) = (t_1, t_2, \ldots, t_n)$. Clearly ψ is surjective by (A2). Therefore ψ is an isomorphism. $\square$

A sub-orthocryptogroup N of S is called *normal* if N is full and $s^{-1}Ns \subset N$ for every s in S (see [8]). For any $s \in S$ and $e \in E(S)$ we have $(s^{-1}es)(s^{-1}es) = s^{-1}(ess^{-1})(ess^{-1})s = s^{-1}ess^{-1}s = s^{-1}es$. Hence, $s^{-1}es \in E(S)$ and so $E(S)$ is normal. Obviously S itself is normal.

For a normal sub-orthocryptogroup N we define a relation ρ_N of S by $s\,\rho_N\,t$ if and only if $s\,\mathcal{H}\,t$ and $st^{-1} \in N$. It is easy to see that ρ_N is an idempotent-separating congruence of S and N coincides with its kernel $\mathrm{Ker}(\rho_N) = \{s \mid s\,\rho_N\,e$ for some $e \in E(S)\}$. Conversely, for every idempotent-separating congruence ρ the kernel $\mathrm{Ker}(\rho) = \{s \mid s\,\rho\,e$ for some $e \in E(S)\}$ is a normal sub-orthocryptogroup of S, and furthermore we have $\rho_{\mathrm{Ker}(\rho)} = \rho$.

Lemma 3.2 *If S is the internal spined product of full sub-orthocryptogroups $H_1, H_2, \ldots, H_n$, then the following conditions hold.*

(B1) Every H_i is normal.
(B2) $S = H_1 H_2 \ldots H_n$.
(B3) $H_i \cap (H_1 \ldots H_{i-1} H_{i+1} \ldots H_n) = E(S)$ for every $i = 1, 2, \ldots n$.

Conversely, if sub-orthocryptogroups $H_1, H_2, \ldots, H_n$ satisfy (B1), (B2), and (B3), then S is the internal spined product $H_1 \bowtie_B H_2 \bowtie_B \ldots \bowtie_B H_n$.

Proof First we suppose S is the internal spined product $H_1 \bowtie_B H_2 \bowtie_B \ldots \bowtie_B H_n$. Then $H_1, H_2, \ldots, H_n$ satisfy (A1) and (A2) by Lemma 3.1. Take elements h in H_1 and s in S. Suppose $h \in H_1(f)$ and $s \in S(e)$. By (A2), there exists an element s_i in $H_i(e)$ for $i = 1, 2, \ldots, n$ such that $s = s_1 s_2 \ldots s_n$. Since all s_i belong to the subgroup $S(e)$, we have $s^{-1} = s_n^{-1} \ldots s_2^{-1} s_1^{-1}$. Note that $s_1^{-1} h s_1 \in H_1 \cap S(efe) = H_1(efe)$ because $s_1, h \in H_1$. Then we have $s_2^{-1}(s_1^{-1}hs_1)s_2 = s_2^{-1}(efe)(s_1^{-1}hs_1)(efe)s_2 = (s_1^{-1}hs_1)s_2^{-1}(efe)(efe)s_2 = (s_1^{-1}hs_1)s_2^{-1}s_2$ because elements of $H_1(efe)$ and $H_2(efe)$ commute by (A1). On the other hand, $(s_1^{-1}hs_1)s_2^{-1}s_2 = (s_1^{-1}hs_1)e = s_1^{-1}hs_1$. Inductively we can show $s_n^{-1} \ldots s_2^{-1}(s_1^{-1}hs_1)s_2 \ldots s_n = s_1^{-1}hs_1$. It follows that $s^{-1}hs = s_1^{-1}hs_1 \in H_1$. Thus H_1 is normal. Similarly we can show H_i is normal for $i = 2, \ldots, n$. Obviously, (A2) implies (B2). Now, take an element s in $H_1 \cap (H_2 \ldots H_n)$. Then $s = s_2 \ldots s_n$ for some $s_2 \in H_2, \ldots, s_n \in H_n$. Suppose $s \in H_1(e)$ for some $e \in E(S)$. By Lemma 1.1 we may assume that $s_i \in H_i(e)$. Then we have $e = s^{-1}s = s^{-1}s_2 \ldots s_n$. By (A2) we have $e = s^{-1} = s_2 = \ldots = s_n$ and $s = e$. Hence, $E(S) = H_1 \cap (H_2 \ldots H_n)$. Similarly we can show $H_i \cap (H_1 \ldots H_{i-1} H_{i+1} \ldots H_n) = E(S)$ for every $i = 2, \ldots, n$. Therefore, (B1), (B2), and (B3) hold.

Conversely, we suppose (B1), (B2), and (B3). Take elements s in $H_i(e)$ and t in $H_j(e)$ $(i \neq j)$. Since $sts^{-1} \in H_j$ and $ts^{-1}t^{-1} \in H_i$, we have $sts^{-1}t^{-1} \in H_i \cap H_j$. By (B3) we have $sts^{-1}t^{-1} \in E(S) \cap S(e)$. Hence, $sts^{-1}t^{-1} = e$. On the other hand, $s^{-1}t^{-1}ts = s^{-1}es = s^{-1}s = e$. Then $st = ste = sts^{-1}t^{-1}ts = ets = ts$. Hence, (A1) holds. Next, take an element s in $S(e)$. By (B2) $s = s_1 s_2 \ldots s_n$

for some $s_i \in H_i$ $(i = 1, 2, \dots, n)$. Moreover, we may take $s_i \in H_i(e)$ for $i = 1, 2, \dots, n$ by Lemma 1.1. Suppose $s_1 s_2 \dots s_n = t_1 t_2 \dots t_n$, where $s_i, t_i \in H_i(e)$ for every $i = 1, 2, \dots, n$. Then, $t_1^{-1} s_1 = t_2 \dots t_n s_n^{-1} \dots s_2^{-1}$. Note that $t_1^{-1} s_1 \in H_1(e)$. Since we have already shown (A1) holds, $t_2 \dots t_n s_n^{-1} \dots s_2^{-1} = t_2 s_2^{-1} t_3 s_3^{-1} \dots t_n s_n^{-1}$. Thus $t_2 \dots t_n s_n^{-1} \dots s_2^{-1} \in H_2(e) H_3(e) \dots H_n(e)$. By (B3) we have $t_1^{-1} s_1 = t_2 \dots t_n s_n^{-1} \dots s_2^{-1} = e$. Therefore, $s_1 = t_1$. Similarly we can show $s_i = t_i$ for every $i = 2, \dots, n$. Consequently we obtained (A2). □

In group theory, the external direct product $G = G_1 \times G_2$ always admits an internal direct decomposition of its subgroups isomorphic to G_1 and G_2. Let H_1 be $\{(g_1, 1) \mid g_1 \in G_1\}$ and H_2 be $\{(1, g_2) \mid g_2 \in G_2\}$, respectively. Then G is the *internal direct product* of H_1 and H_2. Thus, the concept of external and internal direct products are equivalent. This is not the case with wider classes of semigroups as we have seen in the preceding section. Fortunately spined products of orthocryptogroups over the largest band image are similar to direct products of groups.

Theorem 3.3 *Every external spined product of orthocryptogroups over the largest band image admits an internal spined product decomposition.*

Proof Suppose S is the external spined product of S_1 and S_2 over the band B, where $S_1/\mathcal{H} \cong B \cong S_2/\mathcal{H}$. We define subsemigroups H_1 and H_2 of S to be $H_1 = \{(s, e) \mid s \in S_1(e), e \in E(S_2)\}$ and $H_2 = \{(e, t) \mid t \in S_2(e), e \in E(S_1)\}$, respectively. It is routine to check H_1 and H_2 satisfy (B1), (B2), and (B3). Hence, S is the internal spined product of H_1 and H_2. It can be similarly shown for $S_1 \bowtie_B S_2 \bowtie_B \dots \bowtie_B S_n$ for $n \geq 3$. □

4 Spined Product Decompositions

Decomposing an algebraic system into indecomposable ones is an essential problem in mathematics. In group theory, the Krull–Schmidt theorem guarantees the uniqueness of direct product decompositions of groups satisfying certain finiteness conditions into indecomposable factors (see [2]). Ore [4] proved the Krull–Schmidt theorem using a lattice theoretic method. We shall prove the uniqueness of internal spined product decompositions of orthocryptogroups into indecomposable factors using a lattice theoretic method.

A lattice is said to be *of finite length* if there is a bound on the length of its chains. Two elements a and b in a lattice with the least element 0 and the greatest element 1 are said to be *complementary* if $a \vee b = 1$ and $a \wedge b = 0$ hold. In such a case, b is said to be *complement* of a and vice versa. Two elements in a lattice that have a common complement c are said to be *c-related*. A lattice L is called *modular* if it satisfies the modular law

$$a \leq b \Rightarrow (c \vee a) \wedge b = (c \wedge b) \vee a \quad (a, b, c \in L) \tag{4.1}$$

Let L be a modular lattice with the least element 0. A subset $\{a_1, a_2, \ldots, a_n\}$ of finitely many elements of L is said to be *independent* if $a_i \neq 0$ $(i = 1, 2, \ldots, n)$ and

$$a_i \wedge (a_1 \vee \ldots \vee a_{i-1} \vee a_{i+1} \vee \ldots \vee a_n) = 0 \tag{4.2}$$

for every $i = 1, 2, \ldots, n$. If an element $a \in L$ is represented as the join of an independent set, that is, $a = a_1 \vee \ldots \vee a_n$ where $\{a_1, a_2, \ldots, a_n\}$ is independent, then a is said to be the *direct join* of the elements $a_1, a_2, \ldots, a_n$ and we write $a = a_1 \times \ldots \times a_n$. An element a in a lattice L is said to be *indecomposable* if $a \neq 0$ and it admits no direct join $a = b \times c$ with $b \neq a$ and $c \neq a$. If a is written as a direct join of indecomposable elements, then it is called a *complete decomposition* of a. The following theorem is due to Ore (see [1, 3] for a proof).

Proposition 4.1 *In a modular lattice L of finite length, if*

$$1 = a_1 \times \ldots \times a_m$$

and

$$1 = b_1 \times \ldots \times b_n$$

are two complete decompositions of 1, *then each a_i is a_i'-related to some b_j for $i = 1, 2, \ldots, m$, where $a_i' = a_1 \times \ldots \times a_{i-1} \times a_{i+1} \times \ldots \times a_m$.* □

We shall show that the set of normal sub-orthocryptogroups of an orthocryptogroup S forms a lattice. Suppose M and N are normal sub-orthocryptogroups of S. Take $m \in M$ and $n \in N$. Note that S satisfies the Eqs. (1.2) and (1.3). Then we have $mn = mn(mn)^0 = mnm^{-1}mn^0 \in NM$ since $mnm^{-1} \in N$ and $n^0 \in M$. Thus, $MN \subset NM$ and vice versa. Hence, $MN = NM$. Then $(MN)(MN) = MMNN = MN$ and so MN is closed under multiplication. Next we take $m \in M$ and $n \in N$. We have $(mn)^{-1} = m^0n^{-1}m^{-1}n^0 \in MNMN = MN$. Hence, MN is closed under taking inverse. Since M and N are full, $M \subset ME(S) \subset MN$ and $N \subset E(S)N \subset MN$. Thus MN include both M and N. Next take $s \in MN$ and $h \in S$. Suppose $s \in S(e)$. By Lemma 1.1 we can write $s = mn$ for some $m \in M(e)$ and $n \in N(e)$. Then we have $h^{-1}sh = h^{-1}mnh = h^{-1}m(h^{-1}m)^0nh = h^{-1}mhh^{-1}m^0nh \in MN$ since $h^{-1}mh \in M$ and $h^{-1}m^0nh \in N$. Thus MN is normal. Therefore, MN is the smallest normal sub-orthocryptogroup including both M and N. On the other hand, $M \cap N$ is the largest normal sub-orthocryptogroup contained in both M and N. Consequently, the set of normal sub-orthocryptogroups forms a lattice with the join MN and the meet $M \cap N$. This lattice has the greatest element S and the least element $E(S)$. Moreover, we have the following.

Lemma 4.2 *The lattice of normal sub-orthocryptogroups of an orthocryptogroup is modular.*

Proof Let S be an orthocryptogroup. Suppose that A, B, C are normal sub-ortho cryptogroups of S satisfying $A \subset B$. It is enough to show $(CA) \cap B \subset (C \cap B)A$.

Take an arbitrary element s from $(CA) \cap B$. Then $s = ca$, where $c \in C$, $a \in A$ and $s \in B$. Note that $sa^{-1} = caa^{-1}$. Since $A \subset B$, we have $sa^{-1} \in B$. On the other hand, $caa^{-1} \in C$ because C is full. Therefore, $s = ca = caa^{-1}a = (sa^{-1})a \in (C \cap B)A$ and so $(CA) \cap B \subset (C \cap B)A$. □

It is easy to see that the lattice of normal sub-orthocryptogroups is isomorphic to the lattice of idempotent-separating congruences under the correspondence $N \leftrightarrow \rho_N$. Therefore the lattice of idempotent-separating congruences of an orthocryptogroup is modular by Lemma 4.2.

We say that an orthocryptogroup S is *spined indecomposable* if $S \neq E(S)$ and the internal spined product decomposition $S = S_1 \bowtie_B S_2$, where $B = S/\mathcal{H}$, implies either $S_1 = S$ or $S_2 = S$. Note that an orthocryptogroup S always admits the internal spined product decomposition $S = S \bowtie_B E(S)$.

We shall next give a sufficient condition for an orthocryptogroup to admit a spined product decomposition into spined indecomposable factors. An orthocryptogroup S is said to satisfy the *ascending chain condition* if $N_1 \subset N_2 \subset N_3 \subset \ldots$ is a chain of normal sub-orthocryptogroups, then there exists t for which $N_t = N_{t+1} = N_{t+2} = \ldots$, and S is said to satisfy the *descending chain condition* if $K_1 \supset K_2 \supset K_3 \supset \ldots$ is a chain of normal sub-orthocryptogroups then there exists t for which $K_t = K_{t+1} = K_{t+2} = \ldots$.

Theorem 4.3 *Suppose S satisfies either the ascending or descending chain condition. Then S is an internal spined product of a finitely many spined indecomposable factors.*

Proof Suppose the conclusion does not hold. Then S is not spined indecomposable and so it is decomposed as $H_0 \bowtie_B K_0$, where H_0 and K_0 are proper sub-orthocryptogroups. By the assumption, either H_0 or K_0 is not spined indecomposable, say H_0. By induction, there is a sequence of sub-orthocryptogroups $H_0, H_1, H_2, \ldots$, where every H_i is a proper spined factor of H_{i-1}. Then we have a descending chain $S \supsetneq H_0 \supsetneq H_1 \supsetneq H_2 \supsetneq \ldots$. It is easy to see H_i is normal in S. If S satisfies the descending chain condition, this is a contradiction. Now we suppose S satisfies the ascending chain condition. Since each H_i is a spined factor of H_{i-1}, there is a normal sub-orthocryptogroup K_i in H_{i-1} satisfying $H_{i-1} = H_i \bowtie_B K_i$. Since each K_i is normal in S, we have an ascending chain $K_0 \subsetneq K_0 \bowtie_B K_1 \subsetneq K_0 \bowtie_B K_1 \bowtie_B K_2 \subsetneq \ldots$, which is a contradiction. □

We note that a modular lattice is of finite length if and only if it satisfies both the chain conditions (see [3]). Therefore, if an orthocryptogroup S satisfies both the chain conditions, then the lattice of normal sub-orthocryptogroups is of finite length and vice versa.

Theorem 4.4 *Let S be an orthocryptogroup satisfying both the chain conditions and $B = S/\mathcal{H}$. If S has two spined product decompositions $H_1 \bowtie_B H_2 \bowtie_B \ldots \bowtie_B H_m$ and $K_1 \bowtie_B K_2 \bowtie_B \ldots \bowtie_B K_n$, where H_i $(i = 1, 2, \ldots, m)$ and K_j $(j = 1, 2, \ldots, n)$ are spined indecomposable, then $m = n$ and there exists a bijection Ψ of the family*

$\{H_i \mid i = 1, 2, \ldots, m\}$ onto the family $\{K_i \mid j = 1, 2, \ldots, n\}$ such that H_i is isomorphic and H_i'-related to $\Psi(H_i)$.

Proof Note that the lattice of normal sub-orthocryptogroups of S is modular by Lemma 4.2, and it is of finite length because S satisfies both the chain conditions. By Lemma 3.2, $\{H_1, H_2, \ldots, H_m\}$ and $\{K_1, K_2, \ldots, K_n\}$ are independent, respectively. Therefore both $H_1 \bowtie_B H_2 \bowtie_B \ldots \bowtie_B H_m$ and $K_1 \bowtie_B K_2 \bowtie_B \ldots \bowtie_B K_n$ are complete decompositions of S.

Suppose $n \leq m$. By Proposition 4.1, H_1 is H_1'-related to some K_j (say K_1). Recall that $H_1' = H_2 \bowtie_B \ldots \bowtie_B H_m$. We have $S = K_1 \bowtie_B H_1' = K_1 \bowtie_B H_2 \bowtie_B \ldots \bowtie_B H_m$. By induction, we obtain $S = K_1 \bowtie_B K_2 \bowtie_B \ldots \bowtie_B K_n \bowtie_B H_{n+1} \bowtie_B \ldots \bowtie_B H_m$ after renumbering K_j. On the other hand, we have $S = K_1 \bowtie_B K_2 \bowtie_B \ldots \bowtie_B K_n$. Therefore, we have $m = n$. Moreover, each H_i is H_i'-related to K_j for some j by Proposition 4.1.

Next we shall show that if H_1 and K_j (say K_1) is H_1'-related, then H_1 and K_1 are isomorphic. Suppose that $S = H_1 \bowtie_B H_1' = K_1 \bowtie_B H_1'$. Define a mapping $\psi : H_1 \to K_1$ as follows. For $h \in H_1(e)$ ($e \in E(S)$) we set $\psi(h) = k$ where k is an element of $K_1(e)$ satisfying $h = ka$ for some $a \in H_1'(e)$. Such an element is uniquely determined by Lemma 3.1 and so ψ is well defined.

Suppose that $\psi(h_1) = \psi(h_2) = k$ for $h_1, h_2 \in H_1(e)$ ($e \in E(S)$). Then $h_1 = ka_1$ and $h_2 = ka_2$ for some $a_1, a_2 \in H_1'(e)$. We have $h_1^{-1}h_2 = (ka_1)^{-1} ka_2 = a_1^{-1}k^{-1}ka_2 = a_1^{-1}a_2$ as $k, a_1 \in S(e)$. Thus $a_1^{-1}a_2 = h_1^{-1}h_2 \in H_1(e)$. On the other hand, $a_1^{-1}a_2 \in H_1'(e)$. Since $H_1(e) \cap H_1'(e) = \{e\}$, we have $a_1^{-1}a_2 = e$. Therefore, $a_1 = a_1 e = a_1 a_1^{-1} a_2 = ea_2 = a_2$. It follows that $h_1 = ka_1 = ka_2 = h_2$ and ψ is injective. It is easy to see ψ is surjective.

Next we shall show that ψ is a homomorphism. Take arbitrary elements $h_1 \in H_1(e)$ and $h_2 \in H_1(f)$, where $e, f \in E(S)$. Suppose $\psi(h_1) = k_1$ and $\psi(h_2) = k_2$. Then $h_1 = k_1a_1$ and $h_2 = k_2a_2$ for some $a_1 \in H_1'(e)$ and $a_2 \in H_1'(f)$. Then we have $h_1h_2 = k_1a_1k_2a_2 = k_1a_1efk_2a_2 = k_1a_1efefk_2a_2 = k_1efk_2a_1efa_2 = k_1k_2a_1a_2$ since S is orthodox and $a_1ef (\in H_1'(ef))$ and $efk_2 (\in K_1(ef))$ commute by Lemma 3.1. Note that $k_1k_2 \in K_1(ef)$ and $a_1a_2 \in H_1(ef)$. Therefore, $\psi(h_1h_2) = k_1k_2 = \psi(h_1)\psi(h_2)$. Consequently, ψ is an isomorphism of H_1 onto K_1. □

5 Completely Reducible Orthocryptogroups

In the preceding sections, we have considered internal spined products of finitely many sub-orthocryptogroups. We now consider internal spined product of an arbitrary family of sub-orthocryptogroups and examine orthocryptogroups in which any normal sub-orthocryptogroup is an internal spined product factor.

Let B be a band and $\{S_\lambda \mid \lambda \in \Lambda\}$ a nonempty family of orthocryptogroups such that $E(S_\lambda) \cong B$ for every λ in Λ. Note that each S_λ has the same largest homomorphic band image B. Consider the set P of functions defined on Λ for which there exists e_f in B satisfying the following.

1. $f(\lambda) \in S_\lambda(e_f)$.
2. $f(\lambda) = e_f$ for all but finitely many $\lambda \in \Lambda$.

For $f, g \in P$, we define a multiplication fg by $(fg)(\lambda) = f(\lambda)g(\lambda)$. It is easy to see that fg belongs to P and P forms an orthocryptogroup under this multiplication. Then the set of the idempotents is isomorphic to B and we identify it with B. We say that P is the *external spined product* of the family $\{S_\lambda \mid \lambda \in \Lambda\}$ and denote it by $\bowtie_{\lambda\in\Lambda} S_\lambda$. Note that if Λ is finite, then $\bowtie_{\lambda\in\Lambda} S_\lambda$ is exactly the external spined product defined in Sect. 1.

Suppose S is an orthocryptogroup and $\{H_\lambda \mid \lambda \in \Lambda\}$ is a family of full sub-orthocryptogroups of S. If the external spined product $\bowtie_{\lambda\in\Lambda} H_\lambda$ is isomorphic to S under the mapping $f \mapsto f(\lambda_1)f(\lambda_2)\dots f(\lambda_n)$, where $f(\tau) = e_f (\in E(S))$ for $\tau \in \Lambda \setminus \{\lambda_1, \lambda_2, \dots, \lambda_n\}$, then S is said to be the *internal spined product* of $\{H_\lambda \mid \lambda \in \Lambda\}$ and denoted by $S = \bowtie_{\lambda\in\Lambda} S_\lambda$.

A family of sub-orthocryptogroups $\{H_\lambda \mid \lambda \in \Lambda\}$ of S is called *independent* if any finite subset is independent in the lattice of sub-orthocryptogroups, that is, any finite subset satisfies (4.2). A proof of the following lemma is similar to the one for Lemma 3.2 and so we omit it.

Lemma 5.1 *If an orthocryptogroup S is the internal spined product of a family of full sub-orthocryptogroups $\{H_\lambda \mid \lambda \in \Lambda\}$, then the following conditions hold.*

(C1) Every H_λ is normal.
(C2) S is generated by $\bigcup_{\lambda\in\Lambda} H_\lambda$.
(C3) $\{H_\lambda \mid \lambda \in \Lambda\}$ is independent.

Conversely, if the family $\{H_\lambda \mid \lambda \in \Lambda\}$ of full sub-orthocryptogroups satisfy (C1), (C2), and (C3), then S is the internal spined product $\bowtie_{\lambda\in\Lambda} H_\lambda$. □

A full sub-orthocryptogroup H of S is said to be a *spined factor* if there exists a full sub-orthocryptogroup K such that $S = H \bowtie_B K$. For example, both $E(S)$ and S are spined factors. An orthocryptogroup S is called *simple* if $S \neq E(S)$ and there exists no proper normal sub-orthocryptogroup other than $E(S)$. We say that S is *completely reducible* if there exists a family $\{H_\lambda \mid \lambda \in \Lambda\}$ of simple full sub-orthocryptogroups such that $S = \bowtie_{\lambda\in\Lambda} H_\lambda$.

Theorem 5.2 *Let S be an orthocryptogroup. Then the following conditions are equivalent.*

(1) S is completely reducible.
(2) There is a family of simple normal sub-orthocryptogroups $\{H_\lambda \mid \lambda \in \Lambda\}$ such that S is generated by $\bigcup_{\lambda\in\Lambda} H_\lambda$.
(3) Every normal sub-orthocryptogroup H is a spined factor.

Proof (1) implies (2). Suppose $S = \bowtie_{\lambda\in\Lambda} H_\lambda$ where H_λ is simple. By Lemma 5.1, H_λ is normal and S is generated by $\bigcup_{\lambda\in\Lambda} H_\lambda$.

(2) implies (3). Let H be a normal sub-orhtocryptogroup of S. If $H = S$, then we can take $K = E(S)$. So we may assume $H \neq S$. Let $\mathcal{A}$ be the set of all subsets A

of Λ such that the family $\{H\} \cup \{H_\lambda \mid \lambda \in A\}$ is independent. Since $H \neq S$ and S is generated by $\bigcup_{\lambda\in\Lambda} H_\lambda$, there exists $\lambda \in \Lambda$ such that $H_\lambda \not\subset H$. Then $H_\lambda \cap H = E(S)$ because H_λ is simple. Therefore $\mathcal{A}$ is not empty. By Zorn's lemma, there exists a maximal element M in $\mathcal{A}$. Let L be the sub-orthocryptogroup generated by $H \cup (\bigcup_{\lambda\in M} H_\lambda)$. Using Lemma 1.1, we can show L is also normal as H and H_λ are normal. If $L \neq S$, then there exists $\rho \in \Lambda$ such that $H_\rho \not\subset L$. Since H_ρ is simple and $H_\rho \cap L$ is normal, we have $H_\rho \cap L = E(S)$. Then the family $\{H, H_\rho\} \cup \{H_\lambda \mid \lambda \in M\}$ is independent, which contradicts to the maximality of M. It follows that $L = S$. Let K be the sub-orthocryptogroup generated by $\bigcup_{\lambda\in M} H_\lambda$. By Lemma 3.2, $S = H \bowtie_B K$ and so H is a spined factor.

(3) implies (1). We may assume that $S \neq E(S)$. First, we shall show that for any proper normal sub-orthocryptogroup H, there exists a normal simple sub-orthocryptogroup T such that $H \cap T = E(S)$. Choose an element $u \in S$ such that $u \notin H$. Let $\mathcal{B}$ be the family of the normal sub-orthocryptogroups of S containing H but not u. By Zorn's lemma, there exists a maximal element M in the family. Next we shall show that M is a maximal normal sub-orthocryptogroup. Suppose M is not. Then $M \subsetneq L$ for some proper normal sub-orthocryptogroup L. By our assumption, there exists a proper sub-orthocryptogroup V such that $S = L \bowtie_B V$. If $MV \subset M$ then $V \subset E(S)V \subset MV \subset M$. This implies $L \bowtie_B V \subset LM = L$, which is a contradiction. Therefore, $M \subsetneq MV$. By the maximality of M we have $u \in MV \cap L$. By Lemma 4.2, $MV \cap L = M(V \cap L) = ME(S) = M$. This contradicts to the fact that $u \notin M$. Therefore, M is a maximal normal sub-orthocryptogroup. By our assumption, $S = M \bowtie_B T$ for some T. If T is not simple, then there exists a nontrivial proper normal sub-orthocryptogroup $D \subsetneq T$. Then $M \bowtie_B D$ is normal by Lemmas 1.1 and 3.2, but $M \subsetneq M \bowtie_B D \subsetneq S$, which is a contradiction. Therefore, T is simple. Since $H \subset M$ and $M \cap T = E(S)$, we have $H \cap T = E(S)$.

By the preceding argument, there exists a simple normal sub-orthocryptogroup $T \neq E(S)$ since we are assuming $S \neq E(S)$. We consider the family of independent sets of simple normal sub-orthocryptogroups of S. By Zorn's lemma, there exists a maximal set $\{H_\lambda \mid \lambda \in \Lambda\}$. Let H_0 be the sub-orthocryptogroup generated by $\bigcup_{\lambda\in\Lambda} H_\lambda$. Note that H_0 is normal. If $H_0 \subsetneq S$, there exists a normal simple sub-orthocryptogroup C such that $H_0 \cap C = E(S)$ by the preceding argument. Then the family $\{H_\lambda \mid \lambda \in \Lambda\} \cup \{C\}$ is independent, which contradicts to the maximality of the set $\{H_\lambda \mid \lambda \in \Lambda\}$. Hence, $H_0 = S$ and so $S = \bowtie_{\lambda\in\Lambda} H_\lambda$ by Lemma 5.1. Consequently, S is completely reducible. □

Finally we characterize simple orthocryptogroups. Recall that a completely regular semigroup S can be decomposed into a semilattice Γ of completely simple semigroups R_γ $(\gamma \in \Gamma)$. Each R_γ is a $\mathcal{J}$ class of S. Such a completely simple semigroup is called *completely simple component* of S. In particular, every completely simple component is a rectangular group if S is an orthocryptogroup.

Theorem 5.3 *Let S be a simple orthocryptogroup. If S is a semilattice Γ of rectangular groups R_γ ($\gamma \in \Gamma$), then there exists an element δ in Γ such that $R_\delta \cong G \times B_\delta$, where G is a simple group and B_δ is a rectangular band, and R_γ is a rectangular band for every $\gamma \in \Gamma \setminus \{\delta\}$.*

Proof Since S is simple, $S \neq E(S)$ and so at least one completely simple component is not a rectangular band. We shall show that there exists exactly one completely simple component that is not a rectangular band. Suppose that $R_\delta \neq E(R_\delta)$ and $R_\tau \neq E(R_\tau)$ for $\delta, \tau \in \Gamma$ ($\delta \neq \tau$). We may assume $\tau \nleq \delta$. Let H be a set defined by

$$\left(\bigcup_{\tau \leq \rho} E(R_\rho)\right) \cup \left(\bigcup_{\tau \nleq \rho} R_\rho\right).$$

We shall show H is normal. Take $h \in H$ and $s \in S$. If either h or s belongs to $\bigcup_{\tau \nleq \rho} R_\rho$ then so does $s^{-1}hs$. We now suppose that h and s belong to $\bigcup_{\tau \leq \rho} E(R_\rho)$. In this case, h and s are idempotents and so is $s^{-1}hs$. Thus, $s^{-1}hs$ belongs to $\bigcup_{\tau \leq \rho} E(R_\rho)$. It follows that H is a proper normal sub-orthocryptogroup of S. This contradicts to the assumption that S is simple. Hence, there exists exactly one completely simple component R_δ that is not a rectangular band.

Suppose $R_\delta = G \times B_\delta$ for some nontrivial group G and a rectangular band B_δ and that the other completely simple components are rectangular bands. Suppose that G is not simple. There exists a proper normal subgroup N of G. Let $R'_\delta = N \times B_\delta$. Let J be a set defined by

$$\left(\bigcup_{\gamma \in \Gamma \setminus \{\delta\}} R_\gamma\right) \cup R'_\delta.$$

It is easy to see that J is a proper normal sub-orthocryptogroup of S. This is a contradiction. Therefore, G must be simple. □

Acknowledgments The author would like to express his gratitude to Miyuki Yamada for his kind guidance to the theory of semigroups. The author also thanks Yefim Katsov for pointing out some references. This work is supported by Grants-in-Aid for Scientific-Research Program 20540055.

References

1. Cohn, P.M.: Universal Algebra. Harper & Row, New York (1965)
2. Kurosh, A.G.: The Theory of Groups. Chelsea, New York (1960)
3. McKenzie, R.N., McNulty, G.E., Taylor, W.F.: Algebras, Lattices, Valieties. Wadsworth and Brooks/Cole, Monterey (1987)
4. Ore, O.: On the foundations of abstract algebra, II. Ann. Math. **37**, 265–292 (1936)
5. Petrich, M., Reilly, N.R.: Completely Regular Semigroups. Wiley-Interscience Publication, New York (1999)

6. Yamada, M., Kimura, N.: Note on idempotent semigroups II. Proc. Jpn. Acad. **34**, 110–112 (1958)
7. Yamada, M.: Strictly inversive semigroups. Bull. Shimane Univ. (Natl. Sci.) **13**, 128–138 (1964)
8. Yamada, M.: Normal systems in an orthogroup. Mem. Fac. Sci. Shimane Univ. **9**, 1–6 (1975)
9. Yamamura, A.: Completely regular semigroups satisfying formular for inverse of products (in preparation)

http://www.springer.com/978-981-10-1650-9

Algebra and its Applications
ICAA, Aligarh, India, December 2014
Rizvi, S.T.; Ali, A.; Filippis, V.D. (Eds.)
2016, XVI, 430 p., Hardcover
ISBN: 978-981-10-1650-9