数理解析研究所講究録
第 1769 巻 2011 年 23-32

Krull-Schmidt like decompositions of orthocryptogroups

Akihiro Yamamura
Akita University
e-mail: yamamura@ie.akita-u.ac.jp

Abstract

We introduce an internal spined product of orthocryptogroups and show that this coincides with the external spined product. Then we consider an internal spined product decomposition into indecomposable factors of an orthocryptogroup satisfying a certain finiteness condition. We obtain a Krull-Schmidt theorem like result for orthocryptogroups.

1 Introduction

Decomposing an algebraic system into indecomposable ones is an essential problem in mathematics. It is well-known that every semigroup can be decomposed into a subdirect product of subdirectrory indecomposable ones. On the other hand, a subdirect product and subdirectory indecomposable semigroups offer little information. In group theory (or module theory), the Krull-Schmidt theorem claims that if the ascending and descending chain conditions are satisfied, a group (module) has the direct product decompositions into indecomposable factors and the factors are unique. If a group G satisfies both ascending and descending chain conditions then it is decomposed into direct product $G = H_1 \times H_2 \times \cdots \times H_n$, where each H_i is direct product indecomposable, and if $G = K_1 \times K_2 \times \cdots \times K_m$ then $n = m$ and $H_i \cong K_i$ after reindexing. We consider the problem of extending the Krull-Schmidt theorem to a more general class of semigroups and show a similar result for orthocryptogroups.

A semigroup S is called *regular* if for each x in S there is an element x' in S such that $xx'x = x$ and $x'xx' = x'$. An element satisfying this property is called an *inverse* of x. An element e is called an *idempotent* if $e^2 = e$. A semigroup in which every element is an idempotent is called a *band*. A *semilattice* is a commutative band. If every element of a regular semigroup S belongs to a subgroup of S, then it is called a *completely regular*, that is, S is a union of groups, then any element x in S has a *group inverse* x^{-1}, that is, $xx^{-1} = x^{-1}x$, $xx^{-1}x = x$ and $x^{-1}xx^{-1} = x^{-1}$. A maximal subgroup containing an idempotent e is denoted by $S(e)$ and the set of the idempotents of S is denoted by $E(S)$. A regular semigroup S is called *orthogroup* if S is completely regular and its set of idempotents forms a band. A semigroup is called *Clifford* if it is an completely regular and the set of idempotents froms a semilattice. A semigroup is called *cryptic* if the Green's relation $\mathcal{H}$ is a congruence, and a completely regular semigroup which is cryptic is called a *cryptogroup*. An orthodox cryptogroup is called an *orthocryptogroup*. It is known that an orthocryptogroup is a band of groups whose set of idempotents forms a subband. A subsemigroup H of an orthocryptogroup S is called a *suborthocryptogroup* of S if H itself is an orthocryptogroup. It is easy to see that a non-empty subset H of an orthocryptogroup S is a suborthocryptogroup if $a, b \in H$, then $ab^{-1} \in H$.

Green's $\mathcal{H}$-relation of an orthocryptogroup S is the least band congruence β_S, and hence, S has the $\mathcal{H}$ decomposition $\bigcup_{e\in E(S)} S(e)$, where $S(e)$ is a subgroup containing the idempotent e. Note that $E(S)$ is the largest band image of S and $E(S) \cong S/\mathcal{H}$. We also remark that a Clifford semigroup C and a band B have the *structure decomposition* $\bigcup_{\gamma\in\Gamma} C_\gamma$, where C_γ is a subgroup of C and Γ is the structure semilattice, and $\bigcup_{\gamma\in\Gamma} B_\gamma$, where B_γ is a rectangular subband of B and Γ is the structure semilattice, respectively.

Suppose that S is an orthocryptogroup. It is known that an orthocryptogrouop S has the *$\mathcal{H}$-decomposition* $\bigcup_{e\in B} S(e)$, where B is the largest band image of S and $S(e)$ is a subgroup of S, and the *structure decomposition* $\bigcup_{\gamma\in\Gamma} S(\gamma)$, where Γ is the largest semilattice image of S and $S(\gamma)$ is a sub-rectangulargroup.

2 Spined products

2.1 External spined products

Suppose that $\phi_1 : S_1 \to Q$ and $\phi_2 : S_2 \to Q$ are homomorphisms of semigroups S_1 and S_2 onto a semigroup Q, respectively. The *external spined product over Q with respect to ϕ_1 and ϕ_2* is the subsemigroup of $S_1 \times S_2$ consisting of (s_1, s_2) where $\phi_1(s_1) = \phi_2(s_2)$, and denoted by $S_1 \bowtie_Q S_2$. An external spined product is just called a *spined product* in the literature of semigroup theory ([1, 3]) and sometimes called a *fibre product* or a *pullback* in category theory. In the rest of the paper, we consider external spined products, where Q is a band or a semilattice.

Let S and T be orthocryptogroups with the same largest band homomorphic image. Suppose that $\bigcup_{e\in B} S(e)$ and $\bigcup_{e\in B} T(e)$ are the $\mathcal{H}$-decomposition of S and T, respectively. Then the *external spined product of S and T with respect to $\mathcal{H}$* is the subsemigroup of $S \times T$ consisting of (s, t), where $s \in S(e)$, $t \in T(e)$ for some $e \in B$, and denoted by $S \bowtie_{\mathcal{H}} T$ (or $S \bowtie T$ if no confusion occurs). Likewise, if $S_1, S_2, \ldots, S_n$ have the same largest band homomorphic image, we define an external spined product of orthocryptogroups $S_1, S_2, \ldots, S_n$ with respect to $\mathcal{H}$ and denote it by $S_1 \bowtie_{\mathcal{H}} S_2 \bowtie_{\mathcal{H}} \ldots \bowtie_{\mathcal{H}} S_n$ (or $S_1 \bowtie S_2 \bowtie \ldots \bowtie S_n$ if no confusion occurs).

Similarly, we define the external spined product of S and T with respect to the structure decomposition. Suppose that $S \sim \sum\{S_\gamma \mid \gamma \in \Gamma\}$ and $T \sim \sum\{T_\gamma \mid \gamma \in \Gamma\}$ are the structure decomposition of S and T, respectively. Then the *external spined product of S and T with respect to* Γ is the subsemigroup of $S \times T$ consisting of (s, t), where $s \in S_\gamma$, $t \in T_\gamma$ for some $\gamma \in \Gamma$, and denoted by $S \bowtie_\Gamma T$ (or $S \bowtie T$ if no confusion occurs).

It is well-known that an external spined product of a Cifford semigroup and a band is an orthocryptogroup, and conversely every orthocryptogroup S is isomorphic to external spined product $C \bowtie_\Gamma E(S)$ of some Cifford semigroup C and the band $E(S)$ of idempotents of S over the structure semilattice Γ (see [3]).

2.2 Internal spined products

In group theory, an 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 and H_2 be $\{(g_1, 1) \mid g_1 \in G_1\}$ and $H_2 = \{(1, g_2) \mid g_2 \in G_2\}$, respectively. Then S is an *internal direct product* of H_1 and H_2; both H_1 and H_2 are normal subgroups of G and satisfy $H_1 \cap H_2 = 1$ and $H_1H_2 = G$. Equivalently, if elements of normal subgroups H_1 and H_2 commute and every element of G is uniquely written as a product of elements of H_1 and H_2 then G is an internal direct product of H_1 and H_2. Thus, the concepts of external and internal direct products are essentially identical and these are identified.

Now we shall introduce a concept of an *internal spined product* of semigroups. Unlike for groups, this does not coincide with the external spined product. For example, we will see the class of bands is not the case in the next section. However, the coincidence between external and internal direct product in group thoery can be extended to spined products of orthocryptogroups.

Let S be a semigroup and $\phi : S \to Q$ an epimorphism. Suppose S_1 and S_2 are subsemigroups such that $\phi(S_1) = \phi(S_2) = Q$. Then we can define the external spined product $S_1 \bowtie_Q S_2$. Recall that $S_1 \bowtie_Q S_2$ is a subsemigroup of $S_1 \times S_2$ consisting of (s_1, s_2) where $s_1 \in S_1$, $s_2 \in S_2$ and $\phi(s_1) = \phi(s_2)$. If $S_1 \bowtie_Q S_2$ is isomorphic to S under the mapping $(s_1, s_2) \mapsto s_1s_2$, where $s_1 \in S_1$ and $s_2 \in S_2$ satisfying $\phi(s_1) = \phi(s_2)$, then we say that S *is an internal spined product of S_1 and S_2* and denote $S = S_1 \bowtie_Q S_2$. An internal spined product is denoted just by $S_1 \bowtie S_2$ ($S_1 \bowtie_{\mathcal{H}} S_2$ or $S_1 \bowtie_\Gamma S_2$) if the context is unambiguous. Easily we can extend the definition to an *internal spined product* $S = S_1 \bowtie S_2 \bowtie \cdots \bowtie S_n$ of the finite family of subsemigroups $S_1, S_2, \ldots, S_n$ if S is isomorphic to the external spined product under the mapping $(s_1, s_2, \ldots, s_n) \mapsto s_1s_2\cdots s_n$, where $s_i \in S_i$ for every $i = 1, 2, \ldots, n$ satisfying $\phi(s_i) = \phi(s_j)$ for every i and j with $i \neq j$. Then the succeeding theorems imply external and internal direct products coincide for orthocryptogroups.

Theorem 2.1 *Let S be an orthocryptogroup. Suppose H and K are full suborthocryptogroups of S. Then S is an internal spined product $H \bowtie_{\mathcal{H}} K$ if and only if H and K satisfy the following.*

(a1) Elements of H and K commute.

(a2) Every element x of $S(e)$ $(e \in B)$ is uniquely expressed as $x = hk$ for some $h \in H(e)$ and $k \in K(e)$.

Proof. We suppose (a1) and (a2). Let S, H and K have the $\mathcal{H}$-decompositions $\bigcup_{e \in B} S(e)$, $\bigcup_{e \in B} H(e)$, and $\bigcup_{e \in B} K(e)$, respectively. Define a mapping ϕ of $H \bowtie_{\mathcal{H}} K$ into S by $(h,k)\phi = hk$ for $(h,k) \in H \bowtie_{\mathcal{H}} K$. We shall show that ϕ is an isomorphism of $H \bowtie_{\mathcal{H}} K$ onto S. Take any elements (a,p) and (b,q) of $H \bowtie_{\mathcal{H}} K$. Then, $((a,p)(b,q))\phi = (ab,pq)\phi = abpq = apbq = (a,p)\phi(b,q)\phi$ by (a1). Next, suppose that $(h_f,k_f)\phi = (h_e,k_e)\phi$ for $(h_f,k_f) \in H(f) \times K(f)$, $(h_e,k_e) \in H(e) \times K(e)$ and $f,e \in B$. It follows that $h_f k_f = h_e k_e \in H(f)K(f) \cap H(e)K(e) \subset S(f) \cap S(e)$. Therefore, $f = e$. Using (a2), we have $(h_f,k_f) = (h_e,k_e)$. Hence ϕ is injective. Furthermore, ϕ is surjective by (a2).

Conversely, if S is an internal spined product of H and K, then clearly (a1) and (a2) are satisfied. □

A suborthocryptogroup N of S is called *normal* if N is full and $x^{-1}Nx \subset N$ for every x in S. Then we define a relation ρ_N of S by $x \,\rho_N\, y$ for $x,y \in S$ if $x \mathcal{H} y$ and $xy^{-1} \in N$. It is easy to see that ρ_N is an idempotent separating congruence of S. Conversely, for every idempotent separating congruence ρ, the *kernel* $\{s \mid s \,\rho\, e, \text{ for some } e \in E(S)\}$ is a normal suborthocryptogroup.

Theorem 2.2 *Let S be an orthocryptogroup. Suppose H and K are full suborthocryptogroups of S. Then S is the internal spined product of H and K if and only if the following conditions hold.*

(b1) H and K are normal suborthocryptogroups in S,

(b2) $S = HK$,

(b3) $H \cap K = E(S)$.

Proof. We suppose that S, H and K have the structure decompositions $S \sim \sum\{S(e)|e \in B\}$, $H \sim \sum\{H(e)|e \in B\}$, and $K \sim \sum\{K(e)|e \in B\}$ respectively.

First we suppose S is an internal spined product, that is, H and K satisfy (a1) and (a2). Take an arbitrary element h of H (say $h \in H(f)$, $f \in B$). Let x be any element of S (say $x \in S_x i$, $b \in B$. By (a2), there exists elements a of $H(b)$ and p of K_b such that $x = ap$. It follows that $x^{-1}hx = p^{-1}a^{-1}hap = p^{-1}p(a^{-1}ha)$ by (a1) as $a^{-1}ha \in H$. It follows that H is a normal suborthocryptogroup in S. Similarly, K is a normal suborthocryptogroup. Obviously, (b2) is satisfied because of (a2). Now, take an arbitrary element x of $H \cap K$. Then there exists uniquely determined elements $f \in B$, $a \in H(f)$ and $b \in K(f)$ such that $x = ab$. Since x belongs to H, there exist elements $b \in B$ and $p \in H(b)$ such that $x = p$. Since x belongs to K, there exist elements $d \in B$ and $q \in K(d)$ such that $x = q$. Then we can write $x = ab = p1_b = 1_d q$. By (a2), we have $f = b = d$ and $a = 1_d, b = 1_b$, and hence, $x = 1_d 1_b \in B$. Thus, (b3) is satisfied.

Next, we suppose H and K satisfy the conditions (b1), (b2) and (b3). It is easy to see that $H(f)$ and $K(f)$ are normal subgroups of $S(f)$ for each f of B. Take an arbitrary element x of $S(f)$. By (b2), there exist elements $a \in H(b)$ and $b \in K(d)$ such that $x = ab$. It follows that $x = ab = (a1_{bd})(1_{bd}b)$. Then f is equal to bd and $a1_{bd}$ is in $H(f)$ and $1_{bd}b$ is in $K(f)$. Thus, $x \in H(f)K(f)$ and so $S(f) = H(f)K(f)$. By (b3), $H(f) \cap K(f) = \{1_f\}$. Hence $S(f)$ is the direct product of subgroups $H(f)$ and $K(f)$. Take arbitrary elements $a \in H(f)$ and $b \in K_b$. It follows that $ab = (a1_{fb})(b1_{fb}) = (b1_{fb})(a1_{fb}) = ba$ because $a1_{fb} \in H(fb)$, $b1_{fb} \in K(fb)$ and $S(fb) = H(fb) \times K(fb)$. Hence (a1) is satisfied. For any element x of S, there exists a unique element f of B such that $x \in S(f)$. Since $S(f) = H(f) \times K(f)$, there exists a unique pair of elements $h \in H(f)$ and $k \in K(f)$ such that $x = hk$. Hence, (a2) is also satisfied. □

It is easy to extend Theorem 2.2 as follows. Suppose $H_1, H_2, \ldots, H_n$ are full suborthocryptogroups of S. Then S is an *internal spined product* of them if and only if

(c1) Every H_i ($i = 1, 2, \ldots n$) is normal suborthocryptogroup in S

(c2) $S = \prod_{i=1}^{n} H_i$

(c3) $H_i \cap H_1 \cdots H_{i-1} H_{i+1} \cdots H_n = E(S)$ for every $i = 1, 2, \ldots n$.

3 Spined decompositions

In this section, we shall investigate spined product decompositions of orthocryptogroups into indecomposable factors. Note that an orthocryptogroup S admits a spined product decomposition $S = S \bowtie_{\mathcal{H}} E(S)$. We say that S and $E(S)$ are trivial spined product factors of S.

We shall give a sufficient condition for an orthocryptogroup to admit a spined product decompositions into indecomposavle factors. Let S be an orthocryptogroup. We say that S has *ascending chain condition* if every increasing chain of noraml systems stops; if $N_1 \subset N_2 \subset N_3 \subset \cdots$ is a chain of normal suborthocryptogroups of S, then there exists t for which $N_t = N_{t+1} = N_{t+2} = \cdots$. We say that S has *descending chain condition* if every decreasing chain of noraml systems stops; if $K_1 \supset K_2 \supset K_3 \supset \cdots$ is a chain of normal suborthocryptogroups of S, then there exists t for which $K_t = K_{t+1} = K_{t+2} = \cdots$. We say that S has both chain conditions if it has both ascending and descending chain conditions.

Theorem 3.1 *Let S be an orthocryptogroup having either chain condition. Then S is a spined product of a finite number of spined indecomposable orthocryptogroups.*

Proof. Suppose the conclusion of this lemma is not satisfied by S. Then S is not spined indecomposable and can be decomposed as $H_0 \bowtie L_0$, where H_0 and L_0 are proper suborthocryptogroups. Because of our assumption, either H_0 or L_0 are not spined indecomposable, say H_0. By induction, there is a sequence of suborthocryptogroups $H_0, H_1, H_2, \ldots,$

where every H_i is a proper spined factor of H_{i-1}. Then we have a descending chain $S \supsetneq H_0 \supsetneq H_1 \supsetneq H_2 \supsetneq \cdots$. If S has the descending chain condition, this is a contradiction. Now we suppose that S hsa the ascending chanin condition. Since eah H_i is a spined factor of H_{i-1}, there are normal suborthocryptogroups K_i such that $H_{i-1} = H_i \bowtie K_i$. Then there is an ascending chain $K_1 \subsetneq K_1 \bowtie K_2 \subsetneq K_1 \bowtie K_2 \bowtie K_3 \subsetneq \cdots$, which is a contradiction. □

Next we show the uniqueness of the decomposition in the following. An endomorphism ϕ of an orthocryptogroup S is said to be *idempotent fixed* if ϕ maps each idempotent to itself, that is, $e\phi = e$ for each element e of $E(S)$. For example, an endomorphism of S mapping each element x of S to xx^{-1} is normal. Such an endomorphism is denoted by 0. An endomorphism ϕ is called *nilpotent* if $\phi^k = 0$ for some k.

Let ϕ and ψ be idempotent fixed endomorphisms of S. Then we define a mapping $\phi+\psi$ by $x(\phi + \psi) = (x\phi)(x\psi)$ for $x \in S$. Note that $e(\phi + \psi) = e$ for every $e \in E(S)$. It is easy to see that $\phi + \psi$ is an idempotent fixed endomorphism if $(x\phi)(y\psi) = (y\psi)(x\phi)$ for any $x, y \in S$. Suppose that ϕ, ψ and η are idempotent fixed endomorphism of S. Then it is easy to see that following.

1. $(\phi + \psi) + \eta = \phi + (\psi + \eta)$

2. $(\phi + \psi)\eta = \phi\eta + \psi\eta$, and $\eta(\phi + \psi) = \eta\phi + \eta\psi$.

An endomorphism ϕ of an orthocryptogroup S is said to be *normal* if $(c^{-1}xc)\phi = c^{-1}(x\phi)c$ for any elements x and c of S. Suppose ϕ and ψ are normal idempotent fixed endomorphisms of S. It is easy to see the following.

1. $\phi\psi$ is a normal endomorphism.

2. If $\phi + \psi$ is an endomorphism of S, then $\phi + \psi$ is normal.

3. If ϕ is an automorphism of S, then ϕ^{-1} is normal.

4. If N is a normal suborthocryptogroup, then so is $N\phi$.

5. If $(x\phi)(y\psi) = (y\psi)(x\phi)$ for any $x, y \in S$, we have $\phi + \psi = \psi + \phi$.

Let $H_1, H_2, \ldots, H_n$ be orthocryptogroups having the same band homomorphic image B as the largest band image. Suppose that each H_i has the $\mathcal{H}$ decomposition $H_i \sim \sum\{H_i(e)|e \in B\}$ for each $i = 1, 2, \ldots, n$. Put $S = H_1 \bowtie_{\mathcal{H}} H_2 \bowtie_{\mathcal{H}} \cdots \bowtie_{\mathcal{H}} H_n$. The *projection* π_i is defined to be an endomorphism of S defined by $(x_1, \ldots, x_n)\pi_i = (1_e, \ldots, x_i, \ldots, 1_e)$, where $x_j \in H_j(e)$ for every $j = 1, 2, \ldots, n$. It is easy to see that π_i is a normal idempotent fixed endomorphism of S for every $i = 1, 2, \ldots, n$, and $\pi_i + \pi_j$ is an endomorphism of S for any i, j with $i \neq j$. Furthermore, it is easy to see that $\pi_1 + \pi_2 + \cdots + \pi_n$ is equal to the identity mapping of S and $\pi_i^2 = \pi_i$ and $\pi_i\pi_j = 0$ if $i \neq j$.

Let ϕ be an endomorphism of an orthocryptogroup S. We define Kerϕ to be the set $\{s \in S \mid s\phi \in E(S)\}$. It is easy to see that Kerϕ is a normal suborthocryptogroup of S.

Lemma 3.2 *Let S be an orthocryptogroup satisfying both chain conditions. Let ϕ be a normal idempotent fixed endomorphism of S.*
(1) ϕ is surjective if and only if ϕ is injective.
(2) If $S\phi = S\phi^2$, then S is the internal spined product $S\phi \bowtie_{\mathcal{H}} \mathrm{Ker}\phi$.

Proof. (1) Put $N = \mathrm{Ker}\phi$. First we suppose ϕ is surjective. It follows that $S = S\phi = S/(N,_N \phi^i)$. Since ϕ is idempotent fixed, $N\phi^i$ is the least semilattice congruence on N. Thus, $(N,_N \phi^i)$ is equal to N, and hence, S is isomorphic to S/N. Since the lengthof chief composition series is uniquely determined, we shall denote thelengthof chief composition series of S by $\ell(S)$. It follows that N has a normal chain $N = N_0 \subset N_1 \subset \cdots \subset N_r = E(S)$ such that N_i is a normal suborthocryptogroup in S for each $i = 0, 1, \ldots, r$ and there exists no normal suborthocryptogroup K_i in S such that $N_i \subset K_i \subset N_{i+1}$ for each $i = 0, 1, \ldots, r-1$, further, $\ell(S) = r + \ell(S/N)$. Since S is isomorphic to S/N, $\ell(S) = \ell(S/N)$. It follows that $r = 0$ and that $N = E(S)$. This implies that ϕ is injective.

Conversely, assume that ϕ is injective. Then $S\phi$ has a normal chain $S\phi = N_0 \supset N_1 \supset \cdots \supset N_r = E(S)$ such that N_i is a normal suborthocryptogroup in S for each $i = 0, 1, \ldots, r$, and there exists no normal suborthocryptogroup K_i in S such that $N_i \supset K_i \supset N_{i+1}$ for each $i = 0, 1, \ldots, r-1$, and $\ell(S) = r + \ell(S/S\phi)$. We shall show that the chain $S\phi = N_0 \supset N_1 \supset \cdots \supset N_r = E(S)$ is a chief composition series of S. Let K_i be a normal suborthocryptogroup in $S\phi$ such that $N_i \supset K_i \supset N_{i+1}$. It follows from that $K_i\phi^{-1}$ is a normal suborthocryptogroup in S. Take any elements c of S and x of K_i. There exists an element y of $K_i\phi^{-1}$ such that $y\phi = x$. It follows that $c^{-1}xc = c^{-1}(y\phi)c = (c^{-1}yc)\phi \in ((K_i\phi^{-1})^c)\phi \supset (K_i\phi^{-1})\phi = K_i$. This implies that K_i is a normal suborthocryptogroup in S. Then K_i is equal to N_i or N_{i+1}. Consequently, $S\phi = N_0 \supset N_1 \supset \cdots \supset N_r = E(S)$ is a chief composition series of S, and hence, $\ell(S) = \ell(S\phi) = r$. It follows that $\ell(S/S\phi) = 0$ and that $S = S\phi$.

(2) Assume that $S\phi = S\phi^2$. Then the restriction $\phi|_{S\phi}$ of ϕ to $S\phi$ is surjective. By the argument in the proof of part (1), $S\varphi$ has a chief composition series. It follows from (1) that $\phi|_{S\phi}$ is injective. Take any element z of $S\phi \cap N$. Then there exists an element x of S such that $x\phi = z$. Since $z\phi$ is an idempotent, $z\phi^2 = (z\phi)\phi = z\phi = (x\phi)\phi$. Thus, $x\phi = z\phi$, and hence, $z = x\phi$ is in $E(S)$. Accordingly, $S\phi \cap N = E(S)$.

Let S have the decomposition $S \sim \sum\{S(e) | e \in \Gamma\}$. Take any element x of S (say $x \in S(e)$). Since $S\phi = S\phi^2, S(e)\phi = S(e)\phi^2$. There exists an element y of $S(e)$ such that $x\phi = y\phi^2$. It follows that $(x(y^{-1}\phi))\phi = (x\phi)(y\phi^2)^{-1} = 1_e$, $x(y^{-1}\phi) \in 1_e\phi^{-1}$ and $x \in (1_e\phi^{-1})(y\phi) \subset N(S\phi)$. Hence, $S = (S\phi)N$. It follows that S is the internal spined product $S\phi \bowtie N$. □

Lemma 3.3 (A generalization of Fitting's lemma) *Let S be an orthocryptogroup having both chain conditions. Let ϕ be a normal idempotent fixed endomorphism of S. Then there exists a positive integer k such that $S = S\phi^k \bowtie \mathrm{Ker}\phi^k$.*

Proof. Obviously, $[S\phi^j]$ is a normal suborthocryptogroup in S for any positive integer j. Thus $S \supset S\phi \supset S\phi^2 \supset \cdots \supset S\phi^i \supset E(S)$ is a chief normal chain of S for each integer i. Since S has a chief composition series, there exists a positive integer k such that $S\phi^k = S\phi^{k+1}$. Then it follows that $S\phi^k = S\phi^{k+1} = S\phi^{k+2} = \cdots$, especially, $S\phi^k = S(\phi^k)^2$. It follows from Lemma 3.2 that $S = S\phi^k \bowtie \mathrm{Ker}\phi^k$. □

Lemma 3.4 *Let S be a spined indecomposable orthocryptogroup having both chain conditions and $S \supsetneq E(S)$.*
(1) If ϕ is a normal idempotent fixed endomorphism of S, then ϕ is either nilpotent or an automorphism of S.
(2) Let ϕ and ψ be normal idempotent fixed endomorphisms of S. If $\phi + \psi$ is an automorphism of S, then either ϕ or ψ is an automorphism of S.

Proof. (1) There exists a positive integer k such that $S = S\phi^k \bowtie N$ where $N = \mathrm{Ker}\phi^k$. Since S is spined indecomposable, $S\phi^k = E(S)$ or $N = E(S)$. The former implies that $\phi^k = 0$. The latter implies that ϕ^k is injective, and thus, ϕ^k is an automorphism and so is ϕ.

(2) Put $\eta = \phi + \psi$, $\phi_1 = \phi\eta^{-1}$ and $\psi_1 = \psi\eta^{-1}$. It follows that $1_S = (\phi + \psi)\eta^{-1} = \phi_1 + \psi_1$. Obviously, ϕ_1 and ψ_1 are normal idempotent fixed endomorphisms of S. Now, $\phi_1(\phi_1 + \psi_1) = \phi_1 1_S = 1_S\phi_1 = (\phi_1 + \psi_1)\phi_1$, and thus, $\phi_1^2 + \phi_1\psi_1 = \phi_1^2 + \psi_1\phi_1$. Take any element x of S (say $x \in S(e)$, where S has the structure decomposition $S \sim \sum\{S(e) | e \in \Gamma\}$. It follows that $(x\phi_1^2)(x\phi_1\psi_1) = x(\phi_1^2 + \phi_1\psi_1) = x(\phi_1^2 + \psi_1\phi_1) = (x\phi_1^2)(x\psi_1\phi_1)$ and that $x\phi_1\psi_1 = 1_e(x\phi_1\psi_1) = (x\phi_1^2)^{-1}(x\phi_1^2)(x\phi_1\psi_1) = (x\phi_1^2)^{-1}(x\phi_1^2)(x\psi_1\phi_1) = x\psi_1\phi_1$. Assume that neither ϕ nor ψ is an automorphism. Then neither ϕ_1 nor ψ_1 is an automorphism. It follows from (1) that there exist positive integers k and h such that $\phi_1^k = 0$ and $\psi_1^h = 0$. Put $n = max(k, h)$. Then $1_S = \phi_1 + \psi_1 = (\phi_1 + \psi_1)^{2n} = \sum_i^{2n} \phi_1^i \psi_1^{2n-1} = 0$. This contradicts to the fact that $E(S)$ is properly contained in S. Consequently, either ϕ or ψ is an automorphism. □

Theorem 3.5 (A generalization of Krull-Schmidt theorem) *Let S be an orthocryptogroup having both chain conditions. If S has two spined product decompositions $H_1 \bowtie H_2 \bowtie \cdots \bowtie H_m$ and $K_1 \bowtie K_2 \bowtie \cdots \bowtie K_n$, 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 $\{H_i | i = 1, 2, \ldots, m\}$ onto the family $\{K_i | j = 1, 2, \ldots, n\}$ such that H_i is isomorphic to $\Psi(H_i)$.*

Proof. Let us suppose $m \leq n$. We shall show that for each $r = 1, 2, \ldots, m$ there exists an automorphism ϕ_r of S such that $H_p\phi_r = K_{j(p)}$ for some $K_{j(p)}$ for any $p = 1, 2, \ldots, r$, and $\phi_r|_{H_{r+1}\bowtie\cdots\bowtie H_m}$ is the identity mapping on $H_{r+1} \bowtie \cdots \bowtie H_m$. We use an induction on r. Let π_i be the mapping of S onto K_i defined as follows: If an element x of S is written as $x = k_1k_2\cdots k_n$ where $k_i \in (K_i)_e$ for each $i = 1, 2, \ldots, n$, then $x\pi_i = k_i$, that is, π_i is the i-th projection. Put $L = H_2 \bowtie H_3 \bowtie \cdots \bowtie H_m$. Then $S = H_1 \bowtie L$. Let σ and ρ be the first and second projections of S, respectively. Obviously, π_i $(i = 1, 2, \ldots, n)$, σ and ρ are normal idempotent fixed endomorphisms of S. Then $\sigma = 1_S\sigma = (\pi_1 + \pi_2 + \cdots + \pi_n)\sigma =$

$\pi_1\sigma+\pi_2\sigma+\cdots+\pi_n\sigma$, $\sigma|_{H_1}: H_1 \to H_1$ is the identity mapping on H_1 and $\pi_i\sigma|_{H_1}: H_1 \to H_1$ is a normal idempotent fixed endomorphism of H_1. It follows from Theorem 4.3 that there exists a chief composition series $S = S_0 \supset S_1 \supset \cdots \supset S_i = H_1 \supset S_{i+1} \supset \cdots \supset S_r = E(S)$. It follows from Lemma 3.12 that $H_1 = S_i \supset S_{i+1} \supset \cdots \supset S_r = E(S)$ is a chief composition series of H_1. Hence H_1 has a chief composition series.

Since $\sigma|_{H_l} = \pi_1\sigma|_{H_1} + \cdots + \pi_n\sigma|_{H_1}$ is an automorphism of H_1, there is an integer i such that $\pi_i\sigma|_{H_1}$ is an automorphism of H_1. It follows that $H_1 = H_1\pi_i\sigma \subset K_i\sigma \subset H_1$, and that $H_1 = H_1\pi_i\sigma = K_i\sigma$. Then $K_i(\sigma\pi_i)^2 = K_i\sigma\pi_i\sigma\pi_i = H_1\pi_i\sigma\pi_i = K_i\sigma\pi_i$, and in general, $K_i\sigma\pi_i = K_i(\sigma\pi_i)^2 = K_i(\sigma\pi)^3 = \cdots$.

Suppose that $(\sigma\pi_i|_{K_i})^j = 0$ for some j. Then $H_1\pi_i = K_i\sigma\pi_i = K_i(\sigma\pi_i|_{K_i})^j = E(S)$ and so $H_1 = H_1\pi_i\sigma = E(S)\sigma = E(S)$, which contradicts to the fact that $H_1 \supsetneq E(S)$. Therefore, $(\sigma\pi_i|_{K_i})^j \neq 0$ for every j. By Lemma 3.3 (1), we have $\sigma\pi_i|_{K_i}$ is an automorphism of K_i.

Next, we show $\sigma\pi_i$ and ρ satisfy $(x\rho)(y\sigma\pi_i) = (y\sigma\pi_i)(x\rho)$ for any $x, y \in S$. Take elements $x, y \in S$. If $i \neq j$, then $(x\sigma\pi_i)(x\rho\pi_j) = (x\rho\pi_j)(x\sigma\pi_i)$ and $(x\sigma\pi_i)(y\rho\pi_i) = (y\rho\pi_i)(x\sigma\pi_i)$. Hence, $(x\rho)(y\sigma\pi_i) = (x\rho\pi_1)(x\rho\pi_2)\cdots(x\rho\pi_n)(y\rho\pi_j) = (y\rho\pi_j)(x\rho\pi_1)(x\rho\pi_2)\cdots(x\rho\pi_n) = (y\sigma\pi_i)(x\rho)$. Consequently, $\sigma\pi_i + \rho$ is a normal idempotent fixed endomorphism. Put $\phi = \sigma\pi_i + \rho$.

We shall show that $H_1\phi = K_i$. Take any element h of H_1 (say $h \in S_\delta$). Then, $h\phi = (h\sigma\pi_i)(h\rho) = (h\sigma\pi_i)1_\delta = h\sigma\pi_i \in K_i$. Conversely, take any element k of $K_i = H_1\pi_i$. There exists element h of H_1 (say $h \in S_\delta$, $\delta \in E(S)$) such that $h\phi = h\pi_i = k$. Hence, $k = h\phi \in H_1\phi$. Accordingly, $H_1\phi = K_i$.

Take any element x of $L = H_2 \bowtie \cdots \bowtie H_m$ (say $x \in S_\delta$). Then, $x\phi = (x\sigma\pi_i)(x\rho) = 1_\delta(x\rho) = x\rho = x$, and hence, $\phi|_{H_2\bowtie\cdots\bowtie H_m}$ is the identity mapping on $H_2 \bowtie \cdots \bowtie H_m$.

If y is an element of S such that $y\phi = 1_e$, then $1_e = y\phi = (y\sigma\pi_i)(y\rho)$, and thus, $1_e = 1_e\sigma = ((y\sigma\pi_i)(y\rho))\sigma = (y\sigma\pi_i\sigma)(y\rho\sigma) = y\sigma\pi_i\sigma$. Since $y\sigma$ is an element of H_1 and $\pi_i\sigma|_{H_1}$ is an automorphism of H_1, $(y\sigma)(\pi_i\sigma) = 1_e$ implies that $y\sigma = 1_e$. Hence, $1_e = (y\sigma\pi_i)(y\rho) = 1_e(y\rho) = y\rho$, and thus, $y = y1_S = y(\sigma+\rho) = (y\sigma)(y\rho) = 1_e1_e$. This implies that $\mathrm{Ker}\phi = E(S)$. Consequently, ϕ is injective. It follows from Lemma 3.1 that ϕ is an automorphism of S, and further, $H_1\phi = K_i$ and $\phi|_{H_2\bowtie\cdots H_m}$ is the identity mapping on $H_2 \bowtie \cdots \bowtie H_m$. Thus the result id true for $r = 1$.

Next, we suppose the result hold for any integer smaller than r. There exists an automorphism ϕ_{r-1} of S such that $H_i\phi_{r-1} = K_{j(i)}$ for any $i = 1, 2, \ldots, r-1$ and $\phi_{r-1}|_{H_r\bowtie\cdots\bowtie H_m}$ is the identity mapping on $H_r \bowtie \cdots \bowtie H_m$. Since $H_i = K_{j(i)}$ for any $i = 1, 2, \ldots, r-1$, $S = K_{j(1)} \bowtie \cdots \bowtie K_{j(r-1)} \bowtie H_r \bowtie \cdots \bowtie H_m = K_1 \bowtie \cdots \bowtie K_n$. By using a similar argument above, we obtain an automorphism ϕ'_r of S such that $H_r\phi'_r = K_{j(r)}$ for some $j(r)$ and $\phi'_r|_{K_{j(1)}\bowtie\cdots H_m}$ is the identity mapping on $K_{j(1)} \bowtie \cdots K_{j(r-1)} \bowtie H_{r+1} \bowtie \cdots \bowtie H_m$. Put $\phi_r = \phi_{r-1}\phi'_r$. Then ϕ_r is an automorphism of S such that $H_i\phi_r = K_{j(i)}$ for any $i = 1, 2, \ldots, r$ and $\phi_r|_{H_{r+1}\bowtie\cdots\bowtie H_m}$ is the identity mapping on $H_{r+1} \bowtie \cdots \bowtie H_m$. In case of $r = m$, we obtain an automorphism ϕ of S such that $H_i\phi = K_{j(i)}$ for any $i = 1, 2, \ldots, m$. Hence, $S = H_1 \bowtie H_2 \bowtie \cdots \bowtie H_m = K_{j(1)} \bowtie \cdots \bowtie K_{j(m)} \bowtie K_{j(m+1)} \bowtie \cdots \bowtie K_{j(n)}$ and $H_i = K_{j(i)}$ for any $i = 1, 2, \ldots, m$. This implies that $m = n$ since each K_j is not equal to $E(S)$. $\square$

A completely different approach is possible to obtain Krull-Schmidt like theorem using Ore's theorem in lattice theory. The proof using a lattice theoretic method will be published elsewhere [6].

References

[1] J.M.Howie, *Fundamentals of semigroup theory*, Clarendon Press, Oxford (1995).

[2] A.G.Kurosh, *The Theory of Groups*, Chelsea, New York (1960).

[3] M.Petrich and N.R.Reilly, *Completely regular semigroups*, Wiley-Interscience Publication (1999).

[4] D.J.S.Robinson, *A course in the theory of groups*, second edition, Springer-Verlag, (1996).

[5] J.J.Rotman, *An Introduction to the Theory of Groups*, Third edition, Wm C. Brown (1988).

[6] A.Yamamura, "Spined product decompositions of orthocryptogroups", (submitted)