<table>
<thead>
<tr>
<th>Title</th>
<th>Krull-Schmidt like decompositions of orthocryptogroups (Algebras, Languages, Algorithms and Computations)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Yamamura, Akihiro</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (2011), 1769: 23-32</td>
</tr>
<tr>
<td>Issue Date</td>
<td>2011-10</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/171487">http://hdl.handle.net/2433/171487</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
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 subdirectory 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 from 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 $\beta_S$, 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 $C_{\gamma}$ is a subgroup of $C$ and $\Gamma$ is the structure semilattice, and $\bigcup_{\gamma \in \Gamma} B_{\gamma}$, where $B_{\gamma}$ is a rectangular subband of $B$ and $\Gamma$ is the structure semilattice, respectively.

Suppose that $S$ is an orthocryptogroup. It is known that an orthocryptogroup $S$ 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 $\Gamma$ is the largest semilattice image of $S$ and $S(\gamma)$ is a sub-rectangular group.

2 Spined products

2.1 External spined products

Suppose that $\phi_1 : S_1 \rightarrow Q$ and $\phi_2 : S_2 \rightarrow Q$ are homomorphisms of semigroups $S_1$ and $S_2$ onto a semigroup $Q$, respectively. The external spined product over $Q$ with respect to $\phi_1$ and $\phi_2$ 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 $S \bowtie_{\mathcal{H}} T$ 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 $\Gamma$ 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 $S \bowtie_T T$ (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 $C \bowtie T. E(S)$ of some Cifford semigroup $C$ and the band $E(S)$ of idempotents of $S$ over the structure semilattice $\Gamma$ (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 $H_1 H_2 = G$. 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 those 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 theory 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 $(s_1, s_2) \mapsto s_1 s_2$, 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 $S_1 \bowtie S_2$ ($S_1 \bowtie_\Gamma S_2$ 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 $(s_1, s_2, \ldots, s_n) \mapsto s_1 s_2 \cdots s_n$, 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 $H \bowtie \Gamma K$ 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 $\phi$ of $H \triangleright\triangleleft K$ into $S$ by $(h,k)\phi = hk$ for $(h,k) \in H \triangleright\triangleleft K$. We shall show that $\phi$ is an isomorphism of $H \triangleright\triangleleft K$ onto $S$. Take any elements $(a, p)$ and $(b, q)$ of $H \triangleright\triangleleft K$. Then, $((a, p)(b, q))\phi = (ab, pq)\phi = abpq = (a, p)\phi(b, q)\phi$ 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 $\phi$ is injective. Furthermore, $\phi$ is surjective by (a2).

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

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 $\rho_N$ of $S$ by $x \rho_N y$ for $x, y \in S$ if $xH y$ and $xy^{-1} \in N$. It is easy to see that $\rho_N$ is an idempotent separating congruence of $S$. Conversely, for every idempotent separating congruence $\rho$, the kernel $\{s | s \rho e$, 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 that $S$ 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 $x \in S_a$, $b \in B$). 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 $x = ab = p1_b = 1_dq$. By (a2), we have $f = b = d$ and $a = 1_d, b = 1_b$, and hence, $x = 1_d1_b \in B$. 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 $b \in K(d)$. 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 $S = S \triangleright_{\mathcal{H}} E(S)$. 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 indecomposable factors. Let $S$ be an orthocryptogroup. We say that $S$ has ascending chain condition if every increasing chain of normal 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 normal 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 $H_0 \triangleright L_0$, 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 $S$ has the ascending chain condition. Since each $H_i$ 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 $K_1 \subsetneq K_2 \subsetneq K_3 \subsetneq \cdots$, which is a contradiction. 

Next we show the uniqueness of the decomposition in the following. An endomorphism $\phi$ of an orthocryptogroup $S$ is said to be idempotent fixed if $\phi$ 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 $\phi$ is called nilpotent if $\phi^k = 0$ for some $k$.

Let $\phi$ and $\psi$ 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 $\phi, \psi$ and $\eta$ are idempotent fixed endomorphisms 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 $\phi$ 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 $\phi$ and $\psi$ 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 $\phi$ is an automorphism of $S$, then $\phi^{-1}$ 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 $\pi_i$ 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 $\pi_i$ 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 $\phi$ be an endomorphism of an orthocryptogroup $S$. We define $\text{Ker}\phi$ to be the set $\{s \in S | s\phi \in E(S)\}$. It is easy to see that $\text{Ker}\phi$ is a normal suborthocryptogroup of $S$. 

Lemma 3.2 Let $S$ be an orthocryptogroup satisfying both chain conditions. Let $\phi$ be a normal idempotent fixed endomorphism of $S$.

(1) $\phi$ is surjective if and only if $\phi$ is injective.

(2) If $S\phi = S\phi^2$, then $S$ is the internal spined product $S\phi \bowtie_k \ker \phi$.

Proof. (1) Put $N = \ker \phi$. First we suppose $\phi$ is surjective. It follows that $S = S\phi = S\phi/(N_0\phi^i)$. Since $\phi$ is idempotent fixed, $N\phi^i$ is the least semilattice congruence on $N$. Thus, $(N_0\phi^i)$ is equal to $N$, and hence, $S$ is isomorphic to $S/N$. Since the length of chief composition series is uniquely determined, we shall denote the minimal length of 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 $\phi$ is injective.

Conversely, assume that $\phi$ 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 $c^{-1}xc = (c^{-1}yc)\phi \in (K_i\phi^{-1})\phi \supset (K_i\phi^{-1})\phi = K_i$. 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 $\phi$ to $S\phi$ is surjective. By the argument in the proof of part (1), $S\phi$ 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 $S\phi \bowtie_k N$.

Lemma 3.3 (A generalization of Fitting’s lemma) Let $S$ be an orthocryptogroup having both chain conditions. Let $\phi$ be a normal idempotent fixed endomorphism of $S$. Then there exists a positive integer $k$ such that $S = S\phi^k \bowtie_k \ker \phi^k$.

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 $S = S\phi^k \vartriangleright\triangleleft \text{Ker} \phi^k$.

**Lemma 3.4** Let $S$ be a spined indecomposable orthocryptogroup having both chain conditions and $S \supseteq E(S)$.

(1) If $\phi$ is a normal idempotent fixed endomorphism of $S$, then $\phi$ is either nilpotent or an automorphism of $S$.

(2) Let $\phi$ and $\psi$ be normal idempotent fixed endomorphisms of $S$. If $\phi + \psi$ is an automorphism of $S$, then either $\phi$ or $\psi$ is an automorphism of $S$.

**Proof.** (1) There exists a positive integer $k$ such that $S = S\phi^k \vartriangleright N$ where $N = \text{Ker} \phi^k$. 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 $\phi^k$ is injective, and thus, $\phi^k$ is an automorphism and so is $\phi$.

(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, $\phi_1$ and $\psi_1$ are normal idempotent fixed endomorphisms of $S$. Now, $\phi_1(\phi_1 + \psi_1) = \phi_1 1_S = (\phi_1 + \psi_1)\phi_1$, 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 $(x\phi_1^2)(x\psi_1) = x(\phi_1^2 + \phi_1\psi_1) = x(\phi_1^2 + \psi_1\phi_1) = (x\phi_1^2)(x\psi_1\phi_1)$ and that $x\phi_1\psi_1 = 1_e(x\phi_1\psi_1) = (x\phi_1^2)(x\phi_1\psi_1) = (x\phi_1^2)(x\psi_1\phi_1) = x\psi_1\phi_1$. Assume that neither $\phi$ nor $\psi$ is an automorphism. Then neither $\phi_1$ nor $\psi_1$ 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 $1_S = \phi_1 + \psi_1 = (\phi_1 + \psi_1)^{2n} = \sum_i \phi_1^i \psi_1^{2n-1} = 0$. This contradicts to the fact that $F(S)$ is properly contained in $S$. Consequently, either $\phi$ or $\psi$ 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 $H_1 \vartriangleright H_2 \vartriangleright \cdots \vartriangleright H_m$ and $K_1 \vartriangleright K_2 \vartriangleright \cdots \vartriangleright K_n$, 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 $\Psi$ of the family $\{H_i| i = 1, 2, \ldots, m\}$ onto the family $\{K_j| j = 1, 2, \ldots, n\}$ 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 $\phi_r$ of $S$ such that $H_p\phi_r = K_{j(p)}$ for some $K_{j(p)}$ for any $p = 1, 2, \ldots, r$, and $\phi_r|_{H_{r+1} \vartriangleright \cdots \vartriangleright H_m}$ is the identity mapping on $H_{r+1} \vartriangleright \cdots \vartriangleright H_m$. We use an induction on $r$. Let $\pi_r$ be the mapping of $S$ onto $K_r$ defined as follows: If an element $x$ of $S$ is written as $x = k_1 k_2 \cdots k_n$ where $k_i \in (K_i)_e$ for each $i = 1, 2, \ldots, n$, then $x\pi_i = k_i$, that is, $\pi_i$ is the $i$-th projection. Put $L = H_2 \vartriangleright H_3 \vartriangleright \cdots \vartriangleright H_m$. Then $S = H_1 \vartriangleright L$. Let $\sigma$ and $\rho$ be the first and second projections of $S$, respectively. Obviously, $\pi_i \ (i = 1, 2, \ldots, n)$, $\sigma$ and $\rho$ are normal idempotent fixed endomorphisms of $S$. Then $\sigma = 1_S\sigma = (\pi_1 + \pi_2 + \cdots + \pi_n)\sigma$ =
\(\pi_1 \sigma + \pi_2 \sigma + \cdots + \pi_n \sigma|_{H_1} : H_1 \rightarrow H_1\) is the identity mapping on \(H_1\) and \(\pi_i \sigma|_{H_1} : H_1 \rightarrow H_1\) 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 \(\sigma|_{H_1} = \pi_1 \sigma|_{H_1} + \cdots + \pi_n \sigma|_{H_1}\) 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 \(H_1 = H_1 \pi_i \sigma \subset \pi_i \sigma \subset H_1\), 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, \(K_i \sigma \pi_i = K_i(\sigma \pi_i)^2 = K_i(\sigma \pi_i)^3 = \ldots\).

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

Next, we show \(\pi_i \) and \(\rho\) satisfy \((x \rho \pi_i) = (y \rho \pi_i)(x \rho)\) for any \(x, y \in S\). Take elements \(x, y \in S\). If \(i \neq j\), then \((x \sigma \pi_i)(x \pi_j) = (x \pi_j)(x \sigma \pi_i)\) and \((x \sigma \pi_i)(y \pi_i) = (y \pi_i)(x \sigma \pi_i)\). Hence, \((x \pi_j)(y \pi_i) = (x \pi_j)(y \pi_i)\).

 Consequently, \(\pi_i + \rho\) is a normal idempotent fixed endomorphism. Put \(\phi = \sigma \pi_i + \rho\).

We shall show that \(H_i \phi = K_i\). Take any element \(h\) of \(H_1\) (say \(h \in S_0\)). Then, \(h \phi = (h \sigma \pi_i)(h \rho) = (h \sigma \pi_i)1 = h \sigma \pi_i \in K_i\). Conversely, take any element \(k\) of \(K_i = H_i \pi_i\). There exists element \(h\) of \(H_1\) (say \(h \in S_3, \delta \in E(S)\)) such that \(h \phi = h \pi_i = k\). Hence, \(k = h \phi \in H_i \phi\). Accordingly, \(H_i \phi = K_i\).

Take any element \(x\) of \(L = H_2 \cdots H_m\) (say \(x \in S_3\)). Then, \(x \phi = (x \sigma \pi_i)(x \rho) = 1\).

If \(y\) is an element of \(S\) such that \(y \phi = 1\), then \(x \phi = (x \sigma \pi_i)(x \rho)\), and thus, \(1 = (y \sigma \pi_i)(y \rho)\).

Consequently, \(\phi = E(S)\). It follows from Lemma 3.1 that \(\phi\) is an automorphism of \(S\), and further, \(H_i \phi = K_i\) and \(\phi|_{H_2 \cdots H_m}\) is the identity mapping on \(H_2 \cdots H_m\). Thus the result id true for \(r = 1\).

Next, we suppose the result hold for any integer smaller than \(r\). There exists an automorphism \(\phi_{r-1}\) of \(S\) such that \(H_i \phi_{r-1} = K_{j(i)}\) for any \(i = 1, 2, \ldots, r - 1\) and \(\phi_{r-1}|_{H_r \cdots H_m}\) is the identity mapping on \(H_r \cdots H_m\). Since \(H_i = K_{j(i)}\) for any \(i = 1, 2, \ldots, r - 1, S = K_{j(1)} \cdots K_{j(r-1)} \cdots H_r \cdots H_m = K_1 \cdots K_n\). By using a similar argument above, we obtain an automorphism \(\phi_r\) of \(S\) such that \(H_r \phi_r = K_{j(r)}\) for some \(j(r)\) and \(\phi_r|_{K_{j(1)} \cdots H_m}\) is the identity mapping on \(K_{j(1)} \cdots H_r\). Put \(\phi_r = \phi_{r-1}\).

Then \(\phi_r\) is an automorphism of \(S\) such that \(H_i \phi_r = K_{j(i)}\) for any \(i = 1, 2, \ldots, r\) and \(\phi_r|_{H_{r+1} \cdots H_m}\) is the identity mapping on \(H_{r+1} \cdots H_m\). In case of \(r = m\), we obtain an automorphism \(\phi_m\) of \(S\) such that \(H_i \phi = K_{j(i)}\) for any \(i = 1, 2, \ldots, m\). Hence, \(S = H_1 \cdots H_m = K_{j(1)} \cdots K_{j(m)}\) 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 \(E(S)\).
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


