<table>
<thead>
<tr>
<th>Title</th>
<th>On splitting of a factor set in a ring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Nobusawa, Nobuo</td>
</tr>
<tr>
<td>Citation</td>
<td>Osaka Journal of Mathematics. 7(1) P.77-P.80</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1970</td>
</tr>
<tr>
<td>Text Version</td>
<td>publisher</td>
</tr>
<tr>
<td>URL</td>
<td><a href="https://doi.org/10.18910/6070">https://doi.org/10.18910/6070</a></td>
</tr>
<tr>
<td>DOI</td>
<td>10.18910/6070</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
</tbody>
</table>
ON SPLITTING OF A FACTOR SET IN A RING

Dedicated to Professor Keizo Asano on his 60th birthday

NOBUO NOBUSAWA

(Received October 6, 1969)

1. Introduction

In [1] and [2], the present author developed the theory of crossed products, especially, the splitting property of factor sets in division and simple rings. If one takes a close look at the proofs given in these works, one can find a few simple principles making all the results obtainable. The purpose of this note is to give a simpler proof of a generalized theorem in case of a general ring. Let $R$ be a ring with unity $1$ and $G$ a finite automorphism group of $R$. A factor set $\{c_{\sigma, \tau}\}$ is defined to be a system of units $c_{\sigma, \tau}$ ($\sigma, \tau \in G$) in the center of $R$ such that

$$\text{(1)} \quad c_{\sigma, \rho} c_{\sigma, \tau} = c_{\sigma, \tau} c_{\sigma, \rho} \quad (\sigma, \tau, \rho \in G).$$

The factor set $\{c_{\sigma, \tau}\}$ is called splitting if one can find $d_{\sigma}$ in the center of $R$ such that

$$\text{(2)} \quad d_{\tau} = d_{\tau^{-1}} c_{\sigma, \tau}.$$

A theorem we want to establish is that there exist a subring $B'$ in $R$ containing the fixed subring $S$ and a (skew-) Kronecker product of $R$ and $B'$ over $S$ so that $\{c_{\sigma, \tau}\}$ becomes splitting, provided $R$ satisfies some Galois conditions which we shall discuss in 2.

2. Galois conditions

Denote $G=\{\sigma, (=\text{the identity}), \sigma_2, \ldots, \sigma_n\}$. $S$ denotes a subring of $R$ consisting of all elements $t$ in $R$ such that $t^\sigma = t$ for all $\sigma$ in $G$. Consider the following conditions.

[I] There exist $u_1, \ldots, u_n, v_1, \ldots, v_n$ in $R$ such that $\sum_i v_i^\sigma u_i = 0$ unless $\sigma = \sigma_1$, and $=1$ in the latter case.

[II] The elements $u_i$ and $v_j$ in [I] satisfy $\sum_\sigma (u_i v_j)^\sigma = \delta_{i,j}$. 

The conditions [I] and [II] are used, in the following, to prove the main theorem in a very effective way. But the true meaning of them lies in that $R$ satisfies [I] and [II] if
Here $R_r$ stands for the ring of right multiplication by elements of $R$, and $S_l$ the ring of left multiplication by elements of $S$. In this note, we apply operators from right. For example, $t \cdot a_{r, \sigma} = (ta)^\sigma$. Now let us prove that $[\Gamma']$, $[\Pi']$ and $[\Pi']$ imply $[I]$ and $[II]$. Due to $[\Pi']$, every $S_l$ homomorphism $\phi$ of $R$ to $R$ is in $R_r G$ and hence $\phi = \sum a_{r, i} \sigma_i$ with $a_i$ in $R$. Moreover, if $\phi$ maps $R$ to $S$, then $t \phi$ is in $S$, i.e., $(t \phi)^\sigma = t \phi$ for all $t$ in $R$. But this implies $(\sum a_{r, i} \sigma_i)^\sigma = \sum a_{r, i} \sigma_i$. From the condition $[\Pi']$, we have $a_1 = \cdots = a_n$. Therefore, $\phi = a_r (\sum \sigma)$ with an element $a$. Especially, $S_l$ homomorphisms which map $u_i$ to 1 and $u_j$ ($j \neq i$) to 0 (which are possible because of $[\Gamma']$) are expressed as $v_i (\sum \sigma)$ with $v_i$ in $R$. Now $[I]$ follows, since $\sum v_i (\sum \sigma) u_{ir} = 1$ in $GR_r$ and the left hand term is $\sum \sigma \sum (v_i)^\sigma u_{ir}$ and then we use $[\Pi']$. $[II]$ is an immediate consequence of the definition of $v_i (\sum \sigma)$, because then $u_{ir} v_i (\sum \sigma) = \delta_i, j$ which implies $\sum (u_{ir} v_i) = \delta_i, j$. Conversely, suppose $[I]$ and $[II]$. Set $s_{t, i} = \sum_t (tv_i)^\sigma$ for an element $t$ in $R$. We have $\sum s_{t, i} u_i = \sum_t (tv_i)^\sigma u_i = \sum_t t (\sum \sigma v_i u_i) = t$ by $[I]$. On the other hand, if $\sum s_{t, i} u_i = 0$ for $s_{t, i} u_i = 0$ for $s_{t, i} u_i = 0$ then $0 = \sum \sigma \sum s_{t, i} u_i = \sum \sigma \sum s_{t, i} (u_{ir} v_i) = s_{t, i}$ for every $j$, which shows the condition $[\Gamma']$ is satisfied. $[II]$ also implies that $v_i (\sum \sigma)$ map $u_i$ to 1 and $u_j$ to 0, so that under the assumption $[\Gamma']$ the condition $[\Pi']$ is satisfied.

3. Polynomial ring $R[x_1, \cdots, x_n, x_1^{-1}, \cdots, x_n^{-1}]$

Let $x_1, \cdots, x_n$ be $n-1$ variables. For the sake of convenience, we set $x_1 = 1$. We consider a polynomial ring $A = R[x_1, \cdots, x_n, x_1^{-1}, \cdots, x_n^{-1}]$, where $x_1, \cdots, x_n$ are supposed to be in the center of the ring. Every element of $A$ is a sum of a finite number of monomials $a(i_1, \cdots, i_n) x_1^{i_1} \cdots x_n^{i_n}$ where $i_j$ are some positive or negative integers and $a(i_1, \cdots, i_n)$ are elements in $R$. Now, corresponding to a given factor set $\{c_{\sigma, \tau}\}$, we shall extend the automorphism group $G$ of $R$ to one of $A$ as follows. First, write $x_i = x_{\sigma, r}$. We define

$$x_{\sigma, r}^\tau = x_{\tau, r}^{-1} x_{\sigma, r} c_{\sigma, \tau} \quad (\sigma, \tau \text{ in } G).$$

Without losing generality, we suppose $c_{\sigma, r} = 1$ if $\sigma = \sigma_i$ or $\tau = \sigma_i$. Thus $x_{\sigma, r} = x_{\sigma, r}$. Then, in a natural way, an automorphism $\tau$ of $R$ in $G$ is extended to a homomorphism of $A$ to $A$. If $\tau$ and $\rho$ are two elements in $G$, we can show that $(x_{\sigma, r})^\rho = x_{\sigma, r}^\rho$ by following routine computation. $(x_{\sigma, r})^\rho = (x_{\sigma, r})^{-1} x_{\sigma, r}^\rho = x_{\rho, r} x_{\rho, r}^{-1}$.
SPLITTING OF A FACTOR SET IN A RING

By making use of (1). Especially, for $\rho=\tau^{-1},$ we have $(x_i^p)^{-1}=x_{\rho},$ showing $\tau^{-1},$ and hence every element of $G$ gives an automorphism of $A$ (i.e., an onto-monomorphism). Thus $G$ is extended to an automorphism group of $A$ isomorphic to $G,$ for which we use the same letter $G.$

Denote the fixed subring of $A$ (by $G$) by $B.$ Important is that $A/B$ is a Galois extension satisfying [I] and [II]. Therefore by the discussion in 2, $A=BU_1 \oplus \cdots \oplus Bu_n$ (direct). This result is a successful consequence of rather technical conditions [I] and [II]. Note also that in the former papers [1] and [2] a quotient ring of a usual polynomial ring was used, the existence of which in general case might be a problem. Here we can avoid the use of it. Returning to $A,$ in the following, we express elements of $A$ by $\sum b_iu_i$ with $b_i$ in $B.$ The uniqueness of the expression has been guaranteed in the above.

4. (Skew-) Kronecker products and the final result

Set $P(B)={f(x_1,\cdots,x_n,x_1^{-1},\cdots,x_n^{-1})|f(1,\cdots,1,1,\cdots,1)=0},$ and $P=\{\sum b_iu_i\in A|b_i\in P(B)\}.$

Lemma. $P$ is an ideal of $A.$

Proof. It is sufficient to show that $u_ip\in P$ for every element $p$ of $P(B)$ $(i=1,\cdots,n).$ To do so, express $u_ip=\sum b_ku_k$ with $b_k$ in $B.$ Then, $\sum (u_ipv_j)^{\sigma}=$ $=\sum \sum (b_ku_kv_j)^{\sigma}=b_j.$ But $\sum (u_ipv_j)^{\sigma}=$ $=\sum u_i^p\sigma v_j$ become 0 if we set $x_i=\cdots=x_n=1,$ showing $b_j\in P(B).$ This completes the proof.

Now, we consider the residue class ring $A/P$ and denote it by $A'.$ Let us investigate $A'$ more closely. First of all, we have $R\cap P=0.$ Therefore we may identify $R$ with its isomorphic image in $A'.$ Secondly, we see that $P$ is invariant under $G$ as a whole. Therefore, $G$ induces an automorphism group of $A'.$ Observing the effect of $G$ on $R$ in $A',$ the group is seen to be isomorphic to $G,$ so we identify both. The question is, what is the fixed subring? Before discussing that question, we investigate the homomorphic image of $B$ in $A'.$ Let $1=\sum c_iu_i$ with $c_i$ in $S.$ Then every element $b$ of $B$ is expressed as $\sum b_iu_i$ where $b_i=bc_i.$ This implies $b$ is contained in $P$ if and only if $bc_i\in P(B),$ namely, $b\in P(B).$ Thus we may identify $B/P(B)$ with a homomorphic image of $B$ in $A'.$ We denote this by $B'.$ In this case, every element of $A'$ is uniquely expressed as $\sum b_iu_i$ with $b_i$ in $B'.$ That is, $A'=B'u_1\oplus \cdots \oplus B'u_n$ (direct).

On the other hand, $B'$ is obviously contained in the fixed ring of $G$ in $A'.$ Comparing with the discussion in 2, we see that the fixed subring coincides with $B'.$ Here, note that even in $A'$ the conditions [I] and [II] hold. From the above, we also have that $B'\cap R=S.$ $A'$ is, thus, a (skew-) Kronecker product of $R$ and $B'$ over $S,$ (if we may give such a definition.) Now we are in a
position to conclude our final goal. Recalling the definition of $P$, we can see that $x_\sigma$ as well as $x'_\sigma$ are not contained in $P$. Denote the elements of $A'$ represented by $x_\sigma$ by $d_\sigma$. From (3), we have the identities (2).

**Main theorem.** Let $R/S$ be a Galois extension satisfying [I] and [II], and let $\{c_{\sigma, \tau}\}$ be a factor set. Then there exists a subring $B'$ in $R$ containing $S$ such that we can construct a (skew-) Kronecker product of $B'$ and $R$ over $S$ and that this Kronecker product $A'$ is a Galois extension over $B'$ satisfying [I] and [II] (with the same Galois group with that of $R/S$). In $A'$, the factor set $\{c_{\sigma, \tau}\}$ is splitting.

**References**
