CROSSED PRODUCTS OF SIMPLE RINGS

NOBUO NOBUSAWA

Let A be the algebra of all $q\times q$ matrices over a division ring D. Suppose there is given a group G of n automorphisms of A such that

(i) the fixed subring S of G is a simple ring such that $[A:S]=n$ and

(ii) GA_r coincides with the totality of all homomorphisms of the S-left module A to itself where A_r is the ring of right multiplication of elements of A.

Suppose also that there is given a factor system $\{c_{\sigma,\tau}\}(\sigma, \tau\in G)$ in the center K of A. Then a crossed product of A and G is defined via the same formulae as in the commutative case. (See [2].) The purpose of this note is to investigate the splitting property of a factor system by an extension of S as well as of A. This is a generalization of a well-known theorem for the commutative case as well as of a result given in [2].

To begin with, we shall consider a purely transcendental extension of A as follows. Let $x_1, \cdots, x_m$ be m variables. Let $D[x_1, \cdots, x_m]$ be the polynomial ring of $x_1, \cdots, x_m$ over D. We suppose x_i lie in the center of the ring. Then the quotient division ring of $D[x_1, \cdots, x_m]$ is denoted by $D(x_1, \cdots, x_m)$. The existence of the quotient ring is clear from a general theory of quotient ring, or it can be proved directly as follows. Generally let Γ be a ring with no divisor of zero. Moreover suppose that for any nonzero elements a and b of Γ there exist nonzero elements a', b', a'' and b'' such that $aa'=bb'$ and $a''a=b''b$. We consider the set of formal elements $a^{-1}b$ and cd^{-1} ($a, b, c, d\in\Gamma$ and $a\neq 0$, $d\neq 0$). Define $a_1^{-1}b_1=a_2^{-1}b_2$ if and only if there exist nonzero elements c and d such that $a_1c=b_1d$ and $a_2c=b_2d$. It is a good exercise to show that the above equivalent relation is well defined. Similarly, define $b_1a_1^{-1}=b_2a_2^{-1}$ if and only if there exist nonzero elements c and d such that $ca_1=db_1$ and $ca_2=db_2$. Also define $a^{-1}b=cd^{-1}$ if and only if $ac=bd$. To verify that this is well defined is also a good exercise. How to define the algebraic operations in this set is now almost clear. For example, $(a^{-1}b)(c^{-1}d)=(c'a)^{-1}b'd$, where $bc^{-1}=c'^{-1}b'$. Also, $a^{-1}b+c^{-1}d=(c''a)^{-1}(c''b+a''d)$, where $ac^{-1}=c''^{-1}a''$. The set is a division ring called a quotient ring of Γ and it is uniquely determined up to isomorphism. To apply this general theory to our case, we must verify that the above mentioned conditions of Γ are satisfied for $D[x_1, \cdots, x_m]$. To see it, take $D[x_1]$ first. The above

Received by the editors September 10, 1968 and, in revised form, April 14, 1969.

conditions of Γ are easy consequences of the division algorithm in $D[x_1]$. The general case can be proved easily by induction. Thus $D(x_1, \cdots, x_m)$ is constructed. Then we let $A(x_1, \cdots, x_m)$ be the algebra of all $q\times q$ matrices over $D(x_1, \cdots, x_m)$.

The next step is to extend G to an automorphism group of $A(x_1, \cdots, x_m)$. We set $m=n-1$ and let $G=\{\sigma_0=\epsilon, \sigma_1, \cdots, \sigma_m\}$. ($\epsilon$ is the identity.) We rather denote x_i by x_σ $(\sigma=\sigma_i)$ and set $x_\epsilon=1$. Now define

$$x_\sigma^\tau = x_\tau^{-1} x_{\sigma\tau} c_{\sigma,\tau} \tag{1}$$

for a given factor system $\{c_{\sigma,\tau}\}$, where we may assume without losing generality that $c_{\sigma,\epsilon}=c_{\epsilon,\sigma}=1$. This is of course one of classical devices in the theory of factor sets. Using the identities $c_{\tau,\rho}^{-1}c_{\sigma\tau,\rho}c_{\sigma,\tau}^{\rho}=c_{\sigma,\tau\rho}$, we can prove that $(x_\sigma^\tau)^\rho=x_\sigma^{\tau\rho}$. Operating τ on elements of A as usual, we get automorphisms of $A(x_1, \cdots, x_m)$. (The mappings τ are first defined on $D[x_1, \cdots, x_m]$, and then we generalize them on $D(x_1, \cdots, x_m)$ by setting $(a^{-1})^\tau=(a^\tau)^{-1}$ for a in $D[x_1, \cdots, x_m]$.) Thus G is considered to be an automorphism group of $A(x_1, \cdots, x_m)$. Moreover, what is more important, G is a group of outer automorphisms of $A(x_1, \cdots, x_m)$ since every element except the identity of G acts nontrivially on the center $K(x_1, \cdots, x_m)$ of the ring.

Now we are at the position to apply an elementary part of (outer) Galois theory of simple rings. (See [**1**].) If we denote the fixed subring of G by B, B is a simple ring and $[A(x_1, \cdots, x_m): B]=n$ [**1**, Theorem 1, p. 282]. Moreover, if we denote by $u_1, \cdots, u_n$ a basis of the S-left module A, then it is also a basis of the B-left module $A(x_1 \cdots, x_m)$. The main object of constructing the Galois extension $A(x_1, \cdots, x_m)/B$ was in that the factor system $\{c_{\sigma,\tau}\}$ splits in it as is seen from (1). However, the above result is still not satisfactory because B is too general. What we wish to get is a Galois extension A'/B' with B' in A in which $\{c_{\sigma,\tau}\}$ splits. The natural way to get such B' is a specialization method in a sense of algebraic geometry.

A brief discussion of specialization is as follows. Let $R\{t\}$ be a ring of all formal power series for a ring R and a variable t, i.e., elements of $R\{t\}$ are $\sum_{i=-\infty}^{\infty} r_it^i$ where almost all r_i are supposed to be 0 for negative integers i. We define a mapping of $R\{t\}$ to R and a symbol ∞; map $\sum r_it^i$ to r_0 if all $r_i=0$ for negative i, and to ∞ otherwise. Returning to $D(x_1, \cdots, x_m)$, set $t_i=x_i-1$ $(i=1, \cdots, m)$, and therefore $D(x_1, \cdots, x_m)=D(t_1, \cdots, t_m)$. Then embed $D(t_1, \cdots, t_m)$ into the formal power series (division) ring $D\{t_1\} \cdots \{t_m\}$ in a natural way. (First embed $D(t_1)$ into $D\{t_1\}$, then $D(t_1, t_2)$ into $D\{t_1\}\{t_2\}$, and so on.) On the other hand, we can generalize the above mentioned specialization to a case of several variables as follows. First, apply the above process to $R\{t_m\}$, where $R=D\{t_1\} \cdots \{t_{m-1}\}$. Next, map $R=R'\{t_{m-1}\}$ to R' and ∞, where $R'=D\{t_1\} \cdots \{t_{m-2}\}$. Continuing this process in this order, we get a mapping of $D\{t_1\} \cdots \{t_m\}$ to D and ∞. (∞ is always mapped to ∞.) The mapping is called a specialization induced by $x_m \to 1$, $x_{m-1} \to 1, \cdots$, and $x_1 \to 1$ (in this order). Restrict the mapping to the subset $D(x_1, \cdots, x_m)$, we get a specialization of it. To extend it to $A(x_1, \cdots, x_m)$, simply map each entry of a matrix to get a matrix whose entries are either elements of D or ∞. If ∞ appears in a result, we set the result ∞.

Now let B' be the finite image of B in the specialization. Clearly $S \subseteq B' \subseteq A$. Denote the totality of elements of B that have finite images in the specialization by $V(B)$, and the totality of elements of B that are mapped to 0 by $P(B)$. Set

$$U = \left\{ \sum_i b_i u_i \mid b_i \in V(B),\ i = 1, \cdots, n \right\}$$

and

$$P = \left\{ \sum_i p_i u_i \mid p_i \in P(B),\ i = 1, \cdots, n \right\}.$$

LEMMA. *U is a ring and P is an ideal of U.*

PROOF. To prove lemma, it is sufficient to show that $u_i b \in U$ and $u_i p \in P$, where $b \in V(B)$ and $p \in P(B)$. We need some preparation. Observing the condition (ii) of A, we see that every S-left homomorphism ϕ of A to S is expressed as $\phi = \sum a_{ir}\sigma_i$ ($a_i \in A$) and $(a\phi)^\sigma = a\phi$ for every σ in G. Therefore, $a_1 = a_2 = \cdots = a_n$, or $\phi = a_r(\sum \sigma_i)$ with an element a. Especially S-left homomorphisms which map u_j to 1 and $u_i (i \neq j)$ to 0 are expressed as $v_{jr}(\sum \sigma_k)$ with some elements v_j. This implies $\mathrm{Tr}_G(u_i v_j) = \delta_{ij}$. Returning to the proof of lemma, express $u_i b = \sum b_k u_k$ with b_k in B. Then $\mathrm{Tr}_G(u_i b v_j) = b_j$. But $\mathrm{Tr}_G(u_i b v_j) \in V(B)$ if $b \in V(B)$. This shows that $u_i b$ is contained in U. A similar discussion shows that $u_i p \in P$, which concludes the proof.

Lastly, we can show that x_σ are in U but not in P. For, set $x_\sigma = \sum b_i u_i$. As in above, $b_i = \mathrm{Tr}_G(x_\sigma v_i)$, the latter being in $V(B)$ since $x_\sigma^\tau v_i^\tau$ are mapped to $c_{\sigma,\tau} v_i^\tau$, namely, have finite images. Thus $x_\sigma \in U$. Clearly x_σ are not in P. Now, we consider the residue class ring $A' = U/P$. Since G induces an automorphism group of U as well as that of P, it induces an automorphism group of A'. The fixed subring of G in U/P is identified with B'. Moreover, if we denote the residue classes represented by x_σ by x'_σ, then $x'^{\tau}_{\sigma}=x'^{-1}_{\tau}x'_{\sigma\tau}c_{\sigma,\tau}$ in A'. Thus we have obtained a final result.

THEOREM. *The factor system* $\{c_{\sigma,\tau}\}$ *splits in* A'/B'.

REFERENCES

1. T. Nakayama, *Galois theory of simple rings*, Trans. Amer. Math. Soc. **73** (1952), 276–292. MR **14**, 240.

2. N. Nobusawa, *On crossed products of division rings*, Nagoya Math. J. **35** (1969), 47–51.

UNIVERSITY OF HAWAII