N. Nobusawa
Nagoya Math. J.
Vol. 35 (1969), 47–51

ON A CROSSED PRODUCT OF A DIVISION RING

NOBUO NOBUSAWA

1. Let R and C be a ring and its center, and G an automorphism group of R of order n. By a factor set $\{c_{\sigma,\tau}\}$, we mean a system of regular elements $c_{\sigma,\tau}$ $(\sigma,\tau \in G)$ in C such that

$$(1) \qquad c_{\sigma,\tau\rho}c_{\tau,\rho} = c_{\sigma\tau,\rho}c_{\sigma,\tau}^{\rho} .$$

A crossed product $W = W(R, G, \{c_{\sigma,\tau}\})$ is a ring containing R such that $W = \sum_{\sigma\in G} u_\sigma R$ (direct) with regular elements u_σ and $au_\sigma = u_\sigma a^\sigma$ for a in R and $u_\sigma u_\tau = u_{\sigma\tau}c_{\sigma,\tau}$. As usual, we identify $W(R, G, \{c_{\sigma,\tau}\})$ and $W(R,G, \{c'_{\sigma,\tau}\})$ when $c_{\sigma,\tau}$ and $c'_{\sigma,\tau}$ are cohomologous (in C). When $c_{\sigma,\tau} = 1$, the crossed product is called splitting. In this note, we shall deal with a division ring D as R, and when $S = \{a \in D \mid a^\sigma = a$ for all σ in $G\}$, we suppose $[D : S]=n$. In this case, D/S is called a strictly Galois extension with a Galois group G([3],[4]). The purpose of this note is to discuss a splitting property of W by extending the base ring S as well as D, which is an analogy of the classical result of commutative case. We shall show that there exist a division ring D' such that $S \subseteq D' \subseteq D$ and a kind of (non-commutative) Kronecker product $D^* = D \otimes D'$ over S such that $W(D^*, G, \{c_{\sigma,\tau}\})$ becomes splitting. The construction of the Kronecker product seems very interesting to the author and an example will be given in the last section.

2. Let D be a division ring and $x_1, \cdots, x_m$ m indeterminates. A polynomial ring $D[x_1, \cdots, x_m]$ is defined in a natural way, supposing commutativity of multiplication between elements of D and x_i and between x_i and x_j. The quotient division ring of $D[x_1, \cdots, x_m]$ is called the rational function division ring, whose existence is almost clear when we imbed $D[x_1, \cdots, x_m]$ into the formal power series division ring $D\{x_1, \cdots, x_m\} = D\{x_m\}\{x_{m-1}\}\cdots\{x_1\}$ of $x_1, \cdots, x_m$ over D and take the

Received July 16, 1968

minimum division ring containing it. We denote the rational function division ring by $D(x)$. A discrete valuation of rank m is then introduced in $D(x)$ as follows. Every element of $D(x)$ is considered as a formal power series in $D\{x_1, \cdots, x_m\}$, and let us express an element $f(x) = \sum a(i_1, \cdots, i_m)x_1^{i_1} \cdots x_m^{i_m}$. Define a mapping φ such that $\varphi(f(x)) = (s_1, \cdots, s_m)$ where $s_1 = \min i_1$ (the min being taken over all i_1 such that $a(i_1, \cdots, i_m) \neq 0$), $s_2 = \min i_2$ (the min being taken over all i_2 such that $a(s_1, i_2, \cdots, i_m) \neq 0$), $\cdots$, and finally $s_m = \min i_m$ (the min being taken over all i_m such that $a(s_1, \cdots, s_{m-1}, i_m) \neq 0$). Between two m tuples of integers $(i_1, \cdots, i_m)$ and $(j_1, \cdots, j_m)$ we introduce an order such that $(i_1, \cdots, i_m) > (j_1, \cdots, j_m)$ if $i_1 > j_1$, or if $i_1 = j_1$ and $i_2 > j_2$, $\cdots$, or if $i_1 = j_1$, $i_2 = j_2$, $\cdots$, $i_{m-1} = j_{m-1}$ and $i_m > j_m$. All $f(x)$ such that $\varphi(f(x)) \geq (0, \cdots, 0)$ form a ring called the valuation ring and denoted by $V_{D(x)}$, and all $f(x)$ such that $\varphi(f(x)) > (0, \cdots, 0)$ form a prime ideal of $V_{D(x)}$ which is called the valuation ideal and denoted by $P_{D(x)}$. (See [6])

3. Let D, G and $\{c_{\sigma,\tau}\}$ be as in 1. We consider a rational function division ring $D(t_1, \cdots, t_m) = D(t)$ where we suppose $m = n-1$. We want to extend G to an automorphism group of $D(t)$ as follows. G acts on elements of D as usual, but t_i will be mapped in the following manner. Let us express $G = \{\sigma_1, \cdots, \sigma_m, \varepsilon\}$ and set $t_\sigma = t_i$ for $\sigma = \sigma_i$ and $t_\varepsilon = 1$. Then set

$$t_\sigma^\tau = t_\tau^{-1} t_{\sigma\tau} c_{\sigma,\tau} \qquad (\sigma, \tau \in G). \tag{2}$$

(Here we assume that $c_{\sigma,\varepsilon} = c_{\varepsilon,\sigma} = 1$)

It is seen that G induces an automorphism group of $D(t)$, since $(t_\sigma^\tau)^\rho = (t_\tau^{-1} t_{\sigma\tau} c_{\sigma,\tau})^\rho = (t_\rho^{-1} t_{\tau\rho} c_{\tau,\rho})^{-1}(t_\rho^{-1} t_{\sigma\tau\rho} c_{\sigma\tau,\rho}) c_{\sigma,\tau}^\rho = t_{\tau\rho}^{-1} t_{\sigma\tau\rho} c_{\sigma,\tau\rho} = t_\sigma^{\tau\rho}$ due to (1). Let B be the fix ring of G, namely $B = \{f(t) \in D(t) \mid f(t)^\sigma = f(t)$ for all σ in $G\}$. This is an analogue of the Brauer field defined in [5]. Naturally G is a group of outer automorphisms of $D(t)$ and hence $[D(t): B] = n$ by Galois theory of division rings. (See [1]). What is more important, a basis $u_1, \cdots, u_n$ of D/S is also a basis of $D(t)/B$. (2) implies that the crossed product $W(D(t), G, \{c_{\sigma,\tau}\})$ is a splitting crossed product. Now our intension is clear. Specialize B and $D(t)$ as well to get a finite extension D' and D^* such that $W(D^*/D', G, \{c_{\sigma,\tau}\})$ is again splitting. To do so, the discussion in 2 will be applied for the case $x_i = 1 - t_i$ $(i = 1, \cdots, m)$. Thus $D(t) = D(x)$ and, by the specialization with respect to the valuation in 2, $t_\sigma \longrightarrow 1$ and $t_\sigma^\tau \longrightarrow c_{\sigma,\tau}$,

i.e. t_σ and t_σ^τ are all contained in $V_{D(x)} - P_{D(x)}$, which also means t_σ are units. Keep this important fact in mind.
Let V_B be the valuation ring of B; $V_B = V_{D(x)} \cap B$, and P_B the valuation ideal of B; $P_B = P_{D(x)} \cap B$. Then the specialization D' of B with respect to the valuation is V_B/P_B and clearly $S \subseteq D' \subseteq D$. Now consider a set $U = \{\sum_i u_i f_i(x) \mid f_i(x) \in V_B\}$ and a set $P = \{\sum_i u_i p_i(x) \mid p_i(x) \in P_B\}$.

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

Proof. To prove Proposition, it is sufficient to show that $f(x)u_i \in U$ for $f(x)$ in V_B and $p(x)u_i \in P$ for $p(x)$ in P_B. Let $v_1, \cdots, v_n$ be the dual basis of $u_1, \cdots, u_n$ with respect to the trace function Tr of D/S for the Galois group G. That is, $Tr(v_i u_j) = \delta_{ij}$ (Kronecker delters). The existence of such v_i is clear since $Tr(D) \neq 0$, the latter being a consequence of the existance of a normal basis for D/S [2]. (Also see [3].) Put $f(x)u_i = \sum_j u_j h_j(x)$ with $h_j(x) \in B$, and we have $h_k(x) = Tr(v_k f(x) u_i)$. But clearly $Tr(v_k f(x) u_j) \in V_{D(x)}$, and hence $h_k(x) \in V_B$ which implies $f(x)u_i$ are contained in U for $f(x)$ in V_B. The second part is similarly proved.

4. Now put $D^* = U/P$. (Note that P is not necessarily prime although we use the letter P.) Every element of D^* has expression $\sum_i u_i \otimes a_i$ where $a_i \in D'$ and conversely. The multiplication of $\sum u_i \otimes a_i$ and $\sum u_i \otimes b_i$ should be performed as follows. Let $f_i(x)$ (or $g_i(x)$) be elements of V_B such that $f_i(x) \longrightarrow a_i$ (or, $g_i(x) \longrightarrow b_i$) in the specialization. When $(\sum u_i f_i(x))(\sum u_i g_i(x)) = \sum u_i h_i(x)$ with $h_i(x)$ in V_B and $h_i(x) \longrightarrow c_i$, we have $(\sum u_i \otimes a_i)(\sum u_i \otimes b_i) = \sum u_i \otimes c_i$. Due to Proposition, the product is well defined (does not depend on the choice of $f_i(x)$ and $g_i(x)$). D^* is a generalized Kronecker product $D \otimes_S D'$. Lastly, we observe that G induces an automorphism group of U and that of P respectively, and hence G is considered to be an automorphism group of D^*. Clearly the fix ring of G is $D' = S \otimes D'$. Regarding t_σ, set $t_\sigma = \sum u_i f_i(x)$ with $f_i(x)$ in B. Since $f_i(x) = Tr(v_i t_\sigma) = \sum_{\tau \in G} v_i^\tau t_\sigma^\tau \in V_{D(x)} \cap B$, t_σ are in U. Naturally $t_\sigma \notin P$. Applying the same discussion to t_σ^{-1}, we can see $t_\sigma^{-1} \in U - P$. Thus, if we set $s_\sigma = t_\sigma \bmod P$, (2) says $s_\sigma^\tau = s_\tau^{-1} s_{\sigma\tau} c_{\sigma,\tau}$, which proves our result:

THEOREM. *$W(D^*, G, \{c_{\sigma,\tau}\})$ is a splitting crossed product.*

COROLLARY. $W(D, G, \{c_{\sigma,\tau}\}) \subseteq D_n$ (*a matrix algebra over* D).

Proof. By denoting by D_r the right multiplication ring of D, GD_r coincides with the totality of S $(=S_l)$-homomorphisms of D to D by Galois theory of division rings. Now, $W(D, G, \{c_{\sigma,\tau}\}) \subseteq W(D^*, G, \{c_{\sigma,\tau}\}) = W(D^*, G, \{1\})$, the latter being isomorphic to GD^*. From the first discussion, GD^* coincides with the totality of D'-homomorphisms of D^*, which is naturally (isomorhic to) D'_n.

5. Let A denote the quaternion algebra $Q(i, j)$ over the rational number field Q as usual. Consider a simple extension $A/Q(i)$. This is a strictly Galois extension with a Galois group $G = \{\varepsilon, \sigma\}$ where $j^\sigma = -j$ $(=iji^{-1})$. Take a factor set: $c_{\varepsilon,\varepsilon} = c_{\varepsilon,\sigma} = c_{\sigma,\varepsilon} = 1$ and $c_{\sigma,\sigma} = 2$. In this case, (2) says $t^\sigma = 2t^{-1}$. $(t = t_\sigma)$. Then $B = Q(i)(t + 2t^{-1}, j(t - 2t^{-1}))$. By the specialization $t \longrightarrow 1$, $D' = A$ and hence $D^* = A \otimes A$ over $Q(i)$. We take $u_1 = 1$ and $u_2 = j$. Now we show some examples of multiplication. Since $1 \otimes j = 1 \cdot (-j(t - 2t^{-1}) + j \cdot 0 \bmod P$, $(1 \otimes j)(1 \otimes j) = (-j(t - 2t^{-1}))^2 \bmod P = -(t - 2t^{-1})^2 \bmod P = -1 \bmod P = 1 \otimes (-1)$. Since $j \otimes (-1) = 1 \cdot 0 + j \cdot (-1) \bmod P$, $(1 \otimes j)(j \otimes (-1)) = (-j(t - 2t^{-1}))(-j) \bmod P = -(t - 2t^{-1}) \bmod P = j \cdot (j(t - 2t^{-1})) \bmod P = j \otimes (-j)$. Similarly, we have $(j \otimes 1)(1 \otimes j) = j \otimes j$ and $(j \otimes 1)(j \otimes (-1) = 1 \otimes 1$. Thus, combining all results, we have $(1 \otimes j + j \otimes 1)(1 \otimes j + j \otimes (-1)) = 0$, which shows D^* is not a division ring. Since $t = \frac{1}{2}((t + 2t^{-1}) - jj(t - 2t^{-1}))$, $t \bmod P = \frac{1}{2}(1 \otimes 3 + j \otimes j)$, and since $t^\sigma = \frac{1}{2}((t + 2t^{-1}) + jj(t - 2t^{-1}))$, $t^\sigma \bmod P = \frac{1}{2}(1 \otimes 3 - j \otimes j)$. On the other hand, since $j = -j(t - 2t^{-1})$ by $t \longrightarrow 1$, $j \otimes j = j(-j(t - 2t^{-1})) \bmod P$, which shows $(j \otimes j)(j \otimes j) = (t - 2t^{-1})^2 \bmod P = 1 \otimes 1$. Thus, if we set $s = t \bmod P$, $ss^\sigma = \frac{1}{4}(1 \otimes 9 - 1 \otimes 1) = 2$, or $s^\sigma = 2s^{-1}$. This is nothing but (2).

REFERENCES

[1] N. Jacobson, Structure of rings. A.M.S. (1956).

[2] F. Kasch, Über den Endomorphismenring eines Vectorraums und der Satz von der Normalbasen. Math. Ann. **126** (1953) 447–463.

[3] K. Kishimoto, T. Onodera and H. Tominaga, On the normal basis theorems and the extension dimension. J. Fac. Scie. Hokkaido Univ. Ser. 1, **18** (1964) 81–88.

[4] N. Nobusawa and H. Tominaga, Some remarks on strictly Galois extensions of simple rings. Math. J. Okayama Univ. **9** (1959/60) 13–17.

[5] P. Roquette, On the Galois cohomology of the projective groups and its applications. Math. Ann. **150** (1963) 411–439.
[6] O.F.G. Schilling, The theory of valuations. New York (1950).

University of Hawaii