S©MR

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ
Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru
ISSN 1813-3304

Vol. 21, No. 2, pp. 1145–1151 (2024)
https://doi.org/10.33048/semi.2024.21.075

УДК 512.6
MSC 11R52, 16K20, 12J20

A NEW PROOF FOR PART OF THE NONCROSSED PRODUCT THEOREM

M. MOTIEE

Communicated by I.B. Gorshkov

Abstract: The first examples of noncrossed product division algebras were given by Amitsur in 1972. His method is based on two basic steps: (1) If the universal division algebra $U(k,n)$ is a G-crossed product then every division algebra of degree n over k should be a G-crossed product; (2) There are two division algebras over k whose maximal subfields do not have a common Galois group. In this note, we give a short proof for the second step in the case where $\operatorname{char} k \nmid n$ and $p^3|n$.

Keywords: Division algebra, Crossed product, Valuation.

1 Introduction

Let F be a field. An F-central division algebra D is called a crossed product if it contains a maximal subfield K which is Galois over F. If $\mathrm{Gal}(K/F) \cong G$, then D is said to be a G-crossed product. Until 1972, the existence of a noncrossed product division algebra remained unsolved and influenced by Köth's theorem, which says that every division algebra contains a maximal subfield which is separable over its center, many mathematicians believed that the answer to this question is negative. Nevertheless, the first examples of noncrossed products were given by Amitsur in 1972 [1]. His examples of noncrossed products are certain universal division algebras which

Motiee, M., A new proof for part of the noncrossed product theorem.

Received August, 26, 2024, Published November, 27, 2024.

are defined as follows: Let k be an infinite field and let $X = \{x_{ij}^{(r)} | 1 \leq i, j \leq n, r \geq 2\}$ be a set of independent commuting variables. Let $k[X]$ be the integral domain of polynomials in all $x_{ij}^{(r)}$ with coefficients in k and let $k(X)$ the field of fractions $k[X]$. For each r, the standard generic n by n matrices over k are defined by $\xi^{(r)} = \left[x_{ij}^{(r)}\right] \in M_n(F[X]) \subseteq M_n(F(X))$. The F-subalgebra of $M_n(F(X))$ generated by $\{\xi^{(r)} | r < n\}$ is called the generic matrix algebra over k of degree n. We denote this generic algebra by B_n. It is well-known that B_n is a (noncommutative) domain [8, Prop. 20.5], so its center is an integral domain. We define the universal division algebra over k of degree n by $UD(k,n) = B_n \otimes_R L_n$ where R is the center of B_n and L_n is the fraction field of R. Using the theory of PI-rings, it can be shown that $UD(k,n)$ is a division algebra of degree n (cf. [8, Prop. 20.8]). The following theorem is the key result that Amitsur proved in order to show that certain $UD(k,n)$ are noncrossed products. For a proof of this theorem in its full generality[1] see [8, p. 417].

Theorem 1. *If $UD(k,n)$ is a G-crossed product, then every division algebra of degree n whose center contains a subfield isomorphic to k is also a G-crossed product.*

In light of Theorem 1, to prove that $UD(k,n)$ is not a crossed product it suffices to produce two different examples of division algebras over k whose maximal subfields do not have a common Galois group. The aim of this note is to present a simple proof with least possible computations for this step in the case $\operatorname{char} k \nmid n$ and $p^3 | n$ for some prime p. We note that this case is the most general case independent of the properties of k in which it is proved that $UD(k,n)$ is not a crossed product (see [2]). In our approach we employ Skolem-Noether Theorem and a basic property of Henselian fields. We emphasize that our method neither leads to a new insight into the noncrossed product theorem nor enriches the theory of valued division algebras. This is just a shortcut for proving a well-known theorem avoiding standard results about the Galois theory of Henselian fields.

First, we recall some preliminaries from the theory of valued division algebras. Let Γ be a totally ordered additive abelian group. Let ∞ is a symbol such that $\gamma < \infty$ and $\gamma + \infty = \infty + \infty = \infty$ for all $\gamma \in \Gamma$. By a valuation on D we mean a function

$$v : D \to \Gamma \cup \{\infty\}$$

satisfying the following conditions: for all $x, y \in D$

(i) $v(x) = \infty$ if and only if $x = 0$;
(ii) $v(x + y) \geq \min\{v(x), v(y)\}$;
(iii) $v(xy) = v(x) + v(y)$.

[1] In his original paper Amitsur only considers the case $k = \mathbb{Q}$, the field of rational numbers.

To a valuation v on D we associate the following structures: $\Gamma_D = v(D^*)$, the value group of D, which is a subgroup of Γ. $\mathcal{O}_D = \{x \in D \mid v(x) \geq 0\}$, which is a subring of D. $\mathcal{O}_D$ is called the valuation ring of D. It is easy to observe that $\mathcal{O}_D$ is a local ring with unique maximal left ideal $\mathfrak{m}_D = \{x \in D \mid v(x) > 0\}$; so $\mathfrak{m}_D$ is a two-side ideal of $\mathcal{O}_D$. The quotient division ring $\overline{D} = \mathcal{O}_D/\mathfrak{m}_D$ is called the residue division ring. For any $a \in D$ we write $\overline{a}$ for the image of a in $\overline{D}$. Clearly, restricting v to F is a valuation on F. Moreover, it is not hard to show that the inclusion map from F to D gives an embedding $\overline{F} \hookrightarrow Z(\overline{D})$. Hence $\overline{D}$ is an $\overline{F}$-algebra.

Let F be a field equipped with a valuation v. The valued field F (or the valuation v) is called Henselian if v has a unique extension to each field L algebraic over F. So, it is clear that every finite extension of a Henselian field is Henselian. For $f = \sum_{i=0}^{n} a_i X^i \in \mathcal{O}_F[X]$, we write $\overline{f} = \sum_{i=0}^{n} \bar{a}_i X^i \in \overline{F}[X]$ and f' for the formal derivative of f. One can observe that Henselian fields have the following property: for each $f \in \mathcal{O}_F[X]$, if there is a $c \in \overline{F}$ with $\overline{f}(c) = 0$ but $\overline{f}'(c) \neq 0$, then there is a unique $a \in \mathcal{O}_F$ with $f(a) = 0$ and $\bar{a} = c$ (see [4, Th. 4.1.3]).

One of the most important features of a Henselian field F that will be used in our proof is that if $\operatorname{char}\overline{F} \nmid n$, then $1+\mathfrak{m}_F$ is n-divisible, i.e., $(1+\mathfrak{m}_F)^n = 1+\mathfrak{m}_F$. To see this, take any $a \in 1+\mathfrak{m}_F$. Let $f = X^n - a \in \mathcal{O}_F[X]$. Its image in $\overline{F}[X]$ is $\overline{f} = X^n - \overline{1}$. But $\overline{1}$ is a simple root of $\overline{f}$ since $\operatorname{char}\overline{F} \nmid n$. As F is Henselian, f has a root $b \in \mathcal{O}_F$ with $\bar{b} = \overline{1}$. That is $b^n = a$, as desired.

The following lemma is a known fact. However, for convenience of the reader, we provide a proof for it.

Lemma 2. *Let D be a central F-division algebra of index n. Let v be a valuation on D such that the restriction of v to F is Henselian. if* $\operatorname{char}\overline{F} \nmid n$ *then in $1+\mathfrak{m}_D$ each element has a unique n-th root.*

Proof. At first, we note that if $\operatorname{char} D > 0$ then $\operatorname{char}\overline{F} = \operatorname{char} D$ and if $\operatorname{char} D = 0$ then either $\operatorname{char}\overline{F} = 0$ or $\operatorname{char}\overline{F} > 0$. In any case, we have $\operatorname{char} D \nmid n$.

Let $a \in 1+\mathfrak{m}_D$ and Let $K = F(a)$. According to what we mentioned above, the restriction of v to K is Henselian because K/F is a finite extension. On the other hand, it is clear that $a \in 1+\mathfrak{m}_K$. So, by the argument in the last paragraph, a has a n-th root in K, hence in D. It remains to show that this root is unique. Let there are $g, h \in \mathfrak{m}_D$ such that $(1+g)^n = a = (1+h)^n$ and $g \neq h$. Then, we have

$$n(g-h) = \sum_{j=2}^{n} \binom{n}{j} \left(h^j - g^j\right).$$

Set $t = g - h$. Therefore, we can rewrite the above equation as follows

$$nt = \sum_{j=2}^{n} \binom{n}{j} \left(h^j - (t+h)^j\right). \tag{1}$$

But it is clear that $v(t) > 0$. So $v\left(-t^2\right) = v\left(t^2\right) = 2v\left(t\right) > v\left(t\right)$. Likewise $v(th) > v(t)$ and $v(ht) > v(t)$. Hence $v(h^2-(t+h)^2) = v(-t^2-th-ht) > v(t)$. Similarly, it can be concluded that $v(h^j - (t+h)^j) > v(t)$ for all $j \geq 3$. So we have

$$v\left(\sum_{j=2}^{n} \binom{n}{j} \left(h^j - (t+h)^j\right)\right) > v(t). \tag{2}$$

On the other hand, since $\operatorname{char} D \nmid n$, n is invertible in $\mathcal{O}_D$. Therefore, $v(n) = 0$, and we have as a result $v(nt) = v(n) + v(t) = v(t)$. Thus, from (1) and (2) it follows that $v(t) > v(t)$, which is a contradiction. □

In what follows, we recall a certain class of division algebras which are a special case of Mal'cev-Neumann construction (see [6, §14]). Let k be an arbitrary field and let $n_1, \ldots, n_r$ be integers (not necessarily distinct) with $n_i \geq 2$ for all i. let

$$n = n_1 \ldots n_r \quad \text{and} \quad m = \operatorname{lcm}(n_1, \ldots, n_r).$$

Assume that k contains a primitive m-th root of unity ζ_m, and let $\zeta_{n_i} = \zeta_m^{m/n_i}$, for all $i = 1, \ldots, r$; so ζ_{n_i} is a primitive n_i-th root of unity. Let $x_1, y_1, \ldots, x_r, y_r$ be $2r$ independent indeterminates over k. Consider the ring of iterated Laurent series $k((x_1))((y_1)) \ldots ((x_r))((y_r))$ with the multiplication defined by the following rules:

$$\begin{aligned} &x_i a = a x_i, \quad y_i a = a y_i \quad \text{for } a \in k \\ &x_i x_j = x_j x_i, \quad y_i y_j = y_j y_i \\ &x_i y_j = y_j x_i \quad \text{for} \quad i \neq j \\ &x_i y_i = \zeta_{n_i} y_i x_i. \end{aligned} \tag{3}$$

One can observe that with relations defined in (3), $k((x_1))((y_1))...((x_r))((y_r))$ is a division algebra of index n and its center is $F = k((x_1^{n_1}))((y_1^{n_1})) \ldots ((x_r^{n_r}))((y_r^{n_r}))$ (cf. [5, p. 100]). We denote this division algebra by $\Delta_{2r}(k; n_1, ..., n_r)$. Recall that nonzero elements of $\Delta_{2r}(k; n_1, ..., n_r)$ are formal series

$$f = \sum_{(i_1, \ldots, i_n)} a_{(i_1, j_1, \ldots, i_r, j_r)} x_1^{i_1} y_1^{j_1} \ldots x_r^{i_r} y_r^{j_r}, \quad a_{(i_1, j_1, \ldots, i_r, j_r)} \in k \tag{4}$$

where $\operatorname{supp}(f) = \{(i_1, j_1, \ldots, i_r, j_r) | a_{(i_1, j_1, \ldots, i_r, j_r)} \neq 0\}$ is a well-ordered subset of the abelian group $\oplus_{i=1}^{2r} \mathbb{Z}$ ordered by the right-to-left lexicographic ordering. It can be easily seen that the map

$$v(f) = \min \operatorname{supp}(f) \quad \text{for} \quad 0 \neq f \in \Delta_{2r}(k; n_1, \ldots, n_r)$$

is a valuation on $\Delta_{2r}(k; n_1, \ldots, n_r)$ with value group $\Gamma_{\Delta_{2r}(k; n_1, \ldots, n_r)} = \oplus_{i=1}^{2r} \mathbb{Z}$. It is also a known fact that the restriction of v to the center is Henselian with value group $\Gamma_F = \oplus_{i=1}^{r} (n_i \mathbb{Z} \oplus n_i \mathbb{Z})$.

To simplify our notations, for each $\alpha = (i_1, j_1, \ldots, i_r, j_r)$, the monomial $x_1^{i_1} y_1^{j_1} \ldots x_r^{i_r} y_r^{j_r}$ is denoted by x^α. Using this notation, we can rewrite (4) in

the form

$$f = \sum_{\alpha_1<\alpha_2<\dots} a_{\alpha_i} x^{\alpha_i}$$

where $\operatorname{supp}(f) = \{\alpha_1, \alpha_2, \dots\}$ and $a_{\alpha_1} \neq 0$. In particular, we have

$$\ker(v) = \{a_0 + \sum_{0<\alpha_1<\alpha_2<\dots} a_{\alpha_i} x^{\alpha_i} | a_{\alpha_i} \in k^* \text{ for all } \alpha_i\} = k^* (1 + \mathfrak{m}_D) \quad (5)$$

where $D = \Delta_{2r}(k; n_1, \dots, n_r)$.

Now, we are ready for the following proposition.

Proposition 3. *Let $D = \Delta_{2r}(k; n_1, \dots, n_r)$. Let K be a maximal subfield of D which is Galois over F. Let $H = N_{D^*}(K^*)$, the normalizer of K^* in D^*. Then there is a diagram of group homomorphisms*

$$\begin{array}{ccccc} 1 & \longrightarrow & H/F^*(H \cap (1+\mathfrak{m}_D)) & \longrightarrow & \oplus_{i=1}^r (\mathbb{Z}_{n_i} \oplus \mathbb{Z}_{n_i}) \\ & & \downarrow & & \\ & & \operatorname{Gal}(K/F) & & \\ & & \downarrow & & \\ & & 1 & & \end{array} \quad (6)$$

with exact row and column. In particular, both $H/F^*(H \cap (1+\mathfrak{m}_D))$ and $\operatorname{Gal}(K/F)$ are abelian.

Proof. The map $\bar{v} : H \to \Gamma_D/\Gamma_F = \bigoplus_{i=1}^r (\mathbb{Z}_{n_i} \oplus \mathbb{Z}_{n_i})$ induced by the valuation v has kernel $H \cap F^* \ker(v)$. But $F^* \ker(v) = F^*(1 + \mathfrak{m}_D)$ by (5). Hence, $\ker(\bar{v}) = H \cap F^*(1 + \mathfrak{m}_D) = F^*(H \cap (1 + \mathfrak{m}_D))$. This shows that the row of (6) is exact.

For the column of (6), first let $\theta : H \to \operatorname{Gal}(K/F)$ be the map $h \mapsto \theta_h$ where $\theta_h : a \mapsto h^{-1}ah$ for all $a \in K$. By the Skolem-Noether Theorem [3, p. 39], θ is surjective. Also, $\ker(\theta) = C_H(K^*)$, the centralizer of K^* in H. Since K is a maximal subfield of D, $C_H(K^*) = K^*$. Hence, θ induces an isomorphism $H/K^* \cong \operatorname{Gal}(K/F)$. Now take any $h \in H \cap (1 + \mathfrak{m}_D)$. Then, as $|H/K^*| = |\operatorname{Gal}(K/F)| = n$ (recall that $n = n_1 \dots n_r$ is the index of D), one has $h^n \in K^* \cap (1 + \mathfrak{m}_D) = 1 + \mathfrak{m}_K$. Because K is Henselian, h^n has a n-th root in $1 + \mathfrak{m}_K$ which is h itself, as this root is unique in $1 + \mathfrak{m}_D$ by Lemma 2. So $h \in K$. Therefore, $\ker(\bar{v}) = F^*(H \cap (1 + \mathfrak{m}_D)) \subseteq K^* = \ker(\theta)$. Hence, θ induces a well-defined map $H/\ker(\bar{v}) \to \operatorname{Gal}(K/F)$, and this map is surjective as θ is surjective. Thus, the column of (6) is well-defined and exact. □

Theorem 4. *If $\operatorname{char} k \nmid n$ and $p^3 | n$ for some prime p, then $UD(k, n)$ is noncrossed product.*

Proof. On the contrary, suppose that $UD(k, n)$ is a G-crossed product for a group G of order n. Let $n = p_1 \dots p_r$ where p_i is prime for $i = 1, \dots, r$ (note that these prime numbers are not necessarily distinct). Let $D_1 =$

$\Delta_{2r}(k(\zeta_n); p_1, \ldots, p_r)$ and $D_2 = \Delta_2(k(\zeta_n); n)$. By Theorem 1, D_1 is a G-crossed product. Hence, by Proposition 3, G is abelian and each element of G is of prime order. Therefore $G \cong \oplus_{j=1}^{r} \mathbb{Z}_{p_j}$ because $|G| = n$. But $p^3 | n$. So we must have $\mathrm{rank}(G) \geq 3$. Using Theorem 1 again shows that D_2 is a G-crossed product. Now, the exact diagram (6) gives

$$\mathrm{rank}(G) \leq \mathrm{rank}\left(H/F^*\left(H \cap (1 + \mathfrak{m}_D)\right)\right) \leq \mathrm{rank}\left(\mathbb{Z}_n \oplus \mathbb{Z}_n\right) = 2.$$

This contradiction shows that $UD(k, n)$ is not a crossed product. □

We point out that what Amitsure proved about the maximal subfields of $\Delta_{2r}(k; n_1, \ldots, n_r)$ is more than what was done in the above. In fact, he showed that if k is algebraically closed and n_i are prime for all $1 \leq i \leq r$, then all maximal subfields of $\Delta_{2r}(k; n_1, \ldots, n_r)$ are Galois extensions of its center with Galois group isomorphic to $\oplus_{i=1}^{r} \mathbb{Z}_{n_i}$. He obtained the Galois group information by some clever but mysterious calculations using certain integer-valued triangular matrices. His method, along with the Platonov's reduced K-theory, became a source of inspiration for others to develop the theory of valued division algebras. In [7], in an attempt to provide an elementary proof for the above results, the author presents a proof without using Henselian property of the fields of iterated Laurent series for the case $n = p^m$ where p is a prime and $m \geq 3$.

Acknowledgments

The author wishes to thank the referee for his/her constructive comments. He is also grateful to the Research Council of Babol Noshirvani University of Technology for support.

References

1. S.A. Amitsur, On central division algebras, Isr. J. Math., **12** (1972), 408–420. Zbl 0248.16006
2. S.A. Amitsur, The generic division rings, Isr. J. Math., **17** (1974), 241–247. Zbl 0293.16018
3. P.K. Draxl, *Skew fields*, London Mathematical Society Lecture Note Series, **81**, Cambridge University Press, Cambridge etc., 1983. Zbl 0498.16015
4. A.J. Engler, A. Prestel, *Valued fields*, Springer, Berlin, 2005. Zbl 1128.12009
5. N. Jacobson, *PI-algebras. An introduction*, Lecture Notes in Mathematics, **441**, Springer-Verlag, Berlin etc., 1975. Zbl 0326.16013
6. T.Y. Lam, *A first course in noncommutative rings*, Graduate Texts in Mathematics, **131**, Springer-Verlag, New York etc., 1991. Zbl 0728.16001
7. M. Motiee, A note on Amitsure's noncrossed product theorem, arXiv preprint arXiv:2401.03574, 2024.
8. R.S. Pierce, *Associative algebras*, Graduate Texts in Mathematics, **88**, Springer-Verlag, New York etc., 1982. Zbl 0497.16001

Mehran Motiee
Faculty of Basic Sciences, Babol Noshirvani University of Technology,
pr. Koptyuga, 4,
Babol, Iran
Email address: motiee@nit.ac.ir