THE GENERIC DIVISION RINGS

BY

S. A. AMITSUR

ABSTRACT

Let $A = k(X_1, X_2 \ldots, X_m)$ be the division ring generated by generic $n \times n$ matrices over a field k; then A is not a crossed product in the following cases: (i) there exists a prime q such that $q^3 \mid n$; (ii) $[k:Q] = m$, where Q is the field of rationals, then if either $q^3 \mid n$ for some q for which $q-1 \mid m$, or $q^2 \mid n$ for some other prime; (iii) $k = Z_{p^r}$ a finite field of p^r elements and either $q^3 \mid n$ for same $q \mid p^{r-1}$ or $q^2 \mid n$ for some other primes. Other cases are also considered.

1. The main results

Let k be a field of characteristic $p \geqq 0$. Denote $k[X] = k[X_1, X_2, \cdots, X_l]$ $(\infty \geqq l \geqq 2)$ the ring generated by $n \times n$ generic matrices $X_i = (\xi^i_{\lambda\mu})$, $1 \leqq \lambda$, $\mu \leqq n$ over k. Here, the set $\{\xi^i_{\lambda\mu}\}$ are commutative indeterminates over k. The ring $k[X]$ is an Öre domain and has a ring of quotients $k(X)$ which is a division ring of dimension n^2 over its center. It was shown in [1] that $k(X)$ is not a crossed product for $k = Q$ the field of rationals if $8 \mid n$ or $q^2 \mid n$ for some odd prime q. Following [1], Small and Schacher have proved in [2] that if $q^3 \mid n$ for a prime q then the same holds if k is of characteristic zero or of p of transcendence degree $\geqq 1$ over the prime field of p elements, and $(p, n) = 1$.

In the present paper we study further the problem when $k(X)$ is not a crossed product and we prove Theorem 1.

THEOREM 1. i. *If k is a field of algebraic numbers, and $[k: Q] = m$ then $k(X)$ is not a crossed product if either $q^3 \mid n$ for a prime q such that $q - 1 \mid m$, the degree of k over Q, or $q^2 \mid n$ for some other prime.*

ii. *$k = Z_{p^r}$ a finite field of p^r elements and $(n, p) = 1$, then $k(X)$ is not a crossed product if $q^3 \mid n$ for some $q \mid p^r - 1$, or $q^2 \mid n$ for some other prime.*

Received December 20, 1973

iii. *If there exists a field k for which $k(X)$ is a crossed product then there is a finite algebraic extension F_0 of the prime field P $(= Q$ or $Z_p)$ such that $F_0(X)$ is a crossed product and F_0 depends only on the characteristic (and not on k).*

We also take this opportunity to bring two additional results. The first is a slight generalization of Small-Schacher result [5], namely, Theorem 2.

THEOREM 2. *$k(X)$ is not a crossed product in $q^3 \mid n$ for some prime, q and $(n,p) = 1$ if k is of characteristic p.*

This result is a corollary of Theorem 1 (i), (ii) and (iii), but we shall prove this fact using the construction of [1] without using deep results in algebras and algebraic extensions of local fields.

The other result is a known fact.

THEOREM 3. *For arbitrary commutative domain Ω, the ring $\Omega[X]$ is an Öre domain and its ring of quotient is a central division algebra of domain n^2.*

This result is attributed to the present author; it is, in fact, proved in an equivalent form in [2, Th. 3 and 4, p. 472], but at no place does it appear as stated in Theorem 3. Since this result became fundamental in the construction of non-crossed products, we present here a complete proof of this result, which is the reproduction of that proof in the present context.

2. Proof of Theorem 3

The proof of Theorem 3 depends on the following observation.

LEMMA 1. *A polynomial identity $g[x_1, x_2, \cdots] = 0$ (in non-commutative indeterminates x_i) holds in the matrix ring $M_n(\Omega)$ over an infinite commutative domain Ω, if and only if $g[X_1, X_2, \cdots] = 0$ for the substitution $x_i = X_i$ the generic matrices.*

This is equivalent to the following, which will not be used here.

LEMMA 1′. *$\Omega[X] \cong \Omega[x]/M_n$, where $\Omega[x]$ is the free ring and M_n is the ideal of all identities of $M_n(\Omega)$, for an infinite commutative domain Ω.*

Indeed, if $g[x] = 0$ holds in $M_n(\Omega)$ and Ω is infinite, then $g[x] = 0$ holds also n every $M_n(K)$ where K is a commutative ring $\supseteq \Omega$. In particular it will hold for $K = \Omega[\xi]$, the ring of polynomials in the $\{\xi^i_{\lambda\mu}\}$. But $X_i \in M_n(\Omega[\xi])$ and so $g[X] = 0$. Conversely, if $g[X] = 0$ then for any substitution $x_i = A_i = (a^i_{\lambda\mu})$ we have a homomorphism $\phi: \Omega[\xi] \to M_n(\Omega)$ by setting $\xi^i_{\lambda\mu} \to a_{\lambda\mu}$ and this maps

$M_n(\Omega[\xi])$ into $M_n(\Omega)$; in particular, $0 = \phi(g[X]) = g(A)$, that is, $g[x] = 0$ holds in $M_n(\Omega)$.

The proof of Lemma 1 is now evident.

Next we need the following result ([4, Lem. 2.1]).

LEMMA 2. *Given a field k and an integer n, then there exist a field $K \supseteq C$ and a central division algebra over K of dimension n^2 (and of exponent n).*

An alternative construction of such an algebra will be given in the proof of Theorem 2.

We turn now to the proof of Theorem 3. Let $g[X_1, X_2, \cdots]h[X_1, X_2, \cdots] = 0$ hold in $\Omega[X_1, X_2, \cdots]$ and let k be the field of quotients of Ω. It follows by Lemma 1 that $g[x]h[x] = 0$ holds in every $M_n(H)$ for H commutative $\supseteq \Omega$. In particular, choose D a division ring of dimension n^2 over a field $K \supseteq \Omega$ (Lemma 2) and H a splitting field of D; then $M_n(H) \supseteq D$, and so $g[x]h[x] = 0$ holds in D. Thus for every substitution $x_i = d_i \in D$ then $g[d]h[d] = 0$ and since D is a division ring then $g[d] = 0$ or $h[d] = 0$. This clearly implies that D will also satisfy an identity $g[x]zh[x] = 0$ with z a new non-commutative indeterminate. Again, it will follow that $g[x]zh[x] = 0$ holds also in $M_n(H)$ and hence also in every $M_n(K)$ for commutative $K \supseteq \Omega$. In particular this will hold in $M_n(k(\xi))$ where $k(\xi)$ is the field of quotients of $k[\xi]$, and so $g[X]M_n(k(\xi))h[X] = 0$. But $M_n(k(\xi))$ is a simple ring and so either $g[X] = 0$ or $h[X] = 0$.

Finally, $\Omega[x]$ is a ring satisfying the polynomial identities of $M_n(\Omega[\xi])$ and hence, applying Posner's theorem, we obtain the proof of the rest of Theorem 3. Note that a straightforward proof for the existence of the division ring of quotient in the case of a domain is given in [3].

3. Proof of Theorem 2

The study of $k(X)$ in [1] was restricted to the case $k = Q$ and it was pointed out in [5] that the methods work as well for other fields. In particular the construction of [1,Th. 3] and the results of [1, Sect. 1] hold for arbitrary field k of any characteristic. We shall need the following construction:

A. Given a field k and $n = q_1 q_2 \cdots q_r$ a product of different primes (not necessarily different), then there exists a field $K \supseteq k$ and a division ring A of dimension n^2 over its center K, such that the maximal subfields L of A are abelian with the Galois group $\Gamma = S_1 \times S_2 \times \cdots \times S_r$, S_i cyclic of order q_i, that is, Γ is completely reducible ([1, Th. 3]).

The construction given in [1, Th. 3] will also yield:

B. Given a field k and an integer n, then there exists a field $K \supseteq k$ and a division algebra D of dimension n^2 over the center K (of exponent n) such that the maximal normal subfields of D have a Galois group Γ which is a cyclic extension of a cyclic group, that is, there exists an exact sequence $1 \to \Gamma_1 \to \Gamma \to \Gamma_2 \to 1$ such that both Γ_1 and Γ_2 are cyclic.

Indeed, follow the construction of [1, Sect. 2, p. 412] and take $K = \bar{k}\{t_1, t_2\}$ where $\bar{k}$ is the algebraic closure of the field k. Recall that $\bar{k}\{t_1, t_2\} = \bar{k}\{t_1\}\{t_2\}$ where $F\{t\}$ denotes the field of formal power series in t over F. Let D be the cyclic cross product $(K(t_1^{1/n}), \sigma, t_2)$. The proof of [1, Th. 3] holds in this case and one obtains that D is a division algebra with center K of dimension n^2 (it is not difficult to show that its exponent is also n). [1, Prop. 2] yields that the algebraic extensions L of K of degree n are of the form $K[\tau_1, \tau_2]$ where

$$\tau_1^{\nu_{11}} = t_1, \quad \tau_1^{\nu_{21}} t_2^{\nu_{22}} = t_2.$$

We thus obtain the sequence of fields $K \subset K[\tau_1] \subset K[\tau_1, \tau_2]$. The first field $K[\tau_1]$ is a cyclic extension of K since $\tau_1^{\nu_{11}} = t_1$ and K contains all roots of unity; also $K[\tau_1, \tau_2]$ is cyclic over $K[\tau_2]$ since $\tau_2^{\nu_{22}} = t_2 \tau_1^{-\nu_{21}}$. Hence, if $K[\tau_1, \tau_2]$ is a Galois extension of K with the Galois group Γ, then if Γ_1 be the group of automomorphisms leaving $K[\tau_1]$ invariant then Γ_1 is normal and cyclic and Γ/Γ_1 is also cyclic as the Galois group of $K[\tau_1]$ over K, as required.

We shall also need the following:

C. If $k(X)$ is a crossed product with a group Γ, then any division ring D of dimension n^2 over a center $K \supseteq k$ is a crossed product with the same group Γ.

The proof of (C) for $k = Q$ is given in [1, pp. 418–419, starting from line 12], but the same proof is valid for arbitrary k.

The proof of Theorem 2 is now straightforward. If $k(X)$ is a crossed product of a group Γ, then by (A) it follows that Γ is a completely reducible group. Now every subgroup and homomorphic image of a completely reducible group is also completely reducible, and a cyclic group is completely reducible if and only if its order is a product of different primes. It follows now by (B) that we have $1 \to \Gamma_1 \to \Gamma \to \Gamma_2 \to 1$ and so $n = |\Gamma| = |\Gamma_1|\,|\Gamma_2|$ and each $|\Gamma_i|$ is a product of different primes, so for a prime divisor $q \mid n$ at most $q^2 \mid n$, which proves Theorem 2.

We remark that this proof uses only the constructions of [1] and no deeper results on local or global fields are required (as in [1] and [5]). If the latter is used, we are able to obtain the stronger results stated in Theorem 1.

4. Proof of Theorem 1

We need some properties of local fields with finite residue fields, for example, [6, Chapt. 3]).

Consider first the case $p = Q$, and let k be an algebraic number field and $(k: Q) = m$. Let $k = Q(\alpha)$; we can choose α to be integral and so satisfy a minimal polynomial $g[x] = 0$ with integral coefficients. Let $d =$ discriminant of $g[x]$. Choose a prime p such that $(p, n) = 1$ and $p \nmid d$ and consider the p-adic field Q_p. Let $g[x] = g_1[x] \cdots g_s[x]$ be the decomposition of $g[x]$ in Q_p into irreducible factors, and $k_i = Q_p(\alpha_i)$, with α_i a root of $g_i[x] = 0$. The field k_i is also a complete ring with respect to a discrete valuation and the residue field $\bar{k}_i$ is a finite field of p^{f_i} elements where $g_i[x] \equiv h_i[x]^{e_i} \pmod{p}$, $f_i = \deg(h_i[x])$, and $n_i = \deg g_i[x] = e_i f_i$. Furthermore, the field k can be embedded in $k_i = Q_p(\alpha_i)$ by mapping $\alpha \to \alpha_i$.

The normal abelian extension L of k_i of degree n has a group Γ of automorphisms which have a cyclic inertia group Γ_T cyclic of degree f, and Γ/Γ_T is cyclic of degree e with $fe = n$, and $e \,|\, (p^{f_i} - 1)$.

The case $f_i = 1$ is [1, Th. 3]; the proof for arbitrary f_i is identical except that in the case $f_i = 1$, $k_i = Q_p$ and the residue field $\bar{Q}_p$ contains p elements, so the roots of unity of Q_p satisfy $x^{p-1} - 1 = 0$. In the general case, the residue field $\bar{k}_i$ contains $p^{f_i} - 1$ nonzero elements and so $x^e - 1 = 0$ is solvable in k_i if and only if $e \,|\, p^{f_i} - 1$.

Finally, there exists a division algebra B_i of dimension n^2 over the center k_i, thus its maximal abelian subfield has a group of automorphisms Γ of the type described above.

Following the proof of Theorem 2, we observe that if $k(X)$ is a crossed product of a group Γ, then Γ is completely reducible by (A). It follows also by (C) that every division algebra of dimension n^2 over a center $\supseteq k$ will be a crossed product with the group Γ. Hence the preceding remarks yield that Γ is a cyclic extension of a cyclic group and so $n = |\Gamma| = |\Gamma_T|\,|\Gamma/\Gamma_T| = f\,e$, and since Γ_T, Γ/Γ_T are completely reducible, f and e, each is a product of different primes. Thus if a prime q, $q^2 \,|\, n$, then $q \,|\, e$ and so $q \,|\, p^{f_i} - 1$ for all possible values f_i obtained from the decomposition of $g[x]$. Note also that $m = \deg g = \Sigma e_i f_i$ and so $q \,|\, p^m - 1$ since $p^{\Sigma e_i f_i} \equiv \prod (p^{f_i})^{e_i} \equiv 1 \pmod{q}$.

Summarizing, if $k(X)$ is a crossed product and $(k: Q) = m$ then for $q^2 \,|\, n$, $q \,|\, p^m - 1$ for all primes p with the exception of a finite number of primes p. The residue classes mod q form a cyclic group of order $q-1$; let a be a generator of this group; then each number $a+tq$ is also a generating class. This class contains an infinite number of primes, hence there exists a prime $p=a+tq$ whose class mod q generates the cyclic group of order q. Since we can choose the prime p not from the exceptional set, $p^m \equiv 1 \pmod q$ implies that $q-1 \mid m$.

Consequently, if $q^3 \mid n$ for a prime q for which $q-1 \mid m$ or $q^2 \mid n$ for some other prime, then $k(X)$ is not a crossed product. This completes the proof of Theorem 1 (i).

REMARK. This includes the case $m=1$ which was proved in [1].

The proof of part (ii) of Theorem 1 is similar. We need only replace Q_p with the complete field $Z_{p^r}\{t\}$, the field of formal power series in t over Z_{p^r}. Here the residue field $\overline{Z_{p^r}\{t\}}$ is Z_p and so $x^e - 1 = 0$ is solvable in $Z_{p^r}\{t\}$ for $(e,p)=1$ if and only if $e \mid p^r - 1$. Following the proof of (i) we obtain that $k(X)$ is not a crossed product if $q^3 \mid n$ for a prime $q \mid p^r - 1$ or $q^2 \mid n$ for some other prime q, which proves (ii).

To prove (iii), we start with an arbitrary k observing first that if $k(X)$ is a crossed product of a group Γ, then

1. $k_0(X)$ is also a crossed product with Γ for some finitely generated subfield k_0 over the prime field $P(=Z_{p^r}$ or $Q)$;

2. $k_1(X)$ is also a crossed product with Γ for some finite algebraic extension of the prime field P.

The first part follows from the condition that $k(X)$ is a crossed product of Γ can be stated by a finite number of conditions; namely [1, p. 418, conditions (G1)–(G4)]. These conditions where stated in [1] for $k=Q$, but they are valid for arbitrary k. These conditions involve only a finite number of elements of k; let $k_0 \subseteq k$ be the subfield generated by the elements involved, then clearly k_0 satisfies (1).

To prove (2), we let $k_0 = P(t_1, t_2, \cdots, t_s)$ where P is the prime field (that is, Z_p or Q), and note that the conditions (G1)–(G4) of [1, p. 418] plus the additional requirements that some finite elements listed there of $k_0(X)$ are $\neq 0$, constitute a finite set. Hence we can find a specialization of k_0 into $\bar{P}$ the algebraic closure of P, mapping $t_i \to \alpha_i \in \bar{P}$ such that all the preceding conditions will remain valid. The image of this specialization is, clearly, a finite algebraic extension k_1 of P which will satisfy (2), that is, $k_1(X)$ is a crossed product with Γ since (G1)–(G4) and the other requirements hold in $k_1(X)$.

We now apply (1) and (2) in the following cases. Let $\bar{P}$ be the algebraic closure of the prime field P and let F be the algebraic closure of the field of all rational function in $\aleph_0$ commutative indeterminates over $\bar{P}$. If $k(X)$ is a crossed product with Γ, then by (1), $k_0(X)$ is a crossed product with Γ for some field of finite transcendence degree over P. Hence k_0 can be embedded in F and, therefore, (1) implies that $F(X)$ is also a crossed product with Γ. But then (2) yields that there exist a finite algebraic extension F_0 of P such that $F_0(X)$ is a crossed product, and we note that F_0 depends only on the field F which is fixed by the characteristic of k. This completes the proof of (iii) of Theorem 1.

REMARK. The degree $[F_0 : P] = m$ is fixed by the characteristic. Hence we can use parts (i) and (ii) of Theorem 1 and state the following result.

For arbitrary field k of characteristic $p \geqq 0$, there exists an integer m ($m = p^r$ for the case $p \neq 0$) such that $k(X)$ is not a crossed product if either $q^3 \mid n$ for a prime q such that $q - 1 \mid m$ if $p = 0$ or $q \mid m - 1$ for $p \neq 0$, or $q^2 \mid n$ for some other prime q.

We guess that $m = 1$ for $p = 0$,; but as long as we prove that m depends on p and n, it may be that this result yields no more information than that given in Theorem 2, since the primes q for which $q - 1 \mid m$ and $q \mid n$ may include all primes of n.

REFERENCES

1. S. A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972), 408–420.
2. S. A. Amitsur, *The T-ideals of the free rings*, J. London Math. Soc. **30** (1955), 472.
3. S. A. Amitsur, *On ring with identities*, J. London Math. Soc. **30** (1955), 466.
4. S. A. Amitsur, *Some results on central simple algebras*, Ann. of Math. **63** (1965), 287.
5. M. M. Schacher and L. W. Small, *Noncrossed product in characteristic p*, J. Algebra, **24** (1973), 100–103.
6. E. Weiss, *Algebraic number theory*, McGraw Hill, New York, 1963.

INSTITUTE OF MATHEMATICS
THE HEBREW UNIVERSITY OF JERUSALEM
JERUSALEM, ISRAEL