ON CENTRAL DIVISION ALGEBRAS

BY

S. A. AMITSUR

To the memory of A. A. Albert[†]

ABSTRACT

For any integer n such that $8 \mid n$ or for which there exists an odd prime q such that $q^2 \mid n$, there is a central division algebra of dimension n^2 over its center which is not a crossed product. The algebra constructed in this paper is the algebra $Q(X_1,\ldots,X_m)$, the algebra generated over the rational Q by m ($\geqq 2$) generic matrices.

Introduction.

Since the early days of the theory of central simple algebras of finite dimension, the crossed-products have been the basic tools for constructing these algebras˙ The famous result of Nother-Brauer-Hasse that every such algebra over an algebraic number field is a cyclic algebra supported the idea that possibly every central division algebra of finite dimension is a cyclic algebra. This was disproved by Albert [1] who constructed a central division algebra of dimension $16 = 4^2$ which is a crossed-product but which is not cyclic. In fact, Albert [2, p. 179] showed that every central division algebra of dimension 4^2 contains a maximal normal field of degree 4. This, together with Wedderburn's result that all central simple algebra of dimension 3^2 are cyclic and the fact that these algebras are tensor products of algebras of prime power dimension, shows that all central division algebras of dimension n^2 with $n = 2, 3, 4, 6, 12$ are crossed-products. The main question, as to whether all such algebras are crossed-products, remained unsettled although it was expected that such is not the case. The present paper

[†] This paper was originally presented in November, 1971 for publication elsewhere in a volume in honor of Prof. A. A. Albert on the occasion of his 65th birthday. The volume was never published due to the death of Prof. Albert in June 1972.

settles this problem by showing that for every n which is divisible by a square of an odd prime or by 8, there exists a central division algebra of dimension n^2 which is *not* a crossed-product. The problem remains open for $n = 2^{v_0} q_1 q_x \cdots q_k$, $0 \leqq v_0 \leqq 2$, where the $q_i \geqq 3$ are different primes (except for the cases mentioned above).

The algebra we construct is $Q(X_1, X_2, \cdots, X_m)$ — the algebra generated by m generic matrices of order $n \times n$, i.e., matrices whose entries are commutative indeterminates over the rationals Q. The proof that $Q(X)$ is not a crossed-product is obtained by first assuming that this algebra is a croosed-product with a group Γ. Then it is shown that every central simple algebra of dimension n^2 over any field of characteristic zero is a crossed-product with the same group Γ. We then exhibit a field F of power series over which every algebra of that dimension is a crossed-product only of an abelian group which is a direct product of cyclic groups of prime order; therefore, Γ must be such a group. Next, we find a prime p such that for its p-adic field Q_p there exists division rings of dimension n^2 over Q_p whose maximal abelian normal commutative subfields have a group of automorphisms which is a cyclic extension of a cyclic 2-group S_2. Finally, only for $n = 2^{v_0} q_1 q_2 \cdots q_r$, $0 \leqq v_0 \leqq 2$, q_i distinct odd primes, do there exist groups Γ of order n which are both direct products of cyclic groups of prime order as well as cyclic extensions of S_2 by a cyclic group; this clearly proves our main result,

1. Power series fields

Let F be a field of characteristic zero. Denote by $F\{t\}$ the field of power series

$$p\{t\} = \sum_{v \geqq m} a_v t^v, \qquad a_v \in F, \qquad m > -\infty.$$

We need a few properties of these fields.

PROPOSITION 1. *Let H be an algebraic extension of degree n over $K = F\{t\}$, then:*

1. *$H = K_0[\tau]$, where $K_0 = F_0\{t\}$ with F_0 an algebraic extension of degree of F and $\tau = (\gamma^{-1} t)^{1/e}$, $0 \neq \gamma \in F_0$ and $fe = n$.*

2. *$H \cong F_0\{\tau\}$ by the correspondence*

$$\sum_{\rho=0}^{e-1} \left(\sum_{\mu=0}^{f-1} \sum_{v \geqq m} a_{v\mu\rho} t^v \alpha_\mu \right) \tau^\rho \to \sum_{v,\rho} \left(\sum_{\mu} a_{v\mu\rho} \alpha_\mu \gamma^v \right) \tau^{ev+\rho}.$$

3. *If F is algebraically closed, we can choose $\gamma = 1$, and then H is a Kummer extension of K.*

The proof of these facts is well known. For (1) see, e.g., [4, Ex. 1 p. 67]. In this case, K_0 is the inertia subfield of H, and H over K is completely ramified. Part (2) is readily proved by a direct computation.

We extend the last result to the field of power series in any finite number of indeterminates.

Let $t_1, t_2, \cdots, t_r$ be a finite set of indeterminates. Define successively: $F\{t_1, \cdots, t_j\} = (F\{t_1, \cdots, t_{j-1}\})\{t_j\}$. Thus the general element of $F\{t_1, \cdots, t_j\}$ has the form:

$$p\{t_1, \cdots, t_j\} = \sum_{\nu_j \geqq m_j} \quad \sum_{\nu_{j-1} \geqq m_{j-1}} \cdots \sum_{\nu_1 \geqq m_1} a_{\nu_1 \nu_2 \cdots \nu_j} t_1^{\nu_1} t_2^{\nu_2} \cdots t_j^{\nu_j}$$

where $m_i = m_i(\nu_{i+1}, \cdots, \nu_j) > -\infty$ for $i = 1, \cdots, j-1$, $m_j > -\infty$.

Clearly, each $F\{t_1, \cdots, t_j\}$ is a field and the extension of the proposition for these fields is:

Proposition 2. *Let H be an algebraic extension of degree n of $K = F\{t_1, \cdots, t_r\}$. Then:*

(1) *$H = K_0[\tau_1, \cdots, \tau_r]$ where $K_0 = F_0\{t_1, \cdots, t_r\}$ and F_0 is an algebraic extension of degree f over F. The elements $\tau_1, \cdots, \tau_r$ satisfy the relations:*

$$\gamma_1^{-1}\, t_1 = \tau_1^{\nu_{11}}\,, \gamma_2^{-1}\, t_2 = \tau_1^{\nu_{21}}\, \tau_2^{\nu_{22}} . \cdots,$$
$$\gamma_i^{-1}\, t_j = \tau_1^{\nu_{i1}}\, \tau_2^{\nu_{i2}} \cdots \tau_i^{\nu_{ii}} \;\cdots$$

with $\gamma_i \in F_0$, $n = f\nu_{11}\nu_{22} \cdots \nu_{rr'}$, and $[K[\tau_1, \cdots, \tau_i]\colon K[\tau_1, \cdots, \tau_{i-1}]] = \nu_{ii}$.

(2) *$H \cong F_0\{\tau_1, \tau_2, \cdots, \tau_r\}$ by an isomorphism which is completely determined by the correspondence $\tau_i \rightarrow \tau_i$ for all i, and by virtue of being the identity on F_0.*

(3) *If F is algebraically closed, then we can choose $\gamma_i = 1$.*

The proof is by induction on r, and for $r = 1$ our proposition is Proposition 1.

Let $K_{r-1} = F\{t_1, \cdots, t_{r-1}\}$. Then since $K = K_{r-1}\{t_r\}$, it follows by Proposition 1 that $H = K_0[\tau_r]$ where K_0 is an algebraic extension of degree f_{r-1} and $\tau_r = (u^{-1} t_r)^{1/\nu_{rr}}$, $u \in K_0$ and $f_{r-1}\nu_{rr} = n$. By the induction assumption, we have $K_0 = F_0[\tau_1, \cdots, \tau_{r-1}]$ with the τ_i satisfying the relations:

$$\gamma_1^{-1} t_1 = \tau_1^{\nu_{11}}, \gamma_2^{-1} t_2 = \tau_1^{\nu_{21}} \tau_2^{\nu_{22}}, \cdots, \gamma_{r-1}^{-1} t_{r-1} = \tau_1^{\nu_{r+11}} \cdots \tau_{r-1}^{\nu_{r-1\, r-1}}.$$

and $f_{r-1} = f\nu_{11}\nu_{22} \cdots \nu_{r-1\, r-1}$ where $f = [F_0 \colon F]$. We also have

$K_0 \cong F_0\{\tau_1, \cdots, \tau_{r-1}\}$ by the induction assumption (2) in our proposition. Assume, therefore, that $u \in F_0\{\tau_1, \cdots, \tau_{r-1}\}$.

Set $u^{-1} = b_m\tau_{r-1}^m + b_{m+1}\tau_{r-1}^{m+1} + \cdots b_m \neq 0$ in $F_0\{\tau_1, \cdots, \tau_{r-2}\}$, and then $u^{-1/v_r} = b_m^{-1/v_{rr}}\tau_{r-1}^{m/v_{rr}}(1 + c_{1\,r-1}\tau_{r-1} + \cdots)^{1/v^{rr}}$. Now put $u_{r-1}^{-1} = (1 + c_{1\,r-1}\tau_{r-1} + \cdots)^{1/v_{rr}} \in F_0\{\tau_1, \cdots, \tau_{r-1}\}$. The same procedure can be continued with $\bar{b}_m^{-1/v_{rr}}$ etc., and finally we get

$$u^{-1/v_{rr}} = \tau_1^{\alpha_1}\tau_2^{\alpha_2}\cdots\tau_{r-1}^{\alpha_{r-1}}u_0u_1u_2\cdots u_{r-1}.$$

$u_0^{v_{rr}} \in F_0, u_1 = 1 + c_{11}\tau_1 + \cdots, u_2 = 1 + c_{21}\tau_2 + \cdots, \cdots, u_{r-1} = 1 + c_{1\,r-1}\tau_{r-1+} \cdots$. $c_{iv} \in F_0\{\tau_1, \cdots, \tau_{i-1}\}$ and $\alpha = v_{ri}/v_{rr}$ with v_{ri} integers.

Hence $\tau_r = (u^{-1}t_r)^{1/v_{rr}} = \tau_1^{\alpha_1}\tau_2^{\alpha_2}\cdots\tau_{r-1}^{\alpha_{r-1}}u_0u_1\cdots u_{r-1}t^{1/v_{rr}}$.

Finally, setting $u_0^{v_{rr}} = \gamma_r$, and replacing τ_r by $u_1^{-1}u_2^{-1}\cdots u_{r-1}^{-1}\tau_r$ which also generates H over K_0, we get that this new τ_r also satisfies $\gamma_r^{-1}t_r = \tau_1^{v_{r1}}\cdots\tau_r^{v_{rr}}$.

We also have $v_{rr}f_{r-1} = n$. Hence by induction, we get

$$n = fv_{11}v_{22}\cdots v_{rr}.$$

The proof of (2) follows now, by applying (2) of Proposition 1 to $H = K_0[\tau_r]$, and the induction assumption on $K_0 \cong F_0\{\tau_1, \cdots, \tau_{r-1}\}$.

If F_0 is algebraically closed, use induction for $i < r$ to obtain $\gamma_i = 1$ and replace τ_r by $\gamma_r^{1/v_{rr}}\tau_r$, then the corresponding new $\gamma_r = 1$.

Note also that Proposition 1 yields that $[K_0[\tau_r]\colon K_0] = v_{rr}$ and this means that $[K[\tau_1, \cdots, \tau_r]\colon K[\tau_1, \cdots, \tau_{r-1}]] = v_{rr}$. This and the induction assumption conclude the proof.

We shall also need a simple lemma on field extensions.

LEMMA A 1) *Let $H = F[\alpha]$ be an algebraic extension of prime degree p of the field F. Then $H = F[\alpha^m]$ for every m, $(m, p) = 1$, and for which F contains the* m*th roots of one.*

2) *Let $H = F[w_1^{1/q_1}, \cdots, w_n^{1/q_r}]$, $w_i \in F$, be an algebraic extension of F of degree $n = q_1q_2\cdots q_r$. If the q_i are prime and F contains the q_i*th *roots of one for all $i = 1, \cdots, r$, then H is an abelian extension of F with a galois group $S_1 \times \cdots \times S_r$ which is a direct product of cyclic groups S_i of order q_i.*

PROOF. If $\alpha^m \notin F$ then $H \supset F[\alpha^m] \supset F$, and since $[H : F] = p$ is prime we must have $F[\alpha^m] = H$. If $\alpha^m = a \in F$, then $a \neq 1$ since $\alpha \notin F$ and F contains all mth roots of one. The last condition also implies that $F[\alpha]$ is a normal extension of F as a splitting field of $x^m - a$; hence its galois group must be cyclic S of prime order p. Let σ be a generator of S; then $\sigma^p = 1$. But on the other hand, since $\alpha^m - a = 0$, then $\sigma(\alpha) = \omega\alpha$ with ω an mth root of one and, therefore, $\sigma^m(\alpha) = \omega^m\alpha = \alpha$ which implies that $\sigma^m = 1$. This is impossible since $(m, p) = 1$.

To prove (2) we note that H is a normal extension of F as a splitting field of the polynomials $x^{q_i} - \omega_i$. If u_i is a root of this polynomial and σ an automorphism of H over F, then $\sigma(u_i) = \omega_i u_i$ where ω_i is a q_ith root of one. The mapping $\sigma \to (\omega_1, \omega_2, \cdots, \omega_r)$ will define a homomorphism of the galois group into a product $\Gamma = S_1 \times \cdots \times S_r$ of cyclic groups S_i of order q_i. The order of the latter is $q_1 \cdot q_2 \cdots q_r = n$ which is exactly the order of the galois group of H over K, hence this group is isomorphic with Γ. Q.E.D.

The construction of the field of power series $F\{t_1, \cdots, t_r\}$ can be extended to a non-commutative case: Let D be a division ring (not necessarily commutative) and τ be an automorphism of D. Let $D\{x\}$ be the set of all formal power series $\{p(x) = \Sigma_{v \geqq m} d_v x^v;\ d_v \in D,\ m > -\infty\}$. Then $D\{x\}$ becomes a division ring with multiplication defined by the relation $xd = \tau^{-1}(d)x$ (or equivalently, $x\tau(d) = dx$) for every $d \in D$. The commutative case is obtained with $\tau =$ identity and $D = F$ is a commutative field.

The division ring $D\{x_1, \cdots, x_r\}$ is defined successively as $(D\{x_1, \cdots, x_r\})\{x_r\}$, with respect to the given automorphism $\tau_1, \cdots, \tau_r$ where τ_1 is an automorphism of D and τ_{i+1} is an automorphism of $D\{x_1, \cdots, x_i\}$.

2. Division algebras over power series fields

Let F be an algebraically closed field. Consider the commutative field $K = F\{t_1, t_2, \cdots, t_{2r}\}$ of power series in $2r$ indeterminates t_i. Let $n = q_1 \cdot q_2 \cdots q_r$ be a product of r prime numbers (not necessarily different). For each i, consider the cyclic extension of degree q_i, $K_i = K[t_{2i-1}^{1/q_i}]$ of K with the generating automorphism σ_i defined by $\sigma_i(\tau_i) = \omega_i\tau_i$ where $\tau_i = t_{2i-1}^{1/q_i}$ and ω_i is a primitive q_i root of one.

Define the cyclic central simple algebra $A_i = (K_\iota, \sigma_i, t_{2i})$. Thus, $A_i = \Sigma K_i \sigma_i^v$ with multiplication defined by the relations $\sigma_i \cdot k = \sigma_i(k)\sigma_i$ for $k \in K_i$ and $\sigma_i^{q_i} = t_{2i}$.

Our aim is to show:

THEOREM 3. *The algebra $A = A_1 \otimes, \cdots, \otimes A_r$ is a central division algebra* *of dimension n^2 over its center K; and the maximal subfields L of A are abelian extensions of K with a galois group $\Gamma = S_1 \times \cdots \times S_r$ with S_i* cyclic *groups of order q_i.*

Proof. First we obtain a different representation of A: Consider the division ring of non-commutative power series $D = F\{x_1, x_2, \cdots, x_{2r}\}$ with multiplication defined by $x_{2i}x_{2i-1} = (\omega_i x_{2i-1})x_{2i}$ and in all other cases $x_i x_j = x_j x_i$. That is, $\boldsymbol{D}$ is a non-commutative power series division ring obtained successively by $2r$ steps: each even step $2i$ is a non-commutative extension obtained by an automorphism which maps $x_{2i-1} \to \omega_i x_{2i-1}$ and which leaves the other x_j, $j < 2i-1$, invariant.

We will show that $A \cong \boldsymbol{D}$, which will prove that A is a division ring. Since $(A_i : K) = q_i^2$ and K is its center, it follows that $(A : K) = (q_1 \cdot q_2 \cdots q_r)^2 = n^2$ and it is known that K is its center.

Define the isomorphism ϕ: $A \to \boldsymbol{D}$ by the correspondence $\phi(\tau_i) = x_{2i-1}$, $\phi(\sigma_i) = x_{2i}$ where $\tau_i = t_{2i-1}^{1/q_i}$, $i = 1, 2, \cdots, r$. That is, the generic element $a \in A$ has the form

$$a = \sum_{(\nu,\mu)} (\sum_{(\rho)} a_{(\nu\mu\rho)} t_1^{\rho_1} t_2^{\rho_2} \cdots t_{2r}^{\rho_{2r}}) \tau_1^{\nu_1} \cdots \tau_r^{\nu_r} \sigma_1^{\mu_1} \cdots \sigma_r^{\mu_r}$$

and its image will be

$$\phi(a) = \sum a_{(\nu\mu\rho)} x_1^{\nu_1 + q_1\rho_1} x_2^{\mu_1 + q_1\rho_2} \cdots x_{2r-1}^{\nu_{2r-1} + q_r\rho_{2r-1}}. x_{2r}^{\nu_{2r} + q_r\mu_r} \quad .$$

Note that in the sums, $0 \leqq \nu_i < q_i$, and $0 \leqq \mu_i < q_i$. The image $\phi(a)$ is obtained by preserving the relations $\tau_i^{q_i} = t_{2i-1}$, $\sigma_i^{q_i} = t_{2i}$, which requires that $\phi(t_{2i-1}) = x_{2i-1}^{q_i}$ and $\phi(\sigma_i) = x_{2i}^{q_i}$.

The map ϕ defines a one-to-one correspondence between the elements of A and $\boldsymbol{D}$ since every integer m can be uniquely written in the form $m = \nu + q_i\rho$ with $0 \leqq \nu < q_i$. To verify that ϕ is an automorphism, it suffices to show that the basic relations of A are preserved under ϕ. These relations are: the commutativity of the t_i's; $\sigma_i\tau_i = (\omega_i\tau_i)\sigma_i$; $\sigma_i\tau_j = \tau_j\sigma_i$ for $i \neq j$; and $\tau_i^q = t_{2i-1}$, $\sigma_i^{q_i} = t_{2i}$. The definitions of $\boldsymbol{D}$ and ϕ were, in fact, motivated by these conditions, and so they are easily checked, e.g., $\phi(\sigma_i\tau_i) = x_{2i}x_{2i-1} = (\omega_i x_{2i-1})x_{2i}$, $= \phi(\omega_i\tau_i)\sigma_i$, etc.

We shall replace A by $\boldsymbol{D}$ and let L be a maximal subfield of A so that $(L : K) = n$. It follows by Proposition 2 that $L = K[\xi_1, \xi_2, \cdots, \xi_r]$ with the relations:

$$(R_1) \qquad t_1 = \xi_1^{\nu_{11}},\ t_2 = \xi_1^{\nu_{21}}\xi_2^{\nu_{22}}, \cdots, t_i = \xi_1^{\nu_{i1}}\xi_2^{\nu_{i2}} \cdots \xi_i^{\nu_{ii}}$$

with $\nu_{ii} \geqq 1$ and $n = \nu_{11} \cdot \nu_{22} \cdot \cdots \cdot \nu_{2r\,2r}(= q_1 \cdot q_2 \cdots q_r)$.

We introduce the valuation $v(f)$ of D by setting for

$$f = \sum_{\nu_{2r} \geqq m_{2r}} \ \sum_{\nu_{2r-1} \geqq m_{2r-1}} \cdots \sum_{\nu_1 \geqq m_1} a_{\nu_1,\nu_2,\cdots,\nu_{2r}} x_1^{\nu_1} \cdot x_2^{\nu_2} \cdots x_{2r}^{\nu_{2r}},$$

for which $a_{m_1,m_2\cdots,m_{2r}} \neq 0$, the value $v(f) = (m_1, m_2, \cdots, m_{2r}) \in \mathbf{Z}^{2r}$. Since the product of two monomials is a monomial, it follows easily that $v(fg) = v(f) + v(g)$ and $v(f^m) = mv(f)$ where the addition and multiplication are vector addition and scalar multiplication in $\mathbf{Z}^{2r}$.

Hence the relation of (R_1): $\xi_1^{\nu_{i1}} \cdots \xi_i^{\nu_{ii}} = t_i^q = x_i$ where $q = q_{i_0}$ with $i_0 = \left[\dfrac{i+1}{2}\right]$ yields that

$$(R_2) \qquad \nu_{i1}v(\xi_1) + \nu_{i2}v(\xi_2) + \cdots + \nu_{ii}v(\xi_i) = (0,0,\cdots,q,0,\cdots,0).$$

We can show now by induction on i that, for each i, $v(\xi_i) = (\mu_{i1}, \mu_{i2}, \cdots, \mu_i, 0, \cdots, 0) \in \mathbf{Z}^{2r}$. Indeed, for $i = 1$, $\nu_{11}v(\xi_1) = (q_1, 0, 0, \cdots, 0)$ yields that $v(\xi_1) = (\mu_{11}, 0, \cdots, 0)$. A similar application of (R_1) and an induction assumption on i yields that $v(\xi_i)$ has the required form.

Let $\mathscr{N} = (\nu_{ik})$ be the triangular $2r \times 2r$ matrix obtained by integers ν_{ik}, and let $\mathscr{M} = (\mu_{ik})$ the triangular matrix obtained by the rows $v(\xi_i)$. The relations (R_2), for every i, yield the simple matrix relation $\mathscr{N}\mathscr{M} = \text{Diag}\{q_1, q_1, q_2, q_2, \cdots, q_r, q_r\}$.

Some of the primes q_i may be equal, so we could have started from the case, $q_1 = q_2 = \cdots = q_{\lambda_1} = p_1$,

$$q_{\lambda_1+1} = \cdots = q_{\lambda_1+\lambda_2} = p_2, \cdots, q_{\lambda_1+\cdots+\lambda_{s-1}+1} = \cdots = q_r = p_s$$

where p_i are the different primes among the q_j. Let $m = p_1 \cdot p_2 \cdots p_s$, and consider the diagonal matrix $\mathscr{U} = \text{Diag}\{mq_1^{-1}, mq_2^{-1}, \cdots, mq_2^{-1}\}$. Let $\mathscr{R} = \mathscr{M}\mathscr{U}$, which is also a triangular matrix, with integral entries, clearly $\mathscr{N}\mathscr{R} = \mathscr{N}\mathscr{M}\mathscr{U} = \text{Diag}\{q_1, \cdots, q_{2r}\} \cdot \text{Diag}\{mq_1^{-1}, \cdots, mq_{2r}^{-1}\} = m._1$ which is a scalar matrix. Hence $\mathscr{R}$ and $\mathscr{N}$ commute, so $\mathscr{R}\mathscr{N} = m._1$. If $\mathscr{R} = (\rho_{ik})$ then we have the relation $\sum_{\lambda=1}^{k} \rho_{i\lambda}\nu_{\lambda k} = 0$ if $k < i$ and $\sum_{\lambda=1}^{i} \rho_{i\lambda}\nu_{\lambda i} = m$.

Consider the element $k_\iota = \prod_{\lambda=1}^{i} t_\lambda^{\rho_{i\lambda}}\ K$. The preceeding relations show that

$$k_i = \prod_\lambda t_\lambda^{\rho_{i\lambda}} = \prod_\lambda (\xi_1^{\mu_{\lambda 1}} \cdots \xi_\lambda^{\mu_{\lambda\lambda}})^{\rho_{i\lambda}} = \xi_1^0 \cdot \xi_2^0 \cdots \xi_j^m = \xi_i^m,$$

and setting $d_i = mq_{i_0}^{-1}$ where $i_0 = \left[\frac{i+1}{2}\right]$, $\eta_i = \xi_i^{d_i}$, then

$$(R_3) \qquad (d_i, q_{i_0}) = 1 \text{ and } \eta_i^{q_{i_0}} = k_i \in K.$$

Finally, we prove that $L = K[\eta_{j_1}, \eta_{j_2}, \cdots, \eta_{j_r}]$ and $\eta_{j_\lambda}^{q_\lambda} = k_{j_\lambda} \in K$. Since $[L\colon K] = q_1 \cdot q_2 \cdots q_r$, our theorem will follow from Lemma A.

Indeed choose the η_{j_λ} as follows: Let ξ_t be the first $\xi_i \notin K$. Then $K = K_{t-1} = K[\xi_1, \cdots, \xi_{t-1}]$. We have $[K_{t-1}[\xi_t]\colon K_{t-1}] = q_{t_1}$, with $t_1 = \left[\frac{t+1}{2}\right]$. Since q_{t_1} is prime, if we set $t = j_1$, then it follows by (R_3) in view of Lemma A, that $K_t = K[\xi_t] = K[\eta_t]$. Suppose we have chosen $j_1 < j_2 <, \cdots, < j_{\rho-1}$ such that $q_{t_\mu} = [K[\eta_{j_1}, \cdots, \eta_{j_\mu}]\colon K[\eta_{j_1}, \cdots, \eta_{j_{\mu-1}}]]$ and $K[\eta_{j_1}, \cdots, \eta_{j_\mu}] = K[\xi_1, \cdots, \xi_\sigma] = K_\sigma$ for some $\sigma = \sigma(\mu)$. In particular, let $K[\eta_{j_1}, \cdots, \eta_{j_{\rho-1}}] = K[\xi_1, \cdots, \xi_s] = K_s$. Let ξ_v be the first ξ_i for which $\xi_i \notin K_s$, i.e., $K_s = K_{v-1} \neq K_v = K_{v-1}[\xi_v]$. So set $j_\rho = v$, and then again (R_3) in view of Lemma A implies that $K_{v-1}[\eta_{j_\rho}] = K_v$.

Thus, $j_{\rho-1} < j_\rho$ and $[K[\cdots, \eta_{j_\rho}] : K[\cdots, \eta_{j_{\rho-1}}]] = q_t$ and the other relations also hold. Finally we get $K[\eta_{j_1}, \eta_{j_2}, \cdots, \eta_{j_u}] = K[\xi_1, \cdots, \xi_{2r}] = H$. Now $[H\colon K] = q_{t_1} \cdot q_{t_2} \cdots q_{t_u} = n$ and since $n = q_1 \cdot q_2 \cdots q_r$, we must have $u = r$, $q_{t_1} = q_1, q_{t_2} = q_2, \cdots, q_{t_u} = q_r$. This completes the proof of our theorem.

3. Division algebras over p-adic fields

Let n be a fixed integer and Q_p be the field of p-adic numbers. It is well known (e.g., [2, p. 143] that there exists a division algebra B of dimension n^2 over Q_p. Actually, we are going to choose p so that we can restrict the galois groups of the field extensions of degree n of Q_p. But for our application, we prefer to state this result in the form:

THEOREM 3. *There exists a prime p, and a division algebra B of dimension n^2 over Q_p, such that the maximal subfields of B, which are normal abelian extensions of Q_p, are either cyclic or their galois group is $S_2 \times S_m$ with S_2 a cyclic group of order 2, S_m cyclic of order m, and $n = 2m$.*

PROOF. Central division algebras B of dimension n^2 exist for any p. We are going to choose the prime p such that the only normal abelian extensions of Q_p of degree n have the property stated in the theorem.

If $(p, n) = 1$, then any algebraic extension H of Q_p of degree n is tamely ramified and, therefore, can be obtained in two steps, $Q_p \subset T \subset H$, where T is a maximal ramified extension of Q_p in H, and H is totally and tamely ramified over T. Let $(T:Q_p) = f$, $(H:T) = e$; then $n = ef$. If H is assumed to be a normal extension of Q_p, it is also normal over T and hence, $H = T(\Pi)$ where $\Pi^e = \pi \in T$ is a prime element and T contains the primitive eth roots of one (e.g. [5, ch. I, proposition 1]. Let Γ be a galois group of H over Q_p, and Γ_T the inertia subgroup, which is also the group of automorphisms which leave T invariant; in our case, it must be cyclic of order e. Furthermore, Γ/Γ_T is isomorphic with the group of automorphisms of T over Q_p which is cyclic of order f (e.g. [5, corollary, p. 27]. Thus, we have the exact sequence (*) $0 \to \Gamma_T \to \Gamma \to \Gamma/\Gamma_T \to 0$.

By reproducing part of the proof used in constructing the Artin symbol, we show that if $(n,p) = 1$, then $e \mid p-1$: Indeed, let $\sigma \in \Gamma$ arbitrarily and $\tau \in \Gamma_T$ such that $\tau(\Pi) = \omega\Pi$ where ω is a primitive eth root of one. Furthermore, $\sigma(\Pi) = u\Pi$ for a unit $u \in H$. If Γ is *abelian* then $\sigma\tau(\Pi) = \sigma(\omega)\sigma(\Pi) = \sigma(\omega)u\Pi$ and $\tau\sigma(\Pi) = \tau(u)\tau(\Pi) = \tau(u)$ and $\sigma\tau = \tau\sigma$ implies that $\sigma(\omega)u = \tau(u)\omega$. Now $\tau \in \Gamma_T$ and, therefore, passing to the residue field, we have $\overline{\tau(u)} = \bar{u}$. Consequently, $\overline{\sigma(\omega)u} = \overline{\tau(u)\omega}$ implies that $\overline{\sigma(\omega)} = \bar{\omega}$. Finally, ω and $\sigma(\omega)$ are both roots of the polynomial $X^e - 1$. Since $(e,p) = 1$ (as $e \mid n$), it follows that different roots of this polynomial determine different classes in the residue field; and hence, $\sigma(\omega) = \omega$. This being true for every $\sigma \in \Gamma$ implies that $\omega \in Q_p$. But the only roots of one of order $m, (m,p) = 1$, which lie in Q_p are those with $m = p-1$; hence in our case $e \mid p-1$. These facts about the roots of one are an immediate consequence of the result that the extension by an mth root of one is unramified, and its degree is g where g is the minimal integer such that $p^g - 1 \equiv 0(m)$.

Let $n = 2^{\nu_0}q_1^{\nu_1}q_2^{\nu_2}\cdots q_r^{\nu_r}$, where q_i are different odd primes. Take $d \equiv 2 \pmod{q_i}$, $d \equiv 3 \pmod 4$, for all i. Then $(d,n) = 1$, and so by the Dirichlet theorem, there exists a prime number $p = d + 4nb$. For this prime number, $p - 1 = d - 1 + 4nb \equiv 1 \pmod{q_i}$, and $p - 1 \equiv 2 \pmod 4$. Thus neither q_i nor 4 divides $p-1$; hence $(n, p-1) = 1$ or $= 2$.

Thus, given n, we choose the preceding p and respectively, Q_p; then the only ramification factor possible is $e = 1$, or 2 since $e \mid (n, p-1)$. Consequently, the galois group is either cyclic for the case $e = 1$, or a cyclic extension of the group $S_f \cong \Gamma/\Gamma_T$ by $\Gamma_T \cong S_2$. Such a group is commutative if and only if either it is itself cyclic or it is equal to $S_2 \times S_f$. Clearly then $n = 2f$.

COROLLARY 4. *If n is fixed and p is chosen as before, then there may exist a normal abelian extention H of degree n over Q_p whose galois group is a direct* *product of cyclic groups of prime order, only if* $n = 2^{v_0} q_1 q_2 \cdots q_r$, $0 \leqq v_0 \leqq 2$, *and the* q_i *are distinct odd primes.*

Indeed, a cyclic group S_n or the group $S_2 \times S_f$, which are the possible galois groups, is a direct product of cyclic groups of prime order if and only if n, or respectively f, is a product of different primes. This clearly implies the corollary.

4. The generic division algebra

Let $X_1, \cdots, X_m$, $m \geqq 2$, be m-generic matrices of order n over a universal domain $\Omega \supseteqq Q$, i.e., the entries $\xi^i_{\lambda\mu}$, $i = 1, \cdots, m$, λ, $\mu = 1, \cdots, n$, are commutative indeterminates over Q as well as any field of characteristic zero which will occur in our discussions. Let $Q[\xi]$, $Q(\xi)$ be the ring of all polynomials, the rational functions, respectively, in the ξ's over Q. It is well known (e.g., C. Procesi [6]) that the ring $Q[X_1, \cdots, X_m]$ is a domain which has an Ore ring of quotients $Q(X) = Q(X_1, \cdots, X_m) \subseteq M_n(Q(\xi))$. The division ring $Q(X)$ is a division ring of dimension n^2 over its center C. We shall refer to $Q(X)$ as the generic division ring of dimension n^2, and our main result is:

THEOREM 5. *If for some odd prime* q, $q^2 \mid n$, *or* $8 \mid n$, *then the generic division algebra of dimension* n^2 *is not a crossed-product.*

We begin with a lemma on polynomial identities, which actually could be avoided by choosing m to be infinite.

LEMMA 6. *Let* S *be a central simple algebra of dimension* n^2 *over an infinite center* C, *and* $p[x_1, \cdots, x_m] = 0$ *be a non-commutative polynomial relation which vanishes for every substitution* $x_i = s_i \in S$ *such that* $C[s_1, \cdots, s_m] = S$. *Then* $p[x] = 0$ *vanishes for all substitution* $x_i = \bar{s}_i \in S$ *(with no restriction).*

PROOF. Let $x_i = \bar{s}_i \in S$ arbitrary elements, and let $\{s_i\}$ be a set of generators of S over C; such a set exists if $m \geqq 2$. Consider $p[(1-t)\bar{s}_i + ts_i] = \pi(t)$ as a polynomial in a commutative t. If $p[\bar{s}_i] \neq 0$, then $\pi(t)$ does not vanish identically in t. Therefore, there is only a finite number of values of t in C such that $p[(1-t)\bar{s}_i + ts_i] = 0$.

On the other hand, the proper subalgebras of S satisfy the identity $S_{2n-2}[y_1, \cdots, y_{2n-2}]^n = 0$ [3, lemma 6] and since $S = C[s_1 \cdots s_n]$, $S_{2n-2}[y]^n \neq 0$ in S. So there exist polynomials $g_i[x]$ such that $S_{2n-2}[g_1[x], \cdots, g_{2n-2}[x]]^n \neq 0$ for the substitution $x_i = s_i$, i.e., $g_i[s_j]$ are the elements which do not annihilate this polynomial. In particular, this implies that the polynomial $S_{2n-2}[g_1[(1-t)\bar{s}_i + ts_i],$

$\cdots,]^n = h(t)$ is not identically zero as it does not vanish for $t = 1$. Hence, we can find a value $t = t_0 \in C$ such that both $p[(1 - t_0)\bar{s}_i + t_0 s_i] \neq 0$, and $h[t_0] \neq 0$. This leads to a contradiction, since $h[t_0] \neq 0$ implies that the algebra $C[\cdots,(1 - t_0)\bar{s}_i + t_0 s_i,\cdots] = S$ as it does not satisfy $S_{n-2}[x]^n = 0$. But then by assumption of the lemma, we must have $p[(1 - t_0)\bar{s}_i + t_0 s_i] = 0$. Consequently we have shown that $p[\bar{s}_i] = 0$, as required.

We need also the following localization theorem (Small [7]).

THEOREM 7. *Let P be a prime ideal in a prime ring R, which is an algebra over a field F. If R and R/P satisfy exactly the same polynomial identities, then in the quotient ring $Q(R)$ (which exists by Posner's theorem), the set $Q_P(R) = \{a^{-1}b \mid a$ regular $\operatorname{mod} P\}$ is a subring with a maximal ideal $PQ_P(R) = \{a^{-1}b \mid b \in P\}$ and $Q_P(R)/PQ_P(R) \cong R/P$.*

The beginning of the proof of the main Theorem 5 starts by assuming that the generic algebra $Q(X)$ is a crossed-product of a maximal field $C(U)$ with a galois group Γ. This means that U satisfies a polynomial: $(G1)\, 0 = f(U) = U^n + C_1U^{n-1} + C_2U^{n-2} + \cdots + C_n$, $C_i \in C$, and $P_{\theta_1}[U] = U$, $P_{\theta_2}[U],\cdots,P_{\theta_n}[U]]$ are the different roots of $f(\lambda) = 0$; also for each $\theta \in \Gamma$, there exist $Z_\theta \in Q(X)$ such that $(G2)\, Z_\theta\, U\, Z_\theta^{-1} = P_\theta[U]$, $(G3)\, Z_\Psi = Z_{\theta\Psi}\, a(\theta, \psi)$, and $a(\theta, \psi) = P(U;\, \theta, \psi) \in C(U)$ satisfies the co-cycle conditions: $(G4)\ \delta a = 1$. All these elements, together with the elements $(P_{\theta_i}[U] - P_\theta\,[U])^{-1}$, $a(\theta,\psi)^{-1}$ and the coefficients in the $P(U;\theta,\psi)$, are non-zero elements of the form $g[X_1,\cdots,X_m]^{-1}h[X_1,\cdots,X_m]$.

Let $f_G[X_1,\cdots,X_m] \in Q[X]$ be the non-zero product of all polynomials appearing in all nominators and denominators of these fractions.

In the next stage, we consider any field F of characteristic zero and a division algebra D of dimension n^2 over F. Now consider $Q[X] \subseteq F[X]$ since $Q \subseteq F$. The inclusion can be extended to the embedding of quotient rings, i.e., to the generic division rings $Q(X) \subseteq F(X)$. This follows from the fact that an element is regular in $Q[X]$ if and only if its determinant is $\neq 0$, and so also non-zero in $F[X]$; therefore, it is also invertible in $F(X)$. In particular all relations $(G1)$, etc. will be valid also in $F(X)$. In particular, this means that $F(X)$ is also a crossed-product with the group Γ.

But we aim further: Consider all homomorphisms ϕ: $F\ [X] \rightarrow D$, where ϕ is surjective, and then $\cap_\phi \operatorname{Ker}\phi = 0$. Indeed, let $p[X] \in \cap \operatorname{Ker}\phi$. Since every surjective ϕ is obtained by arbitrary mappings of $X_i \rightarrow d_i$, where $F[d_1,\cdots,d_m] = D$, it follows that $p[x_1,\cdots,x_m] = 0$ for all sets of generators of the division algebra D.

But then by Lemma 6, $p[x_1, \cdots, x_m] = 0$ is a polynomial identity of $\boldsymbol{D}$. Now. $(\boldsymbol{D}\colon F) = n^2$; hence $p[x] = 0$ vanishes for all central simple algebras of dimension n^2 over their center [3, p. 477]. In particular, $p[x] = 0$ also in $F(X)$ which means that $p[X_1, \cdots, X_m] = 0$, i.e., $\cap_\phi \operatorname{Ker} \phi = 0$.

A simple consequence of this result is that considering the preceding non-zero polynomial $f_G[X]$, we can find an epimorphism $\phi : F[X] \to \boldsymbol{D}$ such that $f_G[X] \notin \operatorname{Ker} \phi$. Now $(\boldsymbol{D} : \text{Center}) = n^2$; hence it satisfies the same identities as $F[X]$ and therefore we can apply Theorem 7 with $P = \operatorname{Ker} \phi$. Now $f \notin P$; hence all the elements appearing in the conditions $(G1)$, $(G2)$, $\cdots$ will belong to the local quotient ring $Q_P(R)$ and not to the ideal $PQ_P(R)$ as the denominators divide $f_G \notin P$ and therefore they are regular mod P (since $R/P \cong D$ is a division ring). Consequently, the relations $(G1), \cdots$ will hold in $Q_P(R)/PQ_P(R) \cong R/P \cong \boldsymbol{D}$, i.e., the algebra $\boldsymbol{D}$ contains elements satisfying these relations. Note also that the elements of the center remain in the center of the ring of quotients and in the quotient rings as they commute with a set of generators. Denote respectively, by small letters, the elements in $\boldsymbol{D}$ corresponding to the classes in $Q_P(R)/Q_P(R)$, i.e., $U + PQ_P(P) \to u$, etc. Thus the division algebra $\boldsymbol{D}$ will contain the elements $u = p_{\theta_1}(u), \cdots, p_{\theta_n}(u)$ which are n-different roots of the polynomial $f(\lambda) = \lambda^n + c_1\lambda^{n-1} + \cdots + c_n$, and they are different since $[p_{\theta_i}(u) - p_{\theta_j}(u)]^{-1} \in D$ for $i \neq j$. Also $P_\theta(u) \in F(u)$ and $z_\theta u z_\theta^{-1} = p_\theta(u)$, which implies that the inner automorphisms by z_θ induce n different automorphisms on $F(u)$, and, as $\boldsymbol{D} \supseteq F(u)$, it must be a field and $(\boldsymbol{D} : F)) \leqq n$. On the other hand, $f(\lambda)$ has n-different roots so $(F(u) : F) = n$. It follows, therefore, that $F(u)$ is a maximal commutative subfield of F and these automorphisms form the complete set of automorphisms of $F(u)$. Furthermore, since both $a(\theta,\psi)$ and $a(\theta,\psi)^{-1}$ belong to $Q_p(R)$, the relation $z_\theta z_\Psi = z_{\theta\Psi} a(\theta,\psi)$ with $a(\theta,\psi) \in F(u)$ implies that these consist of a group of automorphisms which is clearly isomorphic with the given group Γ. Also, the other relations $(G2)$–$(G4)$ clearly yield that $D \supseteq (F(u), \Gamma, a)$ but, since both are of dimension n^2, $\boldsymbol{D}$ is the crossed-product $(F(u), \Gamma, a)$.

We are now in position to prove Theorem 5:

Assume $Q(X_1, \cdots, X_m)$ is a crossed-product with a group Γ. Then by our preceding result, every central division algebra of dimension n^2 over a field of characteristic zero is a crossed-product of this group Γ. If we apply this theorem to the algebra A of Theorem 3, Γ must be abelian $\cong S_1 \times \cdots \times S_r$, with S_i cyclic. But then applying our result to the algebra $\boldsymbol{B}$ of Theorem 3 and noting that it must be abelian from the previous case, it follows by Corollary 4, that $n = 2^{\nu_0}q_1q_2\cdots q_r$, $0 \leqq \nu_0 \leqq 2$, q_i different odd primes.

Hence, if $8 \mid n$ or if $q^2 \mid n$ for some odd prime q, then $Q(X)$ cannot be a crossed-product. Q.E.D.

References

1. A. A. Albert, *A construction of non-cyclic normal division rings*, Bull. Amer. Math. Soc. **38** (1938), 449–456.

2. A. A. Albert, *Structure of algebras*, Amer. Math. Soc. Colloq. Publ. **XXIV** (1939).

3. S. A. Amitsur, *Prime rings with a polynomial identity*, Proc. Math. Soc. **17** (1967), 470–486.

4. E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, 1967.

5. J. W. Cassels and A. Frohlich, *Algebraic Number Fields*, Academic Press, 1967.

6. C. Procesi, *Non commutative affine rings*, Atti Accade. Naz. Lincei, **VIII** (1967), 239–255.

7. L. Small, To appear in J. Algebra.

The Hebrew University of Jerusalem