Every p-algebra of degree p^2 is a crossed product

Zhengyao Wu
School of Mathematics and Computational Science,
Xiangtan University, Xiangtan, 411105, Hunan, China
wuzhengyao@xtu.edu.cn

July 2, 2026

Contents

Abstract

Let F be a field of characteristic $p > 0$. We resolve Problem 2.2 of Auel–Brussel–Garibaldi–Vishne: every p-algebra of degree p^2 over F is a crossed product.

Keywords: p-algebra, crossed product, cyclic algebra, Artin–Schreier theory, Albert's theorem, Brauer group.

MSC2020: 16K20, 16K50, 12F15.

1 Introduction

Let F be a field of characteristic $p > 0$. A *p-algebra* over F is a central simple F-algebra whose degree is a power of p. A *crossed product* (Definition 2.3) is a central simple algebra containing a Galois maximal étale subalgebra; it is *cyclic* if that subalgebra is a cyclic Galois extension [3, p.221]. Here and below, C_n denotes a cyclic group of order n.

Albert proved that if a field of characteristic p admits a non-trivial p-algebra, then it possesses a cyclic extension of degree p [1, Ch.VII, Theorem 23]; consequently every p-algebra of degree p is cyclic. He also showed that every degree-4 p-algebra in characteristic 2 is a $C_2 \times C_2$-crossed product [1, Ch.XI, Theorem 9]. At the opposite extreme, Saltman showed that over an infinite field of characteristic p, the generic division algebra of degree p^n is not a crossed product for any $n \geq 3$ [11, Theorem 3.4], and Jacob–Wadsworth constructed noncrossed products of index p^m and exponent p^n for all $m \geq n \geq 3$ [7, Theorem 5.4].

Problem 2.2 of Auel–Brussel–Garibaldi–Vishne [3, Problem 2.2] asks for the remaining boundary case:

Determine whether p-algebras of degree p^2 are crossed products.

For odd p, the problem has been completely open. Amitsur and Saltman constructed noncyclic p-algebras of degree p^2 [2, Theorem 3.2], but these are *abelian* crossed products with group $C_p \times C_p$; noncyclic does not imply noncrossed. McKinnie showed that these algebras remain noncyclic after any prime-to-p extension [9, Corollary 3.10], but this does not affect their crossed product status. Rowen and Saltman proved that every degree-p^2 division algebra becomes a $C_p \times C_p$-crossed product over some prime-to-p extension [10, Corollary 1.3], establishing a strong necessary condition that any counterexample would have to violate. All known noncrossed p-algebra constructions require degree $\geq p^3$ (characteristic p), or cohomological dimension ≥ 3 (characteristic 0): Brussel–Tengan constructed noncrossed products over function fields of p-adic curves [5, Theorem 6.1], whose function fields have cohomological dimension 3; neither setting applies to degree p^2 in characteristic p.

In this paper we prove that the answer to Problem 2.2 is affirmative:

Theorem 1.1 (Main)**.** *Let F be a field of characteristic $p > 0$. Then every p-algebra of degree p^2 over F is a crossed product.*

The proof rests on Albert's structure theorem [1, Ch.VII, Theorem 28]: every p-algebra of degree p^2 is similar (Brauer equivalent) to a tensor product of two degree-p cyclic p-algebras $(\alpha, t)_p \otimes_F (\beta, s)_p$, where each factor is a degree-p cyclic algebra as in Definition 2.1: α and β are the Artin–Schreier parameters, t and s the norm parameters. The crossed product status is then determined by the F_p-linear dependence or independence of α and β in the quotient $F/\wp(F)$.

When α, β are F_p-independent, we exhibit the tensor product explicitly as a $C_p \times C_p$ crossed product (Proposition 3.1). When α, β are dependent, Brauer bilinearity forces the index to drop to at most p, reducing the algebra to a matrix algebra $M_{p^2/d}(C)$ over a degree-d cyclic algebra C with $d \leq p$. For $d = p$, the case p-rank $= 1$ is handled by a direct cyclicity criterion (Proposition 4.1); when the p-rank of F exceeds 1, a linear disjointness argument for Artin–Schreier extensions settles the case (Proposition 5.1).

Declaration of generative AI and AI-assisted technologies in the manuscript preparation process. During the preparation of this work, the author used DeepSeek-v4 in order to assist with brainstorming, literature searching, drafting, and proofreading. After using this tool/service, the author reviewed and edited the content as needed and takes full responsibility for the content of the published article.

Acknowledgements. The author is supported by Xiangtan University project 09KZ-KZ08101 *algebraic invariants and local-global principles.*

2 Preliminaries

Throughout this paper, F denotes a field of characteristic $p > 0$. The Artin–Schreier operator is $\wp(a) = a^p - a$. For $\alpha \in F \setminus \wp(F)$, the extension $F(\wp^{-1}(\alpha))$ is cyclic Galois of degree p.

Definition 2.1 (Cyclic p-algebra)**.** For $\alpha \in F$ and $t \in F^\times$, the *cyclic p-algebra* $(\alpha, t)_p$ is the associative F-algebra generated by elements u, w subject to the relations

$$\wp(u) = \alpha, \qquad w^p = t, \qquad wuw^{-1} = u + 1.$$

It is a central simple F-algebra of degree p. By [1, Ch.VII, Theorem 17], a cyclic algebra of prime degree p is a division algebra if and only if its norm parameter is not a norm from the cyclic extension; for $(\alpha, t)_p$ this means $\alpha \notin \wp(F)$ and t is not a norm from $F(\wp^{-1}(\alpha))$.

Lemma 2.2 (Linear disjointness of Artin–Schreier extensions)**.** *For $\alpha, \beta \in F$, the Artin–Schreier extensions $F(\wp^{-1}(\alpha))$ and $F(\wp^{-1}(\beta))$ are linearly disjoint over F (i.e., their compositum has degree p^2 over F) if and only if α and β are F_p-linearly independent in $F/\wp(F)$.*

Proof. Two Artin–Schreier extensions coincide if and only if their parameters differ by a nonzero F_p-multiple modulo $\wp(F)$ [6, Proposition 4.3.10]. For two Galois extensions of prime degree p, the Galois group of their compositum embeds into $C_p \times C_p$ with surjective projections [8, Ch.VI, Theorem 1.14]; its order is either p (the extensions coincide) or p^2 (they are linearly disjoint). Thus they are linearly disjoint precisely when they are distinct. Hence $F(\wp^{-1}(\alpha))$ and $F(\wp^{-1}(\beta))$ are linearly disjoint over F (i.e., their compositum has degree p^2) if and only if $\bar{\alpha}, \bar{\beta}$ are F_p-linearly independent in $F/\wp(F)$. $\square$

This lemma is used in Propositions 3.1 and 5.1 to construct the compositum of two independent Artin–Schreier extensions as a $C_p \times C_p$-Galois maximal subfield.

Definition 2.3 (Crossed product)**.** Let G be a finite group. A central simple F-algebra of degree n is a G-*crossed product* if it contains a G-Galois maximal étale subalgebra (i.e., a direct sum of copies of a G-Galois field extension, of total dimension n over F) [3, p.221]; it is *cyclic* if G is cyclic.

Lemma 2.4 (Height-1 splitting)**.** *[6, Lemma 9.1.7]: every central simple F-algebra of period p is split by a height-1 extension K/F (i.e., $K^p \subseteq F$).*

This is used in the exponent-p subcase of Proposition 4.1 to reduce to a simple purely inseparable splitting field.

Lemma 2.5 (Simple purely inseparable extensions)**.** *If $[F : F^p] = p$, then every finite purely inseparable extension of F is simple; more precisely, $K = F(\gamma^{1/p^f})$ for some $\gamma \in F$ and $f \geq 0$, and $[K : F] = p^f$.*

Proof. Pick $t \in F \setminus F^p$; then $t^p \in F^p$, so $[F^p(t) : F^p] \leq p$. Since $t \notin F^p$, $[F^p(t) : F^p] > 1$; but $[F : F^p] = p$ forces equality $F = F^p(t)$. Hence $1, t, \ldots, t^{p-1}$ form a basis of F over F^p and $\{t\}$ is a p-basis (a minimal generating set for F over F^p; [4, Ch.V, § 13, n°1, Def. 1]). The Frobenius isomorphism $x \mapsto x^p$ induces $[L^{1/p} : L] = [L : L^p]$ for any field L of characteristic p. Taking $L = F^{1/p^{f-1}}$ and noting $(F^{1/p^{f-1}})^p = F^{1/p^{f-2}}$, induction on f yields $[F^{1/p^f} : F^{1/p^{f-1}}] = p$ and consequently $[F^{1/p^f} : F] = p^f$ and $F^{1/p^f} = F(t^{1/p^f})$.

Let K/F be a finite purely inseparable extension of exponent p^e (the smallest e such that $K^{p^e} \subseteq F$). Then $K \subseteq F^{1/p^e} = F(t^{1/p^e})$. It remains to show that every intermediate field of $F(t^{1/p^e})/F$ is simple. Set $\alpha = t^{1/p^e}$. For $F \subseteq M \subseteq F(\alpha)$, the minimal polynomial of α over M divides $X^{p^e} - t = (X - \alpha)^{p^e}$; hence it equals $(X - \alpha)^{p^r} = X^{p^r} - \alpha^{p^r}$ for some $r \leq e$. Here r is minimal with $\alpha^{p^r} \in M$. Now $\alpha^{p^r} = t^{1/p^{e-r}}$; writing $k = e - r$, we have $t^{1/p^k} \in M$, so $F(t^{1/p^k}) \subseteq M$. Since each step $F(t^{1/p^{i+1}})/F(t^{1/p^i})$ has degree p by the computation above, $[F(\alpha) : F(t^{1/p^k})] = p^{e-k} = p^r$, while $[F(\alpha) : M] = p^r$ by definition of r. Hence $M = F(t^{1/p^k})$, a simple extension. $\square$

This lemma is used in Proposition 4.1 to write the pure inseparable splitting field as $F(\gamma^{1/p^f})$ and deduce $[K : F] = p^f$, thereby controlling the exponent bound.

Proposition 2.6 (Albert cyclicity criterion)**.** *[1, Ch. VII, Theorem 27]: a p-algebra $\mathfrak{A}$ is cyclic if and only if there exists a simple purely inseparable field $\mathfrak{K}$ whose degree over F is at most the degree of $\mathfrak{A}$ and such that $\mathfrak{K}$ splits $\mathfrak{A}$.*

This cyclicity criterion applies to all p-algebras, not merely division algebras. It is used in the exponent-p subcase of Proposition 4.1.

Proposition 2.7 (Albert pure inseparable splitting)**.** *[1, Ch. VII, Theorem 21]: every p-algebra of index p^e over F possesses a pure inseparable splitting field K/F of finite degree, whose exponent over F (i.e., the smallest r such that $K^{p^r} \subseteq F$) is at most p^e.*

This is used in the $\exp(D) = p^2$ subcase of Proposition 4.1 to obtain a pure inseparable splitting field whose degree is bounded by the exponent.

Proposition 2.8 (Albert cyclicity criterion for division algebras)**.** *[1, Ch. VII, Theorem 26]: a division p-algebra $\mathfrak{D}$ of degree p^e is cyclic if and only if $\mathfrak{D}$ is split by a simple purely inseparable extension $F(\gamma^{1/p^e})$ of degree p^e over F.*

This will be applied in the p-rank 1 case (Proposition 4.1) to verify cyclicity when a pure inseparable splitting field is available.

Proposition 2.9 (Albert degree-p cyclicity)**.** *[1, Ch. VII, Theorem 23]: every division algebra of degree p over a field of characteristic p is cyclic; in particular, a field of characteristic p containing a non-trivial p-algebra possesses a cyclic Galois extension of degree p.*

This is used in Proposition 5.1 to obtain the cyclic extension inside the degree-p cyclic division algebra C, and in case (C3) of the proof of Theorem 1.1 to conclude that a degree-p division algebra is cyclic.

Definition 2.10 (Similarity)**.** Two central simple F-algebras A_1, A_2 are *similar*, written $A_1 \sim A_2$, if their underlying division algebras are isomorphic [1, Ch.IV, §8]. This is Brauer equivalence: $A_1 \sim A_2$ if and only if $[A_1] = [A_2]$ in $\mathrm{Br}(F)$ [6, Remark 2.4.6, 1.].

Proposition 2.11 (Albert cyclic decomposition). *[1, Ch. VII, Theorem 28] states: let $\mathfrak{A}$ be a p-algebra over F split by a purely inseparable extension $\mathfrak{K} = F(\gamma_1^{1/n_1}, \ldots, \gamma_t^{1/n_t})$ with $n_i = p^{e_i}$. Then*

$$\mathfrak{A} \sim \mathfrak{B}_1 \times \cdots \times \mathfrak{B}_t,$$

where each $\mathfrak{B}_i$ is a cyclic algebra $(\mathfrak{S}_i, S_i, \gamma_i)$ of degree m_i dividing n_i.

Lemma 2.12 (Albert decomposition for degree p^2). *[1, Ch. VII, Theorem 28 and the concluding paragraphs of §7.9]: every p-algebra D of degree p^2 over F is either cyclic (case (C1) below) or similar to a tensor product of two degree-p cyclic p-algebras. In the latter case, the Artin–Schreier parameters of the two factors are either F_p-independent or F_p-dependent. The following trichotomy covers all possibilities (the cases need not be mutually exclusive):*

(C1) D is similar to a cyclic algebra of degree p^2;

(C2) there exist degree-p cyclic p-algebras $A = (\alpha, t)_p$ and $B = (\beta, s)_p$ such that $D \sim A \otimes_F B$ and α, β are F_p-independent in $F/\wp(F)$;

(C3) there exist degree-p cyclic p-algebras $A = (\alpha, t)_p$ and $B = (\beta, s)_p$ such that $D \sim A \otimes_F B$ and α, β are F_p-dependent in $F/\wp(F)$; in this case $\mathrm{ind}(D) \leq p$.

Proof. The classification is Proposition 2.11. For (C3), write $\beta = c\alpha + \wp(\gamma)$ with $c \in \mathbb{F}_p^\times$ and $\gamma \in F$. In $\mathrm{Br}(F)$, the class of a cyclic p-algebra depends only on the first parameter modulo $\wp(F)$ [6, Proposition 4.7.3]; hence $[(\beta, s)_p] = [(\wp(\gamma) + c\alpha, s)_p] = [(c\alpha, s)_p]$. The isomorphism $\mathrm{Br}(F)[p] \cong H^2(F, \mathbb{F}_p)$ endows $\mathrm{Br}(F)[p]$ with the structure of an $\mathbb{F}_p$-vector space in which $c \cdot [(\alpha, t)_p] = [(c\alpha, t)_p] = [(\alpha, t^c)_p]$ for $c \in \mathbb{F}_p^\times$ [6, Proposition 4.7.3]. Consequently $[(\beta, s)_p] = [(\alpha, s^c)_p]$. By bilinearity, $[(\alpha, t)_p] + [(\beta, s)_p] = [(\alpha, t)_p] + [(\alpha, s^c)_p] = [(\alpha, ts^c)_p]$. The latter class is represented by the cyclic algebra $(\alpha, ts^c)_p$ of degree p; thus its index divides p and $\mathrm{ind}(D) \leq p$. □

This lemma provides the case distinction for the proof of the Main Theorem (Section 6).

3 The independent case

We prove that when the Artin–Schreier parameters are F_p-independent, the tensor product is a $C_p \times C_p$-crossed product.

Proposition 3.1. *Let $A = (\alpha, t)_p$ and $B = (\beta, s)_p$ be two degree-p cyclic p-algebras over F. Assume that the classes of α and β are F_p-linearly independent in $F/\wp(F)$. Then the tensor product $A \otimes_F B$ is a $C_p \times C_p$-crossed product.*

Proof. Write $A = (\alpha, t)_p$ and $B = (\beta, s)_p$ with generators u_A, w_A for A and u_B, w_B for B as in Definition 2.1. In $A \otimes_F B$, set $x = u_A \otimes 1$, $y = 1 \otimes u_B$, $z_A = w_A \otimes 1$, $z_B = 1 \otimes w_B$, and $K = F(x, y)$. Then $xy = (u_A \otimes 1)(1 \otimes u_B) = u_A \otimes u_B = (1 \otimes u_B)(u_A \otimes 1) = yx$. The field $K = F(x, y)$ satisfies $\wp(x) = \alpha$ and $\wp(y) = \beta$. By Lemma 2.2 and the F_p-independence hypothesis, the extensions $F(x)$ and $F(y)$ are linearly disjoint over F; their compositum $K = F(x, y)$ is therefore a field with $[K : F] = p^2 = \deg(A \otimes_F B)$. The inclusion $K \hookrightarrow A \otimes_F B$ is a nonzero F-algebra homomorphism from a field, hence injective; consequently K is a maximal étale subalgebra of $A \otimes_F B$ in the sense of Definition 2.3. The Galois group is $\mathrm{Gal}(K/F) \cong C_p \times C_p$, generated by

$$\sigma_A : \begin{cases} x \mapsto x + 1, \\ y \mapsto y, \end{cases} \qquad \sigma_B : \begin{cases} x \mapsto x, \\ y \mapsto y + 1. \end{cases}$$

From $w_A^p = t$ and $w_B^p = s$ we have $z_A^p = t$, $z_B^p = s$. Moreover, $z_A z_B = (w_A \otimes 1)(1 \otimes w_B) = w_A \otimes w_B = (1 \otimes w_B)(w_A \otimes 1) = z_B z_A$. By the defining relations of A and B (Definition 2.1) and the tensor product structure, their conjugation action on K is

$$z_A x z_A^{-1} = x + 1, \quad z_A y z_A^{-1} = y, \qquad z_B x z_B^{-1} = x, \quad z_B y z_B^{-1} = y + 1,$$

and $z_A f z_A^{-1} = z_B f z_B^{-1} = f$ for all $f \in F$ (since w_A, w_B centralize F).

Basis verification. The algebra A has F-basis $\{u_A^a w_A^i : 0 \le a, i < p\}$, and similarly for B. Their tensor product D has basis $\{u_A^a w_A^i \otimes u_B^b w_B^j : 0 \le a, b, i, j < p\}$. Using the commutation relation $w_A u_A = (u_A + 1) w_A$ (and its iteration $w_A^i u_A^a = (u_A + i)^a w_A^i$), every basis element can be rewritten as

$$u_A^a w_A^i \otimes u_B^b w_B^j = (u_A^a \otimes u_B^b)(w_A^i \otimes 1)(1 \otimes w_B^j) = k \cdot z_A^i z_B^j$$

with $k = u_A^a \otimes u_B^b \in K$. Hence the $p^2 \cdot p^2 = p^4$ elements $\{k z_A^i z_B^j : k \in F\text{-basis of } K, 0 \le i, j < p\}$ span D. A dimension count ($\dim_F D = p^4$, $\dim_F K = p^2$, p^2 choices for (i, j)) shows they are linearly independent, hence an F-basis. The multiplication rules $z_A k = \sigma_A(k) z_A$, $z_B k = \sigma_B(k) z_B$ for $k \in K$, together with $z_A^p = t$, $z_B^p = s$, $z_A z_B = z_B z_A$, follow directly from the defining relations of A and B.

These relations show that $A \otimes_F B$ is a $C_p \times C_p$-crossed product (Definition 2.3). □

Remark 3.2. Even when $\mathrm{ind}(A \otimes_F B) < p^2$ (e.g. when $A \cong B^{-1}$ in $\mathrm{Br}(F)$), the tensor product $A \otimes_F B$ itself, as constructed in Proposition 3.1, is already a $C_p \times C_p$ crossed product; the fact that it is a matrix algebra over a cyclic division algebra does not affect the crossed product structure exhibited in the proof. Thus the crossed product conclusion of Proposition 3.1 holds unconditionally, regardless of the index.

4 The p-rank 1 case

When $[F : F^p] = p$ (i.e., p-rank 1), the uniqueness of the degree-p purely inseparable extension provides a direct path to cyclicity, which handles all exponent-p and exponent-p^2 algebras uniformly.

Proposition 4.1. *Let F be a field of characteristic p with $[F : F^p] = p$. Then every p-algebra of degree p^2 over F is a crossed product.*

Proof. Let D be a p-algebra of degree p^2 over F (not necessarily a division algebra). Since $\exp(D) \mid \deg(D) = p^2$, $\exp(D) \in \{1, p, p^2\}$. We treat the three cases separately.

If $\exp(D) = 1$, then $D \cong M_{p^2}(F)$ is trivially a crossed product.

If $\exp(D) = p$, then by Lemma 2.4 the algebra D is split by a finite height-1 extension K/F. A height-1 extension satisfies $K^p \subseteq F$, hence $K \subseteq F^{1/p}$. By Lemma 2.5, $F^{1/p} = F(t^{1/p})$ (where t is a p-basis element) and $[F^{1/p} : F] = p$. Hence K is a subfield of $F^{1/p}$, so $[K : F] \mid p$. Since D is not split over F, $[K : F] \neq 1$; thus $[K : F] = p$ and $K = F^{1/p}$, a simple purely inseparable extension of degree $p \leq p^2 = \deg(D)$. Applying Proposition 2.6 to D with splitting field $F^{1/p}$, we conclude that D is cyclic, hence a C_{p^2}-crossed product.

If $\exp(D) = p^2$, then D is a division algebra (since $\exp(D) \mid \mathrm{ind}(D) \mid \deg(D)$, [6, Theorem 2.8.7, 1.]). By Proposition 2.7, the algebra D has a pure inseparable splitting field K/F. By Lemma 2.5, $K = F(\gamma^{1/p^f})$ for some $\gamma \in F$ and $f \geq 0$, and $[K : F] = p^f$. The exponent bound from Proposition 2.7 yields $f \leq 2$. We first exclude $f \leq 1$. If $f \leq 1$, then $[K : F] \leq p$. The restriction-corestriction formula $\mathrm{cor}_{K/F} \circ \mathrm{res}_{K/F} = [K : F] \cdot \mathrm{id}$ on $\mathrm{Br}(F)$ [6, Proposition 4.2.12] gives $[K : F] \cdot [D] = 0$ in $\mathrm{Br}(F)$; hence $\exp(D) \mid [K : F] \leq p$, contradicting $\exp(D) = p^2$. Hence $f = 2$. By Proposition 2.8, the algebra D is cyclic, hence a C_{p^2}-crossed product (Definition 2.3). $\square$

5 The dependent and p-rank ≥ 2 case

When the Artin–Schreier generators are $\mathbb{F}_p$-dependent, the Brauer class reduces to a cyclic algebra of degree at most p. The degree-p^2 algebra is then a matrix algebra over that cyclic algebra. The p-rank 1 subcase was settled above (Section 4); this section treats the remaining case p-rank ≥ 2.

Proposition 5.1. *Let F be a field of characteristic p with $[F : F^p] \geq p^2$. Let C be a cyclic division algebra of degree p over F. Then $M_p(C)$ is a $C_p \times C_p$-crossed product.*

Proof. By Proposition 2.9, applied to C, there exist $\alpha \in F \setminus \wp(F)$ and $c \in F^\times$ such that $C \cong (\alpha, c)_p$. Set $L = F(\wp^{-1}(\alpha))$; then L/F is a cyclic Galois extension of degree p.

The Artin–Schreier isomorphism $F/\wp(F) \cong \mathrm{Hom}_{\mathrm{cont}}(\mathrm{Gal}(F^{\mathrm{sep}}/F), \mathbb{F}_p)$ [4, Ch.V, § 11, n°9, Th. 5] yields $\dim_{\mathbb{F}_p} F/\wp(F) \geq 2$ (since $[F : F^p] \geq p^2$). Since $\bar{\alpha} \neq 0$ in $F/\wp(F)$, there exists $\beta \in F$ such that $\bar{\beta}$ is F_p-linearly independent from $\bar{\alpha}$. Define $M = F(\wp^{-1}(\beta))$.

By Lemma 2.2, the extensions L/F and M/F are linearly disjoint over F; hence their compositum $L \otimes_F M$ is a field of degree p^2 over F, Galois with group $C_p \times C_p$.

The regular representation of M (using $[M : F] = p$) embeds M as a maximal commutative subalgebra of $M_p(F)$ [1, Ch. IX, § 5]. Since C contains L by construction (Definition 2.1), we have inclusions $L \subseteq C$ and $M \subseteq M_p(F)$. Their tensor product yields an F-algebra homomorphism

$$\iota : L \otimes_F M \longrightarrow C \otimes_F M_p(F) \cong M_p(C),$$

where the isomorphism $C \otimes_F M_p(F) \cong M_p(C)$ is the standard base-change property of matrix algebras [1, Ch. IV, § 8]. By Lemma 2.2, $L \cap M = F$ and the extensions are linearly disjoint; hence $L \otimes_F M$ is a field (the compositum). The map ι is a nonzero homomorphism from a field to a ring, therefore injective. Moreover, $[L \otimes_F M : F] = p^2 = \deg(M_p(C))$, so its image is a maximal étale subalgebra, Galois with group $C_p \times C_p$ by the linear disjointness argument above. By Definition 2.3, $M_p(C)$ is a $C_p \times C_p$-crossed product. $\square$

6 Proof of the Main Theorem

Proof of Theorem 1.1. Let D be a p-algebra of degree p^2 over F (not necessarily a division algebra). By Lemma 2.12, D satisfies at least one of the cases (C1), (C2), (C3); if it satisfies more than one, resolving any single case suffices.

Case (C1): D is similar to a cyclic algebra C of degree p^2. Since D and C have the same degree p^2, similarity implies isomorphism [6, Remark 2.4.6, 2.]. A cyclic algebra is a crossed product (Definition 2.3).

Case (C2): there exist degree-p cyclic p-algebras $A = (\alpha, t)_p$ and $B = (\beta, s)_p$ such that $D \sim A \otimes_F B$ and α, β are F_p-independent in $F/\wp(F)$. By Proposition 3.1, the tensor product $A \otimes_F B$ is a $C_p \times C_p$ crossed product. If $\mathrm{ind}(A \otimes_F B) = p^2$, then $D \cong A \otimes_F B$ and we are done. If $\mathrm{ind}(A \otimes_F B) < p^2$, then $\mathrm{ind}(D) = \mathrm{ind}(A \otimes_F B)$ (similarity preserves the underlying division algebra, Definition 2.10). Since $\mathrm{ind}(D) \mid \deg(D) = p^2$ and $\mathrm{ind}(D) < p^2$, we have $\mathrm{ind}(D) \leq p$; thus the argument of case (C3) below applies.

Case (C3): there exist degree-p cyclic p-algebras $A = (\alpha, t)_p$ and $B = (\beta, s)_p$ such that $D \sim A \otimes_F B$ and α, β are F_p-dependent in $F/\wp(F)$; hence $\mathrm{ind}(D) \leq p$. Then $D \cong M_{p^2/d}(C)$ where C is a degree-d division algebra with $d = \mathrm{ind}(D) \leq p$.

- If $d = 1$, then $D \cong M_{p^2}(F)$, trivially a crossed product.
- If $d = p$, then C is cyclic by Proposition 2.9.
  - If $[F : F^p] = p$, then Proposition 4.1 shows that every degree-p^2 p-algebra over F is a crossed product; hence D is a crossed product.
  - If $[F : F^p] \geq p^2$, then Proposition 5.1 shows that $D \cong M_p(C)$ is a $C_p \times C_p$-crossed product.

Lemma 2.12 guarantees that every degree-p^2 p-algebra satisfies (C1), (C2), or (C3). All cases yield a crossed product (Definition 2.3). □

Example 6.1 (Independent generators)**.** Take $A = (x, y)_p$ and $B = (x + 1, y + 1)_p$ over $F = \mathbb{F}_p(x, y)$. The classes $\bar{x}$ and $\overline{x + 1}$ are F_p-independent in $F/\wp(F)$ because $1 \notin \wp(F)$ (an Artin–Schreier equation $t^p - t = 1$ has no solution in F by degree considerations). The tensor product $A \otimes_F B$ is a $C_p \times C_p$ crossed product with maximal subfield $K = F(\wp^{-1}(x), \wp^{-1}(x+1))$ of degree p^2. This illustrates case (C2) of Theorem 1.1: the algebra $A \otimes_F B$ has independent Artin–Schreier parameters and is a degree-p^2 p-algebra, hence a crossed product.

Example 6.2 (Dependent generators)**.** Take $A = (x, y)_p$ and $B = (x, y+1)_p$ over $F = \mathbb{F}_p(x, y)$. The left slots coincide: both are x. By bilinearity, $[A] + [B] = [(x, y(y + 1))_p]$, so $\mathrm{ind}(A \otimes_F B) \leq p$. The underlying division algebra is cyclic of degree p, and $A \otimes_F B$ is a matrix algebra over it. This illustrates case (C3) of Theorem 1.1: the algebra $A \otimes_F B$ has dependent Artin–Schreier parameters and index $\leq p$, hence is a matrix algebra over a cyclic division algebra and a crossed product.

References

[1] A. Adrian Albert. *Structure of algebras*, volume 24 of *Colloq. Publ., Am. Math. Soc.* American Mathematical Society (AMS), Providence, RI, 1939. 2, 3, 5, 6, 9

[2] S. A. Amitsur and D. Saltman. Generic Abelian crossed products and p-algebras. *J. Algebra*, 51:76–87, 1978. 2

[3] A. Auel, E. Brussel, S. Garibaldi, and U. Vishne. Open problems on central simple algebras. *Transform. Groups*, 16(1):219–264, 2011. 2, 4

[4] Nicolas Bourbaki. *Éléments de mathématique. Algèbre. Chapitres 4 à 7.* Berlin: Springer, reprint of the 1981 original edition, 2007. 4, 9

[5] Eric Brussel and Eduardo Tengan. Formal constructions in the Brauer group of the function field of a p-adic curve. *Trans. Am. Math. Soc.*, 367(5):3299–3321, 2015. 2

[6] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Camb. Stud. Adv. Math.* Cambridge: Cambridge University Press, 2nd revised and updated edition edition, 2017. 4, 5, 6, 8, 9

[7] Bill Jacob and Adrian R. Wadsworth. A new construction of noncrossed product algebras. *Trans. Am. Math. Soc.*, 293:693–721, 1986. 2

[8] Serge Lang. *Algebra.*, volume 211 of *Grad. Texts Math.* New York, NY: Springer, 3rd revised ed. edition, 2002. 4

[9] Kelly McKinnie. Prime to p extensions of the generic Abelian crossed product. *J. Algebra*, 317(2):813–832, 2007. 2

[10] Louis H. Rowen and David J. Saltman. Prime to p extensions of division algebras. *Isr. J. Math.*, 78(2-3):197–207, 1992. 2

[11] David J. Saltman. Noncrossed product p-algebras and Galois p-extensions. *J. Algebra*, 52:302–314, 1978. 2