TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 293, Number 2, February 1986

A NEW CONSTRUCTION OF NONCROSSED PRODUCT ALGEBRAS

BY

BILL JACOB[1] AND ADRIAN R. WADSWORTH[2]

ABSTRACT. New examples of noncrossed product division algebras are obtained, using methods different from all previous noncrossed product constructions. The examples are division algebras over intersections of p-Henselian valued fields, and they have Schur index p^m and exponent p^n for any prime number p and any integers $m \geq n \geq 2$ ($n \geq 3$ if $p = 2$). The basic tools used in the construction are valuation theory and Galois cohomology; no generic methods are applied and there is no p.i. theory. Along the way, local-global principles are proved for central simple algebras over intersections of p-Henselian valued fields.

The first examples of central simple division algebras which are not crossed products were obtained by Amitsur in [**Am**] in 1972. Amitsur thereby settled a question that had been one of the outstanding open problems in the theory of algebras for at least thirty years. His examples were the generic division algebras $UD(\mathbf{Q}, n)$ of index n over $\mathbf{Q}$ (the rational numbers) for any natural number n such that $p^2|n$, p an odd prime, or $8|n$. All subsequent constructions of noncrossed products in [**SS**, $\mathbf{Sa_1}$–$\mathbf{Sa_3}$, **Ri**, **Ro**, and **Ti**] have heretofore been based on Amitsur's specialization argument, and they are all generic division algebras or extensions of generic division algebras. The centers of these noncrossed product algebras are not known, nor are the Brauer groups, nor the absolute Galois groups of the centers.

We present here a new method of constructing noncrossed product algebras. In our approach, the noncrossed product is realized as the underlying division algebra D of a tensor product of suitably chosen cyclic algebras over a field $F = L_1 \cap L_2$, where each L_i is a pth root Henselian valued field. We prove local global principles relating the splitting fields of D to those of $D \otimes_F L_i$, $i = 1, 2$. It is shown that the p-part of the Brauer group of F is completely determined by that of L_1 and L_2. Computations for central simple F-algebras thus become very tractable. For example, we not only show that D is not a crossed product, but also calculate exactly how large r must be so that the matrix ring $M_r(D)$ is a crossed product, and how large s must be so that $M_s(D)$ is a tensor product of cyclic algebras. Indeed, the structure of the Brauer group of F is so nice that we were somewhat surprised that noncrossed products could possibly exist over F.

Received by the editors March 19, 1985.

1980 *Mathematics Subject Classification*. Primary 16A39; Secondary 12J10, 12G05.

[1]This collaboration resulted from the first author's visit to U.C.S.D. during 1984-85. He would like to thank the U.C.S.D. Mathematics Department for its hospitality. He was also supported in part by the N.S.F.

[2]Supported in part by the N.S.F.

0002-9947/86 $1.00 + $.25 per page

The paper is organized as follows: In §1 we define terminology and describe the p-Galois cohomology and the pth root Henselian valuations that will be used throughout the paper. We develop in §§2 and 3 the "local" theory of valued division algebras and the p-Brauer group of fields with pth root Henselian valuations. The bridge between the "local" theory for pth root Henselian valued fields L_i and the "global" theory for $L_1 \cap L_2$ is provided in §4: We prove that (under suitable hypotheses) the p-part of the absolute Galois group of $L_1 \cap L_2$ is the free product (in the category of pro-p-groups) of the p-parts of the absolute Galois groups of L_1 and L_2 (Theorem 4.3). Finally in §§5 and 6 we give the noncrossed product examples. At the end of §5 we indicate how the same methods yield examples of indecomposable algebras with index exceeding the exponent.

A number of results given here can be proved either by valuation theory or by cohomological methods. Both perspectives are worthwhile, and we will try to steer a middle course to give a good sampling of each approach.

1. Preliminaries from the theory of algebras, Galois cohomology and valuation theory. All algebras considered in this paper will be finite dimensional over some field F. If A is a central simple F-algebra, $[A]$ denotes the class of A in the Brauer group $\mathrm{Br}(F)$ of F. We write $\exp(A)$ for the exponent of A, which is the order of $[A]$ in $\mathrm{Br}(F)$. By Wedderburn's theorem $A \cong M_n(D)$, i.e., $n \times n$ matrices over some F-central division algebra D. The integer $\sqrt{\dim_F D}$ is the (Schur) index of A, denoted $\mathrm{index}(A)$. We will need the fact (cf. [**R**, Theorems 29.22, 29.24]) that $\exp(A) | \mathrm{index}(A)$ and $\exp(A)$ and $\mathrm{index}(A)$ have the same prime factors. It is standard that every maximal subfield K of D splits A and $[K:F] = \mathrm{index}(A)$. More generally, we recall from [**R**, pp. 238–240, Theorem 28.5, Corollary 28.10]:

(1.1) Let $A \cong M_n(D)$ be a central simple F-algebra (D the associated division algebra). If $L \supseteq F$ is a field with $[L:F] < \infty$ and L splits A, then $[L:F] = s \cdot \mathrm{index}(A)$ for some integer s, and L is isomorphic to a (maximal) subfield of $M_s(D)$. Conversely, if $K \supseteq F$ is any subfield of $M_s(D)$ and $[K:F] = s \cdot \mathrm{index}(A)$, then K splits A.

Recall that a central simple F-algebra A is a crossed product just when A has a (maximal) subfield M Galois over F, with $[M:F]^2 = \dim_F A$. For such an algebra, the multiplication table on a base is completely determined by the multiplication in M, the Galois group $\mathcal{G}(M/F)$ and a 2-cocycle of $\mathcal{G}(M/F)$. It is through crossed products that one obtains the cohomological interpretation of the Brauer group: $\mathrm{Br}(F) \cong H^2(\mathcal{G}(\tilde{F}/F), \tilde{F}^*)$, where $\tilde{F}$ is a separable closure of F (cf. [**CF**, pp. 125–126; **R**, p. 246, Theorem 29.12; or $\mathbf{Se}_2$, Chapter X, §§4–5]). Our strategy for constructing central simple algebras which are not crossed products is to produce an algebra A with $\dim_F A = d^2$ so that A has a splitting field of degree t over F, $t|d$, but A has no splitting field Galois over F with degree dividing t. Then (1.1) shows that $A \cong M_{d/t}(A')$ for some central simple F-algebra A', but A' cannot be a crossed product, nor a matrix algebra over a crossed product.

The algebras A in our example will be built from cyclic algebras, for which we will use the following notation: If K is a Galois extension field of F with $\mathcal{G}(K/F)$ cyclic

of order n with generator σ, and if $b \in F^* = F - \{0\}$, then $A(K/F, \sigma, b)$ denotes the ring generated over K by an element x subject to the relations $xk = \sigma(k)x$ for all $k \in K$, and $x^n = b$. Recall that $A(K/F, \sigma, b)$ is a central simple F-algebra of dimension n^2 over F in which K is a maximal subfield. A very nice account of cyclic algebras is given in [**R**, §30].

Suppose F contains a primitive nth root of unity ω. We write $A_\omega(a, b; F)$ for the "symbol" determined by a and b, i.e., the central simple n^2-dimensional F-algebra with generators i, j and relations $i^n = a$, $j^n = b$, $ij = \omega ji$. Of course, Kummer theory shows that with $\omega \in F$ every cyclic F-algebra of dimension n^2 is a symbol.

Fix a prime number $p \neq \operatorname{char} F$. Let ${}_{p^n}\mathrm{Br}(F)$ denote the subgroup of $\mathrm{Br}(F)$ consisting of those $[A]$ with $\exp(A) | p^n$, and let $\mathrm{Br}_p(F) = \bigcup_{n=1}^{\infty} {}_{p^n}\mathrm{Br}(F)$, the p-primary component of $\mathrm{Br}(F)$. Our noncrossed product examples will all have exponent (hence index) a p-power. One reason for this is that key cohomological results in §4 hold for pro-p-groups, but are not known for arbitrary profinite groups. It is easy to work from our examples to construct noncrossed products of composite exponent; we will not do so, preferring to focus attention on the more basic ideas involved in the construction.

For any profinite group G and discrete G-module M, $H^i(G, M)$ denotes the ith continuous cohomology group of G with coefficients in M (as described e.g., in [**CF**, Chapter V; **Sh**, Chapter II; $\mathbf{Se}_1$, Chapter I; **T**, §2]). In particular, if N is any closed subgroup of G, $\mathrm{res}_{G \to N}$: $H^i(G, M) \to H^i(N, M)$ denotes the restriction map; if N is normal in G, then $\inf_{G/N \to G}$: $H^i(G/N, M^N) \to H^i(G, M)$ is the inflation map.

Given a field F with $\operatorname{char} F \neq p$, let μ_{p^n} denote the group of all p^nth roots of unity in $\tilde{F}$, a separable closure of F. Then μ_{p^n} is a discrete module for the profinite group $G(F) := \mathcal{G}(\tilde{F}/F)$, and we recall the standard isomorphisms

$$(1.2) \qquad H^1\big(G(F), \mu_{p^n}\big) \cong F^*/F^{*p^n} \quad \text{and} \quad H^2\big(G(F), \mu_{p^n}\big) \cong {}_{p^n}\mathrm{Br}(F),$$

which are derived the same way as (1.7) below, but with $\tilde{F}$ replacing $\tilde{F}_p$. For $a \in F^*$ we write (a) (or $(a)_F$) for the image of aF^{*p^n} in $H^1(G(F), \mu_{p^n})$.

Suppose now that $\mu_{p^n} \subseteq F$. Then we have the $G(F)$-module isomorphism $\mu_{p^n} \cong \mathbf{Z}/p^n\mathbf{Z}$ (where $\mathbf{Z}/p^n\mathbf{Z}$ is always viewed as a trivial $G(F)$-module). This isomorphism is not canonical, since it depends on the choice of a generator of μ_{p^n}. From the isomorphism $\mathbf{Z}/p^n\mathbf{Z} \otimes \mathbf{Z}/p^n\mathbf{Z} \cong \mathbf{Z}/p^n\mathbf{Z}$ given by ring multiplication, we obtain a noncanonical $G(F)$-module mapping $\mu_{p^n} \otimes \mu_{p^n} \to \mu_{p^n}$ which induces the cup-product pairing

$$\cup : H^1\big(G(F), \mu_{p^n}\big) \times H^1\big(G(F), \mu_{p^n}\big) \to H^2\big(G(F), \mu_{p^n}\big).$$

Recall (cf. [**T**, (4.2), p. 266]) that under the second isomorphism in (1.2) $(a) \cup (b) \in H^2(G(F), \mu_{p^n})$ corresponds to the Brauer class of the symbol $A_\omega(a, b; F)$, where ω is the generator of μ_{p^n} mapped to 1 in $\mathbf{Z}/p^n\mathbf{Z}$. We will need to use the powerful theorem of Merkurjev and Suslin [**MS**, Theorem 11.5]:

THEOREM 1.3 (MERKURJEV - SUSLIN). *Let F be an field with $\mu_{p^n} \subseteq F$ (so $\operatorname{char} F \neq p$). Then there is a short exact sequence*

$$0 \to S \to H^1\big(G(F), \mu_{p^n}\big) \otimes H^1\big(G(F), \mu_{p^n}\big) \to H^2\big(G(F), \mu_{p^n}\big) \to 0,$$

where S is the Steinberg relation group of F, i.e., the subgroup of $\otimes_{i=1}^{2} H^1(G(F), \mu_{p^n})$ *generated by* $\{(a) \otimes (1-a) | a \in F^*, a \neq 1\}$.

In this exact sequence the map into $H^2(G(F), \mu_{p^n})$ is the cup product. Of course, the surjectivity of this map says that ${}_{p^n}\mathrm{Br}(F)$ is generated by cyclic algebras whenever $\mu_{p^n} \subseteq F$.

Because of the need to work with pro-p-groups, we will use a p-version of Galois cohomology, which we now describe. For any field F with $\mathrm{char} F \neq p$, let $F(p)$ denote the *p-closure* of F, which is the compositum in $\tilde{F}$ of all the Galois extensions K of F with $[K:F]$ a power of p. Then $\mathcal{G}(F(p)/F)$ is a pro-p-group. Since every maximal proper subgroup of a finite p-group is normal of index p, we have,

(1.4) If $F \subseteq L \subseteq F(p)$ and $[L:F] < \infty$, then there is a chain of fields $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_m = L$, such that $[K_i : K_{i-1}] = p$ and K_i is Galois over K_{i-1} for $i = 1, 2, \ldots, m$.

In §6 we will work with fields F with $\mu_p \not\subseteq F$. When this occurs it is desirable to work with a somewhat larger extension than $F(p)$, but one which agrees with $F(p)$ when $\mu_p \subseteq F$. We define the *pth root closure* of F, denoted $\tilde{F}_p$, to be $F(\mu_p)(p)$. From Kummer theory we see

$$\tilde{F}_p = \bigcup_{i=1}^{\infty} K_i, \quad \text{where } K_0 = F \text{ and } K_{i+1} = K_i\big(\{c^{1/p} | c \in K_i\}\big). \tag{1.5}$$

Clearly $\tilde{F}_p$ is Galois over F and $\mathcal{G}(\tilde{F}_p/F)$ is pro-solvable, though not a pro-p-group when $\mu_p \not\subseteq F$. Since $\tilde{F}_p^p = \tilde{F}_p$ and $\mu_{p^n} \subseteq \tilde{F}_p$, the Merkurjev-Suslin theorem shows that $\mathrm{Br}(\tilde{F}_p)$ has no p-primary torsion. By contrast, it is unknown whether $\mathrm{Br}_p(F(p)) = (0)$ when $\mu_p \not\subseteq F$.

We will use the notation $G_p(F)$ for $\mathcal{G}(\tilde{F}_p/F)$. For any discrete $G_p(F)$-module M, we write $H_p^i(F, M)$ for $H^i(G_p(F), M)$; we call $H_p^*(F, -)$ the *p-Galois cohomology* of F. When $p = 2$ this coincides with the quadratic cohomology $H_q^*(F, -)$ considered in [**AEJ**]. (For whenever $\mathrm{char} F \neq 2$, $\mu_2 \subseteq F$, so $\tilde{F}_2 = F(2)$ which is the quadratic closure of F.)

Now, $\tilde{F}_p^*$ is a discrete $G_p(F)$-module and we recall [**CF**, pp. 124–126] that $H_p^0(F, \tilde{F}_p^*) \cong F^*$, $H_p^1(F, \tilde{F}_p^*) = 0$ (the homological Hilbert Theorem 90), and $H_p^2(F, \tilde{F}_p^*) \cong \mathrm{Br}(\tilde{F}_p/F) := \ker(\mathrm{Br}(F) \to \mathrm{Br}(\tilde{F}_p))$. Following the same route that led to formulas (1.2), we consider the short exact sequence of $G_p(F)$-modules

$$1 \to \mu_{p^n} \to \tilde{F}_p^* \xrightarrow{p^n} \tilde{F}_p^* \to 1, \tag{1.6}$$

where the right-hand map is $a \mapsto a^{p^n}$. In view of the description just given of $H_p^i(F, \tilde{F}_p^*)$, the long exact sequence in cohomology obtained from (1.6) begins

$$0 \to \mu_{p^n} \to F^* \xrightarrow{p^n} F^* \to H^1\big(F, \mu_{p^n}\big) \to 0$$

$$\to 0 \to H^2\big(F, \mu_{p^n}\big) \to \mathrm{Br}\big(\tilde{F}_p/F\big) \xrightarrow{p^n} \mathrm{Br}\big(\tilde{F}_p/F\big) \to \cdots.$$

Thus, we find,

$$H_p^1\big(F, \mu_{p^n}\big) \cong F^*/F^{*p^n} \quad \text{and} \quad H_p^2\big(F, \mu_{p^n}\big) \cong {}_{p^n}\mathrm{Br}(F). \tag{1.7}$$

The second isomorphism in (1.7) uses the nontrivial fact noted above that $\mathrm{Br}_p(\tilde{F}_p) = 0$, which implies that ${}_{p^n}\mathrm{Br}(F) \subseteq \mathrm{Br}(\tilde{F}_p/F)$. By comparing (1.7) with (1.2) we see that the canonical inflation map $H_p^i(F, \mu_{p^n}) \to H^i(G(F), \mu_{p^n})$ must be an isomorphism, $i = 1, 2$. Consequently, the Merkurjev-Suslin Theorem 1.3 remains valid when we replace $H^i(G(F), \mu_{p^n})$ by $H_p^i(F, \mu_{p^n})$, $i = 1, 2$.

We conclude this section with some valuation theory, in particular valuation theory relative to the field extension $\tilde{F}_p/F$. Let G be an ordered abelian group, written additively, and let $v\colon F^* \to G$ be a Krull valuation on the field F. We will use the following notation: Γ_F for the value group of v; V_F for the valuation ring of v; M_F for the unique maximal ideal of V_F; U_F for the group of units of V_F; and $\bar{F}$ for the residue field V_F/M_F of V_F. For $a \in V_F$, we write $\bar{a}$ for the image of a in $\bar{F}$. Usually we will be considering only one valuation at a time on a given field F, but when there is more than one we avoid ambiguity by writing $\Gamma_{F,v}, \ldots, U_{F,v}, \bar{F}_v$. Good references for valuation theory are [**E** and **Bo$_2$**].

If v is a valuation on F, we say that v is *pth root Henselian* if $\mathrm{char}\,\bar{F} \neq p$ and v has a unique extension to $\tilde{F}_p$. (This is an example of the Ω-Henselian valuations considered in [**Br**], with $\Omega = \tilde{F}_p$. From Bröcker's observations we have that v is pth root Henselian just when $\mathrm{char}\,\bar{F} \neq p$ and Hensel's lemma applies to all monic polynomials $f \in V_F[X]$ which split in $\tilde{F}_p$. See [**Br**, (1.2)].) When $\mu_p \subseteq F$ and $\mathrm{char}\,\bar{F} \neq p$, a pth root Henselian valuation is the same as a p-Henselian valuation as considered in [$\mathbf{W}_1$, §1], and we then use the terms "p-Henselian" and "pth root Henselian" interchangeably. The following easy lemma was proved in [$\mathbf{W}_1$, (1.2), (1.4)].

LEMMA 1.8. *Let (F, v) be a valued field with $\mu_p \subseteq F$ and $\mathrm{char}\,\bar{F} \neq p$. Then,*
(i) *v is p-Henselian iff $1 + M_F \subseteq F^{*p}$;*
(ii) *if v is p-Henselian, then $U_F/U_F^{p^n} \cong \bar{F}^*/\bar{F}^{*p^n}$; hence*

$$F^*/F^{*p^n} \cong \left(\bar{F}^*/\bar{F}^{*p^n}\right) \oplus \left(\Gamma_F/p^n\Gamma_F\right).$$

For any valued field (F, v) with $\mathrm{char}\,\bar{F} \neq p$ we can construct the *pth root Henselization* of (F, v) by a process analogous to the construction of the usual Henselization, as in [**E**, pp. 131–132]: Let w be any extension of v to $\tilde{F}_p$, and let K be the fixed field of the decomposition group of $(\tilde{F}_p, w)$ over (F, v). The pth root Henselization of (F, v) is defined to be $(K, w|_K)$. It is easy to see that $(K, w|_K)$ is pth root Henselian and is an immediate extension of (F, v). Note that the pth root Henselization is, up to isomorphism, independent of the choice of w.

In analogy with the terminology of algebraic geometry we will call a valued field (F, v) *strictly p-Henselian* if it is pth root Henselian and $\bar{F} = \tilde{\bar{F}}_p$. Let $\hat{\mathbf{Z}}_p = \varprojlim_n \mathbf{Z}/p^n\mathbf{Z}$, the p-adic integers, which is the free abelian pro-p-group of rank 1.

LEMMA 1.9. *Suppose (F, v) is strictly p-Henselian. Then*
(i) *$\mu_{p^n} \subseteq F$ for all n;*
(ii) *$U_F \subseteq F^{*p}$;*
(iii) *$F^*/F^{*p^n} \cong \Gamma_F/p^n\Gamma_F$;*
(iv) *if $\dim_{\mathbf{Z}/p\mathbf{Z}}(\Gamma_F/p\Gamma_F) = m$, then $G_p(F) \cong \oplus_{i=1}^m \hat{\mathbf{Z}}_p$.*

PROOF. Because $\mu_p \subseteq \bar{F}$ and v extends uniquely to $F(\mu_p) \subseteq \tilde{F}_p$ we must have $\mu_p \subseteq F$. The rest of (i)–(iii) follow easily from Lemma 1.8. If $K \supseteq F$ is any finite degree Galois extension of F with $K \subseteq \tilde{F}_p$, then $[K:F] = p^k$, v extends uniquely to K and $\tilde{\bar{F}}_p = \bar{F} \subseteq \bar{K} \subseteq \tilde{\bar{F}}_p = \tilde{\bar{F}}_p$. So, $\bar{K} = \bar{F}$. Since $\operatorname{char} \bar{F} \nmid [K:F]$, the argument of [S, p. 66] shows that K is a Kummer extension of F. Thus, by Kummer theory,

$$\tilde{F}_p = \bigcup_{n=1}^{\infty} F_n, \quad \text{where } F_n = F\left(\left\{ c^{1/p^n} | c \in F^* \right\}\right).$$

Because Γ_F is a torsion-free abelian group, any inverse image of a $\mathbf{Z}/p\mathbf{Z}$-base of $\Gamma_F/p\Gamma_F$ is a base of $\Gamma_F/p^n\Gamma_F$ as a free $\mathbf{Z}/p^n\mathbf{Z}$-module. By Kummer theory and (iii), $\mathcal{G}(F_n/F) \cong F^*/F^{*p^n} \cong (\mathbf{Z}/p^n\mathbf{Z})^m$. Consequently,

$$G_p(F) = \lim_{\leftarrow} \mathcal{G}(F_n/F) \cong (\hat{\mathbf{Z}}_p)^m,$$

as desired. □

For any valued field (F,v) with $\operatorname{char} \bar{F} \neq p$, let w be an extension of v to $\tilde{F}_p$. Let L be the fixed field of the inertia group of $(\tilde{F}_p, w)$ over (F, v). We call $(L, w|_L)$ the *strict p-Henselization* of (F, v). Note $(L, w|_L)$ is strictly p-Henselian and is a maximal unramified extension of (F, v) in $\tilde{F}_p$. The strict p-Henselization is unique up to isomorphism. (Similarly, we obtain a "strict Henselization" of (F, v) by replacing $\tilde{F}_p$ by $\tilde{F}$ in this construction.)

2. Valuation theory of division algebras. In this section we will give a construction for obtaining valued division algebras, and we will show how a valuation on a division algebra can restrict the possible Galois groups over the center of maximal subfields.

Let D be a division algebra and let $D^* = D - \{0\}$. A valuation v on D is a function $v\colon D^* \to \Gamma$ (where Γ is a totally ordered group), such that for all a, $b \in D^*$,

(i) $v(ab) = v(a) + v(b)$;

(ii) $v(a + b) \geq \min(v(a), v(b))$ if $b \neq -a$.

We use the same notation as with fields for the objects associated to v: the value group of v is $\Gamma_D = v(D^*)$; the valuation ring of D is $V_D = \{a \in D^* | v(a) \geq 0\} \cup \{0\}$; the unique maximal left ideal and unique maximal right ideal of V_D is $M_D = \{a \in D^* | v(a) > 0\} \cup \{0\}$; the residue division ring is $\bar{D} = V_D/M_D$; and the group of units of V_D is $U_D = V_D - M_D$. We will consider only division algebras finite dimensional over their centers; for such a D, with center F, Γ_F is central in Γ_D and Γ_D/Γ_F is torsion. Hence Γ_D must be abelian, justifying our additive notation for it. The standard reference for valued division algebras is Schilling's book [S].

Let E be a subdivision algebra of the valued division algebra (D, v), and suppose $[D:E] < \infty$, where $[D:E]$ denotes the dimension of D as a right E vector space. Then the restriction $v|_E$ of v to E^* is a valuation on E. Recall [S, p. 21] that the following version of the "fundamental inequality" holds for the extension v over $v|_E$:

$$[\bar{D}:\bar{E}] \cdot |\Gamma_D : \Gamma_E| \leq [D:E]. \tag{2.1}$$

We say that v is *totally ramified* over $v|_E$ if $|\Gamma_D:\Gamma_E| = [D:E]$. Then, of course, $\overline{D} = \overline{E}$.

The next proposition and its corollaries provide the link between Galois groups and value groups of division algebras. The proposition is well known (cf. [**E**, (20.11) (d), (20.18); **S**, p. 66, p. 86, Remark 1]), but we sketch a proof since it is vital for our examples.

PROPOSITION 2.2. *Let $F \subseteq K$ be fields with $[K:F] < \infty$ and K Galois over F. Suppose K has a valuation v which is totally ramified over $v|_F$, and suppose* $\operatorname{char}\overline{K} \nmid [K:F]$. *Then $\mathcal{G}(K/F) \cong \Gamma_K/\Gamma_F$, and $\overline{F}$ contains a primitive lth root of unity, where l is the exponent of the abelian group Γ_K/Γ_F.*

SKETCH OF THE PROOF. Since $\overline{\sigma(u)} = \bar{u}$ for $u \in U_K$, the function $\mathcal{G}(K/F) \times K^* \to \overline{K}^* = \overline{F}^*$ given by $(\sigma, a) \mapsto \overline{\sigma(a)/a}$ induces a bimultiplicative pairing γ: $\mathcal{G}(K/F) \times \Gamma_K/\Gamma_F \to \overline{F}^*$. The proposition follows easily once it is known that γ is nondegenerate. Assume first that $(F, v|_F)$ is Henselian with separably closed residue field. Then K is a Kummer extension of F by [**S**, p. 64, Theorem 3], and the nondegeneracy of γ follows from the nondegeneracy of the Kummer pairing. Dropping the restrictions on F, let L be a maximal unramified extension of $(F, v|_F)$ in $\tilde{F}$. Then L is Henselian with separably closed residue field, and L and K are linearly disjoint over F as K/F is totally ramified. Since $\mathcal{G}(K \cdot L/L) \cong \mathcal{G}(K/F)$ and $\Gamma_{K\cdot L} = \Gamma_K$, $\Gamma_L = \Gamma_F$, the pairing γ for K over F coincides with the corresponding pairing of $K \cdot L$ over L, which we have seen to be nondegenerate.

COROLLARY 2.3. *Let D be a division algebra finite dimensional over a field F. Suppose D has a valuation v totally ramified over $v|_F$, and suppose* $\operatorname{char}\overline{F} \nmid [D:F]$. *If $K \supseteq F$ is any subfield of D which is Galois over F, then $\mathcal{G}(K/F)$ is isomorphic to a subgroup of Γ_D/Γ_F.*

PROOF. By the fundamental inequality (2.1) and the transitivity formula for ramification index, $v|_K$ must be totally ramified over $v|_F$. Hence, by the proposition, $\mathcal{G}(K/F) \cong \Gamma_K/\Gamma_F \subseteq \Gamma_D/\Gamma_F$. □

COROLLARY 2.4. *Let (F, v) be a valued field with* $\operatorname{char}\overline{F} \neq p$ *and $\mu_p \not\subseteq \overline{F}$ for some prime p. Suppose K is a Galois extension field of F with $[K: F] = p^n$, and suppose v has a unique extension to a valuation w of K. Then K is an inertial extension of F (i.e., $[\overline{K}:\overline{F}] = [K:F]$) and $\mathcal{G}(K/F) \cong \mathcal{G}(\overline{K}/\overline{F})$.*

PROOF. Let L be the inertia field of w over F. Then as v is indecomposed in K and $\overline{K}$ is separable over $\overline{F}$ (since $\operatorname{char}\overline{F} \nmid [K:F]$ and $[\overline{K}:\overline{F}]|[K:F]$) we have L/F is inertial and Galois, $\overline{L} = \overline{K}$, $\overline{L}/\overline{F}$ is Galois, and $\mathcal{G}(\overline{L}/\overline{F}) \cong \mathcal{G}(L/F)$ (cf. [**E**, §19]). So, it suffices to see that $K = L$. Because $\overline{L} = \overline{K}$ and $w|_L$ extends uniquely to K and $\operatorname{char}\overline{L} \nmid [K:L]$, (K, w) must be totally ramified over $(L, w|_L)$. Since $[K:L]$ is a p-power, if $K \neq L$ then Proposition 2.2 implies $\mu_p \subseteq \overline{L}$. However, $[\overline{L}:\overline{F}] = [L:F]$ is a p-power, so $\mu_p \not\subseteq \overline{L}$, as $\mu_p \not\subseteq \overline{F}$. Hence, $K = L$, as desired. □

The next theorem gives the criterion we will use for the existence of a valuation on an algebra. The somewhat cumbersome hypotheses cover the examples both in §5 and in §6. Similar theorems will appear in [$\mathbf{W}_2$].

THEOREM 2.5. *Let A be an algebra finite dimensional over a field, and let $L \subseteq A$ be a field. Let v be a valuation on L, and let Δ be the divisible hull of Γ_L (so $\Delta \cong \Gamma_L \otimes_{\mathbf{Z}} \mathbf{Q}$). Suppose there are elements $a_1, \ldots, a_m$ of the group of units A^* of A satisfying*

(i) *$\{a_1, \ldots, a_m\}$ is a base of A as a right L-vector space;*

(ii) *for each $l \in L^*$ and each a_i, $a_i l a_i^{-1} \in L$ and $v(a_i l a_i^{-1}) = v(l)$;*

(iii) *$a_i a_j a_i^{-1} a_j^{-1} \in U_L$ (the group of units of v) for all i, j;*

(iv) *$\mathscr{A} := \{a_1 L^*, \ldots, a_m L^*\}$ is an abelian subgroup of $N_{A^*}(L^*)/L^*$, where $N_{A^*}(L^*)$ is the normalizer of L^* in A^*.*

Then there is a well-defined group homomorphism $\bar{w}\colon \mathscr{A} \to \Delta/\Gamma_L$ given by $a_i L^* \mapsto \frac{1}{m} v(a_i^m) + \Gamma_L$. Suppose $\bar{w}$ is injective. Then v extends to a valuation w on A; hence A is a division ring. Γ_A is the subgroup of Δ such that $\Gamma_A/\Gamma_L = \bar{w}(\mathscr{A})$. Furthermore, (A, w) is totally ramified over (L, v), and $\bar{A} = \bar{L}$.

PROOF. Condition (iv) shows that $a_i^m \in L^*$ for each i. Hence, the function $\bar{w}$ is well defined. For any a_i and any $c \in L^*$ we have the general identity

$$(a_i c)^m = c^{a_i} c^{a_i^2} \cdots c^{a_i^m} a_i^m,$$

where c^{a_i} means $a_i c a_i^{-1}$. Hence, by (ii),

$$v\big((a_i c)^m\big) = m v(c) + v(a_i^m). \tag{1}$$

Let T be the subgroup of A^* generated by $\{a_1, \ldots, a_m\}$, and T' its commutator subgroup. By (ii), TU_L is a group in which U_L is a normal subgroup. By (iii), TU_L/U_L is abelian, so $T' \subseteq U_L$. Since for any i, j, $(a_i a_j)^m = a_i^m a_j^m t$ with $t \in T' \subseteq U_L$, we have

$$v\big((a_i a_j)^m\big) = v(a_i^m) + v(a_j^m). \tag{2}$$

From (1) and (2) it follows that $\bar{w}$ is a group homomorphism.

Because Δ is torsion-free and Δ/Γ_L is torsion, the ordering on Γ_L has a unique extension to Δ which makes Δ a totally ordered abelian group. This is the ordering on Δ we use.

Now suppose $\bar{w}$ is injective. Define a function $w\colon A - \{0\} \to \Delta$ as follows: For any a_i and any $c \in L^*$, set

$$w(a_i c) = \frac{1}{m} v(a_i^m) + v(c).$$

Now, for any $\alpha \in A - \{0\}$, α has a unique representation $\alpha = \sum_{i=1}^m a_i c_i$ with the $c_i \in L$, some $c_i \neq 0$; define $w(\alpha) = \inf\{w(a_i c_i) | c_i \neq 0\}$. Since $\bar{w}$ is injective, $w(a_i c_i) \neq w(a_j c_j)$ for $i \neq j$. Thus, there is a unique summand $a_j c_j$ of α with $w(a_j c_j) = w(\alpha)$; we call $a_j c_j$ the *leading term* of α. Take any $\beta = \sum a_i d_i \in A - \{0\}$ ($d_i \in L$) with $\beta \neq -\alpha$. Let $a_k(c_k + d_k)$ be the leading term of $\alpha + \beta$. We have, if $c_k \neq 0$, $d_k \neq 0$,

$$\begin{aligned} w(a_k(c_k + d_k)) &= \frac{1}{m} v(a_k^m) + v(c_k + d_k) \\ &\geqslant \inf\left(\frac{1}{m} v(a_k^m) + v(c_k), \frac{1}{m} v(a_k^m) + v(d_k)\right) \\ &= \inf(w(a_k c_k), w(a_k d_k)) \geqslant \inf(w(\alpha), w(\beta)). \end{aligned}$$

Hence, $w(\alpha+\beta)=w(a_k(c_k+d_k))\geqslant \inf(w(\alpha),w(\beta))$; this inequality still holds if $c_k=0$ or $d_k=0$. Since $w(-\alpha)=w(\alpha)$, the usual argument shows:

(3) if $w(\alpha)\neq w(\beta)$, then $w(\alpha+\beta)=\inf(w(\alpha),w(\beta))$.

It remains to check that $w(\alpha\beta)=w(\alpha)+w(\beta)$. Take any a_i and a_j and write $a_ia_j=a_ke$ with $e\in L^*$. Then for any $c,\ d\in L^*$,

$$
\begin{aligned}
(4)\qquad w(a_icda_jd) &= w\big(a_ke\big(a_j^{-1}ca_j\big)d\big)\\
&= \frac{1}{m}v(a_k^m)+v(e)+v\big(a_j^{-1}ca_j\big)+v(d)\\
&= \frac{1}{m}v\big((a_ke)^m\big)+v(c)+v(d)\quad \text{by (1) and (ii)}\\
&= \frac{1}{m}\big[v(a_i^m)+v\big(a_j^m\big)\big]+v(c)+v(d)\quad \text{by (2)}\\
&= w(a_ic)+w\big(a_jd\big).
\end{aligned}
$$

Now, for any $\alpha=\sum a_ic_i$ and $\beta=\sum a_id_i\in A-\{0\}$ we have

$$
\begin{aligned}
(5)\qquad w(\alpha\beta) &= w\Big(\sum_{i,l}a_ic_ia_ld_l\Big)\geqslant \inf_{i,l}\{w(a_ic_ia_ld_l)|c_i,\ d_l\neq 0\}\\
&= \inf_{i,l}\{w(a_ic_i)+w(a_ld_l)|c_i,\ d_l\neq 0\}\geqslant w(\alpha)+w(\beta).
\end{aligned}
$$

Say a_jc_j is the leading term of α, and set $\alpha'=\alpha-a_jc_j$. So, $w(\alpha)=w(a_jc_j)<w(\alpha')$ (or $\alpha'=0$). Likewise, set $\beta'=\beta-a_kd_k$, where a_kd_k is the leading term of β. Then,

$$\alpha\beta=(a_jc_ja_kd_k)+\alpha'(a_kd_k)+(a_jc_j)\beta'+\alpha'\beta'.$$

By (4) and (5) the first summand here has value strictly smaller than the other three. Hence, by (3) and (4), $\alpha\beta\neq 0$ and

$$w(\alpha\beta)=w\big(a_jc_ja_kd_k\big)=w(a_jc_j)+w(a_kd_k)=w(\alpha)+w(\beta).$$

Since we have just seen that the finite dimensional algebra A has no zero divisors, it must be a division algebra. Our calculations show that $w\colon A-\{0\}\to\Delta$ is a valuation on A. It is easy to check that $w|_L=v$.

Clearly the value group Γ_A is the subgroup of Δ generated by $\{w(a_1),\dots,w(a_m)\}$ and Γ_L; so $\Gamma_A/\Gamma_L=\operatorname{im}(\overline{w})$. As $\overline{w}$ is injective, $|\Gamma_A/\Gamma_L|=|\mathscr{A}|=m=[A:L]$, i.e. A is totally ramified over L. Take any $\alpha=\sum a_ic_i\in A^*$ with $w(\alpha)=0$. If the leading term of α is a_jc_j, we have $w(a_jc_j)=w(\alpha)=0$. Since $w(a_j)=-w(c_j)\in\Gamma_L$, the injectivity of $\overline{w}$ implies $a_j\in L^*$; so $a_jc_j\in U_L$. Hence, in $\overline{A}$, $\bar{\alpha}=\overline{a_jc_j}\in\overline{L}$. Thus, $\overline{A}=\overline{L}$. □

COROLLARY 2.6. *Consider the algebra*

$$A=A_{\omega_1}(b_1,c_1;\ F)\otimes_F\cdots\otimes_F A_{\omega_k}(b_k,c_k;\ F),$$

where ω_m is a primitive n_mth root of unity in a field F and $b_1,\ c_1,\dots,b_k,\ c_k\in F^*$. Let $n=n_1\cdots n_k$ and $l=\operatorname{lcm}(n_1,\dots,n_k)$. Let v be a valuation on F. Suppose $\{(l/n_m)v(b_m),(l/n_m)v(c_m)|1\leqslant m\leqslant k\}$ generates a subgroup of order n^2 in $\Gamma_F/l\Gamma_F$.

Then A is a division algebra and v extends to a valuation on A totally ramified over F, with $\overline{A} = \overline{F}$ and with value group Γ_A generated by $\{(1/n_m)v(b_m), (1/n_m)v(c_m) | 1 \leqslant m \leqslant k\}$ and Γ_F. So,

$$\Gamma_A/\Gamma_F \cong \prod_{m=1}^{k} (\mathbf{Z}/n_m\mathbf{Z} \times \mathbf{Z}/n_m\mathbf{Z}).$$

PROOF. For $1 \leqslant m \leqslant k$, let i_m, $j_m \in A$ be the standard generators of

$$A_{\omega_m}(b_m, c_m;\ F).$$

We want to apply the theorem with $L = F$ and the a_i all being products $i_1^{r_1} j_1^{s_1} \cdots i_k^{r_k} j_k^{s_k}$ with $0 \leqslant r_m < n_m$, $0 \leqslant s_m < n_m$, for $1 \leqslant m \leqslant k$. There are n^2 of the a_i and they clearly form an F-base of A. Every commutator $a_i a_j a_i^{-1} a_j^{-1}$ is a product of roots of unity. Condition (ii) holds trivially since F is the center of D. It follows easily that (i)–(iv) of the theorem all hold. We have $\overline{w}(i_m F^*) = (1/n_m)v(b_m) + \Gamma_F$ and $\overline{w}(j_m F^*) = (1/n_m)v(c_m) + \Gamma_F$. The assumption on the values of the b_m and c_m implies that $\overline{w}(\mathscr{A})$ is a subgroup of order n^2 of $(1/l)\Gamma_F/\Gamma_F$. Hence, $\overline{w}$ must be injective, and the corollary follows from the theorem. □

EXAMPLE 2.7. Let K be a field containing a primitive p^rth root of unity ω for some prime p. Let $z_1, \ldots, z_{2l}$ be independent commuting indeterminates over K, and let $F = K(z_1, \ldots, z_{2l})$. The lexicographic ordering makes $\Gamma := \prod_{i=1}^{2l} \mathbf{Z}$ into a totally ordered abelian group. There is a unique valuation v: $F^* \to \Gamma$ such that $v(z_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$ (the 1 in the ith place) for each i and $v(c) = 0$ for all $c \in K^*$. Specifically, v is defined first on $K[z_1, \ldots, z_{2l}] - \{0\}$ by

$$v\left(\sum_{i_1} \cdots \sum_{i_{2l}} c_{i_1 i_2 \cdots i_{2l}} z_1^{i_1} \cdots z_{2l}^{i_{2l}}\right) = \inf\left\{(i_1, \ldots, i_{2l}) | c_{i_1 \cdots i_{2l}} \neq 0\right\}.$$

Then v is extended to the quotient field F by defining $v(a/b) = v(a) - v(b)$ for all $a,\ b \in K[z_1, \ldots, z_{2l}] - \{0\}$. Let $A = A_\omega(z_1, z_2;\ F) \otimes_F \cdots \otimes_F A_\omega(z_{2l-1}, z_{2l};\ F)$. By the corollary, A is a division algebra and v extends to a valuation on A which is totally ramified over F, with $\Gamma_A/\Gamma_F \cong (\mathbf{Z}/p^r\mathbf{Z})^{2l}$ and $\overline{A} = \overline{F} = K$. Hence, by Corollary 2.3, if $K \supseteq F$ is any subfield of A which is Galois over F, then $\mathscr{G}(K/F)$ is isomorphic to a subgroup of $(\mathbf{Z}/p^r\mathbf{Z})^{2l}$. Note also that if $L \supseteq F$ is any field which has an unramified extension of v, then Corollary 2.6 applies equally well to $A \otimes_F L$. So, $A \otimes_F L$ is also a valued division algebra, with $\Gamma_{A \otimes L}/\Gamma_L \cong \Gamma_A/\Gamma_F$.

REMARK 2.8. For any prime p, let k be any field with $\operatorname{char} k \neq p$, and let $K = k(\mu_{p^n})$ for some fixed $n \geqslant 3$. If we let $r = 1$ and $l = n$ in the preceding example, then we obtain a division algebra D_1 of index p^n in which every maximal subfield of D_1 Galois over its center has an elementary abelian Galois group of order p^n. If we let $r = n$ and $l = 1$ in the example we obtain another division algebra D_2 of index p^n. The Galois group over the center of D_2 of any Galois maximal subfield must be a subgroup of $(\mathbf{Z}/p^n\mathbf{Z}) \times (\mathbf{Z}/p^n\mathbf{Z})$ of order p^n. Such a group cannot be elementary abelian, as $n \geqslant 3$. Since no group can occur as a Galois group of a maximal subfield for both D_1 and D_2, it follows by Amitsur's argument (cf. [**Am**, pp. 418–419; or **Ja**, p. 93, Theorem 4]) that the generic division algebra

$UD(k, p^n)$ of index p^n ($n \geq 3$) over k is not a crossed product. Amitsur proved this in his original paper (for $\operatorname{char} k = 0$, and Schacher-Small [**SS**] did the case $\operatorname{char} k =$ prime $\neq p$). Amitsur did not mention valued division algebras, but the valuation theory given here applies to (and perhaps clarifies) his examples, which were iterated twisted Laurent power series division algebras.

We now give one more corollary to Theorem 2.5, which will apply to the examples in §6.

COROLLARY 2.9. *Let F be a field with valuation v. Let $K_1, \dots, K_k$ be cyclic Galois extensions of F, and let $A = A(K_1/F, \sigma_1, b_1) \otimes_F \cdots \otimes_F A(K_k/F, \sigma_k, b_k)$ for some $b_1, \dots, b_k \in F^*$. Let $[K_i : F] = n_i$, $n = n_1 \cdots n_k$, and $l = \operatorname{lcm}(n_1, \dots, n_k)$. Suppose*

(i) *each K_i is an inertial extension of (F, v), i.e., v extends (uniquely) to a valuation v_i on K with residue field $\overline{K}_i$ such that $[\overline{K}_i : \overline{F}] = [K_i : F]$;*

(ii) *$\overline{K}_1, \dots, \overline{K}_k$ are all linearly disjoint over $\overline{F}$;*

(iii) *$\{(l/n_i)v(b_i) \mid 1 \leq i \leq k\}$ generates a subgroup of order n in $\Gamma_F/l\Gamma_F$.*

Then A is a division algebra and v extends to a valuation w on A with residue division algebra $\overline{A} = \overline{K}_i \cdot \cdots \cdot \overline{K}_k$ and value group Γ_A generated by $\{(1/n_i)v(b_i)\}$ and Γ_F. So, $[\overline{A} : \overline{F}] = |\Gamma_A : \Gamma_F| = n$.

PROOF. Let L be the compositum $K_1 \cdot \cdots \cdot K_k$ in $\tilde{F}$, and let u be any extension of v to L, with $\overline{L}$ the residue field of u. Since $u|_{K_i} = v_i$ by (i), we have each $\overline{K}_i \subseteq \overline{L}$. Then from (2.1), (ii), and (i),

$$[L : F] \geq [\overline{L} : \overline{F}] \geq [\overline{K}_1 \cdot \cdots \cdot \overline{K}_k : \overline{F}] = \prod_{i=1}^{k} [\overline{K}_i : \overline{F}] = \prod_{i=1}^{k} [K_i : F] \geq [L : F].$$

So equality must hold throughout. Hence, L is an inertial extension of F, $\overline{L} = \overline{K}_1 \cdot \cdots \cdot \overline{K}_k$ and $K_1, \dots, K_k$ are all linearly disjoint over F, so $L \cong K_1 \otimes_F \cdots \otimes_F K_k$.

Let $x_j \in A$ be the standard generator of $A(K_j/F, \sigma_j, b_j)$ over K_j. We will apply Theorem 2.5, taking for the a_i, $1 \leq i \leq n$, all products $x_1^{r_1} \cdots x_k^{r_k}$ with $0 \leq r_j < n_j$ for each j. For L we take $K_1 \otimes_F \cdots \otimes_F K_k \subseteq A$ which we have seen has a unique extension of v on F. Clearly the a_i form an L-base of A. Condition (ii) of Theorem 2.5 holds since the a_i conjugate each K_j to itself and the extension of v to L is unique. Condition (iii) holds trivially because $a_i a_j = a_j a_i$, all i, j, and (iv) also clearly holds. We have $\overline{w}(x_j L^*) = (1/n_j)v(b_j) + \Gamma_L$, and $\Gamma_L = \Gamma_F$ as L/F is inertial. Assumption (iii) implies that $\overline{w}(\mathscr{A})$ is a subgroup of order n in $(1/l)\Gamma_L/\Gamma_L$. Since $|\mathscr{A}| = n$, $\overline{w}$ must be injective. The conclusions of the corollary follow from the theorem and the observations above about L. □

3. Cohomology of free abelian pro-p-groups. For any prime number p and any natural number m, let $P_m := \oplus_{i=1}^{m} \hat{\mathbf{Z}}_p$, which is the free abelian pro-p-group of rank m. As we saw in Lemma 1.9(iv) this group arises as $G_p(F)$ for a strictly p-Henselian valued field if $\Gamma_F/p\Gamma_F$ has rank m. In this section we prove a result on splitting of elements of $H^2(P_m, \mathbf{Z}/p\mathbf{Z})$ by subgroups of P_m. We will give purely cohomological arguments, although other approaches are possible. We always consider $\mathbf{Z}/p\mathbf{Z}$ as a trivial P_m-module. Then $H^1(P_m, \mathbf{Z}/p\mathbf{Z}) \cong \operatorname{Hom}(P_m, \mathbf{Z}/p\mathbf{Z}) \cong (\mathbf{Z}/p\mathbf{Z})^m$, which will be viewed as a vector space over $\mathbf{Z}/p\mathbf{Z}$.

LEMMA 3.1. *Suppose* $\chi_1, \chi_2, \ldots, \chi_{2t}$ *are linearly independent in* $H^1(P_m, \mathbf{Z}/p\mathbf{Z})$. *Then,*

$$\chi_1 \cup \chi_2 + \chi_3 \cup \chi_4 + \cdots + \chi_{2t-1} \cup \chi_{2t} \neq 0 \quad \text{in } H^2(P_m, \mathbf{Z}/p\mathbf{Z}).$$

PROOF. We verify this by direct calculation, using additive notation for the group operation on P_m. The cohomology class in question is represented by the 2-cocycle

$$z(r,s) = \chi_1(r)\chi_2(s) + \chi_3(r)\chi_4(s) + \cdots + \chi_{2t-1}(r)\chi_{2t}(s),$$

as the group action is trivial (cf. [**Sh**, p. 38]). Clearly $z(r,0) = z(0,s) = 0$. If z is a coboundary, there is a continuous function $f\colon P_m \to \mathbf{Z}/p\mathbf{Z}$ with $z(r,s) = f(s) - f(r+s) + f(r)$. So $f(0) = z(0,0) = 0$. Now, choose $a_1, a_2 \in P_m$ with $\chi_i(a_j) = \delta_{ij}$ (Kronecker delta), $i = 1, \ldots, 2t$, $j = 1, 2$. We calculate: $f(a_1) + f(-a_1) = z(a_1, -a_1) = 0$. Thus, as P_m is abelian,

$$\begin{aligned} f(a_2) &= f(a_1 + a_2 + -a_1) = f(a_1 + a_2) - z(a_1 + a_2, -a_1) + f(-a_1) \\ &= f(a_1) - z(a_1, a_2) + f(a_2) - 0 - f(a_1) = -1 + f(a_2). \end{aligned}$$

This contradiction proves the lemma. □

REMARK 3.2. For an alternative proof observe that Lemma 3.1 is an immediate consequence of the isomorphism $H^2(P_m, \mathbf{Z}/p\mathbf{Z}) \cong H^1(P_m, \mathbf{Z}/p\mathbf{Z}) \wedge H^1(P_m, \mathbf{Z}/p\mathbf{Z})$ (exterior product) which can be verified by induction on m using the Künneth formula. The lemma is also deducible from Corollary 2.6.

REMARK 3.3. Suppose $\Delta \subseteq P_m$ is a subgroup of index p. Then $\Delta \supseteq pP_m$. Using the fact that every lift of a $\mathbf{Z}/p\mathbf{Z}$-base of P_m/pP_m is a base of P_m as a free abelian pro-p-group, it is easy to see that $\Delta \cong P_m$ as profinite groups. It follows by induction that for any subgroup H of finite index in P_m, H is open in P_m and $H \cong P_m$.

The main result of this section is needed for the study of splitting fields of the examples in §5. What we need is obtainable by adapting to the strictly p-Henselian situation the following theorem of Tignol and Amitsur [**TA**]: If D is a central simple division algebra over a field F with strictly Henselian valuation and $\operatorname{char} \overline{F} \nmid [D:F]$, then every splitting field of D algebraic over F contains a maximal subfield of D. We prefer to give an entirely cohomological formulation and proof. For algebras of prime exponent the Tignol-Amitsur theorem is actually deducible from our next theorem.

THEOREM 3.4. *Suppose* $\chi_1, \chi_2, \ldots, \chi_{2t} \in H^1(P_m, \mathbf{Z}/p\mathbf{Z})$ *are linearly independent, and set* $\gamma = \chi_1 \cup \chi_2 + \chi_3 \cup \chi_4 + \cdots + \chi_{2t-1} \cup \chi_{2t} \in H^2(P_m, \mathbf{Z}/p\mathbf{Z})$. *Let* N *be an open subgroup of* P_m *with* $\operatorname{res}_{P_m \to N}(\gamma) = 0$. *Then, there is a base* $\psi_1, \ldots, \psi_{2t}$ *of* $\operatorname{span}\{\chi_1, \ldots, \chi_{2t}\} \subseteq H^1(P_m, \mathbf{Z}/p\mathbf{Z})$ *such that* $\gamma = \psi_1 \cup \psi_2 + \cdots + \psi_{2t-1} \cup \psi_{2t}$ *and* $N \subseteq \bigcap_{i=1}^{t} \ker \psi_{2i-1}$. *Hence,* $(\mathbf{Z}/p\mathbf{Z})^t$ *is a homomorphic image of* P_m/N.

PROOF. We argue by induction on t. Since $N \cong P_m$, we may apply Lemma 3.1 over N to see that $\{\operatorname{res}_{P_m \to N}(\chi_i) | 1 \leqslant i \leqslant 2t\}$ must be linearly dependent in $H^1(N, \mathbf{Z}/p\mathbf{Z})$. That is, for some nonzero linear combination $\delta = a_1\chi_1 + \cdots + a_{2t}\chi_{2t} \in H^1(P_m, \mathbf{Z}/p\mathbf{Z})$, $0 = \sum a_i \operatorname{res}_{P_m \to N}(\chi_i) = \operatorname{res}_{P_m \to N}(\delta)$. Hence, $N \subseteq \ker(\delta)$. After renumbering the χ_i if necessary and replacing δ by $a_1^{-1}\delta$ we may

assume $a_1 = 1$; that is, $\chi_1 = \delta - a_2\chi_2 - \cdots - a_t\chi_t$. If $t = 1$, we have $\gamma = \chi_1 \cup \chi_2 = \delta \cup \chi_2$ (as $\chi_2 \cup \chi_2 = 0$[3]), and the desired result follows by setting $\psi_1 = \delta$ and $\psi_2 = \chi_2$. Now assume $t > 1$. From the formula for χ_1 (together with $\chi_2 \cup \chi_2 = 0$[3]) we find

$$\begin{aligned}\gamma &= \delta \cup \chi_2 + (\chi_3 + a_4\chi_2) \cup (\chi_4 - a_3\chi_2) \\ &\quad + \cdots + (\chi_{2t-1} + a_{2t}\chi_2) \cup (\chi_{2t} - a_{2t-1}\chi_2) \\ &= \delta \cup \chi_2 + \sum_{i=2}^{t} \varphi_{2i-1} \cup \varphi_{2i},\end{aligned}$$

where $\varphi_{2i-1} = \chi_{2i-1} + a_{2i}\chi_2$ and $\varphi_{2i} = \chi_{2i} - a_{2i-1}\chi_2$. Clearly $\{\delta, \chi_2, \varphi_3, \ldots, \varphi_{2t}\}$ is a base of $\operatorname{span}\{\chi_1, \ldots, \chi_{2t}\}$.

Let $\gamma' = \gamma - (\delta \cup \chi_2) = \sum_{i=2}^{t} \varphi_{2i-1} \cup \varphi_{2i}$. Since $N \subseteq \ker\delta$, $\operatorname{res}_{P_m \to N}(\gamma') = \operatorname{res}_{P_m \to N}(\gamma) = 0$. By induction there are $\psi_3, \psi_4, \ldots, \psi_{2t} \in H^1(P_m, \mathbf{Z}/p\mathbf{Z})$ with $\operatorname{span}\{\psi_3, \ldots, \psi_{2t}\} = \operatorname{span}\{\varphi_3, \ldots, \varphi_{2t}\}$, $\gamma' = \sum_{i=2}^{t} \psi_{2i-1} \cup \psi_{2i}$, and $N \subseteq \bigcap_{i=2}^{t} \ker\psi_{2i-1}$. Set $\psi_1 = \delta$ and $\psi_2 = \chi_2$. Clearly $\psi_1, \ldots, \psi_{2t}$ have all the required properties. Let $K = \bigcap_{i=1}^{t} \ker\psi_{2i-1} \supseteq N$. Then P_m/K is a homomorphic image of P_m/N, and $P_m/K \cong (\mathbf{Z}/p\mathbf{Z})^t$ as $\psi_1, \psi_3, \ldots, \psi_{2t-1}$ are linearly independent. □

4. Free products of pro-p-groups. In this section we prove that, for certain p-Henselian fields L_1 and L_2, $G_p(L_1 \cap L_2)$ is the free product of $G_p(L_1)$ and $G_p(L_2)$ (Theorem 4.3). This will allow us to prove local global principles (Theorem 4.11) relating central simple $(L_1 \cap L_2)$-algebras to algebras over L_1 and L_2. Our main tools are a cohomological characterization of free products of pro-p-groups (Theorem 4.1) and the analogue for pro-p-groups of Kurosch's theorem on subgroups of free products (Theorem 4.5).

Let $\mathcal{G}_p$ denote the category of pro-p-groups, a subcategory of the category $\mathcal{G}$ of all groups. For $G_1, G_2 \in \mathcal{G}_p$, let $G_1 *_p G_2$ denote the free product (coproduct) of G_1 and G_2 in $\mathcal{G}_p$. (This is not the same as the free product of G_1 and G_2 in $\mathcal{G}$, nor even in the category of all profinite groups.) The existence of free products in $\mathcal{G}_p$ can be verified by observing that the inclusion functor $\mathcal{G}_p \hookrightarrow \mathcal{G}$ has a left adjoint, and free products exist in $\mathcal{G}$. More explicitly, one can construct the free product in $\mathcal{G}_p$ as follows: Let $G_1, G_2 \in \mathcal{G}_p$. Denote by $G_1 * G_2$ the usual free product of G_1 and G_2 in $\mathcal{G}$. Then

$$G_1 *_p G_2 = \varprojlim_N ((G_1 * G_2)/N),$$

as N ranges over all normal subgroups of $G_1 * G_2$ with $|G_1 * G_2 : N|$ a power of p. The easy verification that $G_1 *_p G_2$ has the desired universal mapping property is omitted.

---

[3] For any $\chi \in H^1(P_m, \mathbf{Z}/p\mathbf{Z})$, $\chi \cup \chi = 0$. For, there is a closed subgroup H of P_m with $P_m/H \cong P_1$ and a $\chi' \in H^1(P_m/H, \mathbf{Z}/p\mathbf{Z})$ with $\chi = \inf_{P_m/H \to P_m}(\chi')$. Since P_m/H is a free pro-p-group, $H^2(P_m/H, \mathbf{Z}/p\mathbf{Z}) = 0$. Hence, $\chi \cup \chi = \inf_{P_m/H \to P_m}(\chi' \cup \chi') = 0$.

The basic cohomological properties of free products in $\mathscr{G}_p$ are recalled in convenient form in the next two theorems, which are due to Neukirch [**N**, Sätze 4.3, 4.2]. (For a version of Theorem 4.1, see also [**Er**, Proposition 2].) Theorem 4.2 is the pro-p analogue to a well-known result for the usual free products of groups (cf. [**HS**, p. 220]).

Recall that $\mathbf{Z}/p\mathbf{Z}$ is always viewed as a trivial G-module for any $G \in \mathscr{G}_p$.

THEOREM 4.1 (NEUKIRCH). *Suppose* G, $G_1, \ldots, G_k$ *are pro-p-groups, and* f_j: $G_j \to G$ *are continuous homomorphisms,* $j = 1, 2, \ldots, k$. *Then the induced map* $G_1 *_p G_2 *_p \cdots *_p G_k \to G$ *is an isomorphism iff the map*

$$H^i(G, \mathbf{Z}/p\mathbf{Z}) \to \bigoplus_{j=1}^{k} H^i(G_j, \mathbf{Z}/p\mathbf{Z})$$

induced by the f_j *is an isomorphism for* $i = 1$ *and a monomorphism for* $i = 2$.

In his version of Theorem 4.1 Neukirch assumes that the G_j are subgroups of G. But his proof works in the situation described here, without initially assuming the f_j to be injective.

THEOREM 4.2 (NEUKIRCH). *Suppose* $G_1, \ldots, G_k$ *are pro-p-groups, and that* $G = G_1 *_p G_2 *_p \cdots *_p G_k$. *Then for any finite discrete G-module M and any* $i \geqslant 2$ *the map*

$$\text{res: } H^i(G, M) \to \bigoplus_{j=1}^{k} H^i(G_j, M)$$

(*induced by the inclusions* $G_j \hookrightarrow G$) *is an isomorphism. Moreover, if M is a trivial G-module,* res *is an isomorphism for* $i = 1$, *as well.*

The crucial observation needed for our examples is that free products of very nice groups can occur as $G_p(F)$ for suitable fields F. This is the conclusion of the next key theorem. (A special case of this theorem was proved by a different method in [**J**, Lemma 9′].)

Two valuations v_1 and v_2 on a field F are said to be *independent* if no proper subring of F contains both valuation rings V_{F,v_1} and V_{F,v_2}. Recall that the approximation theorem [**E**, (11.16); or **Bo**$_2$, §7, No. 2, Theorem 1] holds between any two independent valuations v_1 and v_2.

THEOREM 4.3. *Let* (L_i, v_i) *be p-Henselian valued fields with* $\mu_p \subseteq L_i$ *and* char $\overline{L}_i \neq p$, $i = 1, 2$. *Let* $F = L_1 \cap L_2$. *Suppose that the valuations* $v_1|_F$ *and* $v_2|_F$ *on F are independent and that the maps* $\Gamma_{F,v_i}/p\Gamma_{F,v_i} \to \Gamma_{L_i}/p\Gamma_{L_i}$ *and* $\overline{F}_{v_i} \to \overline{L}_{v_i}$ *are surjective,* $i = 1, 2$. *Then,*

$$G_p(F) \cong G_p(L_1) *_p G_p(L_2).$$

PROOF. For short we denote the unit group U_{F,v_i} by U_i, the value group Γ_{F,v_i} by Γ_i, the residue field $\overline{F}_{v_i}$ by $\overline{F}_i$, and $H_p^j(K, \mu_p) \cong H_p^j(K, \mathbf{Z}/p\mathbf{Z})$ by $H^j(K)$ for $K = F$ or L_1 or L_2. Let $\text{res}_{F \to L_i}$: $H^j(F) \to H^j(L_i)$ denote the map induced by the restriction homomorphism $G_p(L_i) \to G_p(F)$. Set $B_1 = L_2^p \cap F^*$ and $B_2 = L_1^p \cap F^*$.

Consider the commutative diagram:

$$
\begin{array}{lccccc}
0 \to & (U_1 \cap U_2)/(U_1 \cap U_2)^p \to & F^*/F^{*p} & \to & \Gamma_1/p\Gamma_1 \oplus \Gamma_2/p\Gamma_2 & \to 0 \\
(*) & \alpha \downarrow & \beta \downarrow & & \gamma \downarrow & \\
0 \to & U_{L_1}/U_{L_1}^p \oplus U_{L_2}/U_{L_2}^p \to & L_1^*/L_1^{*p} \oplus L_2^*/L_2^{*p} & \to & \Gamma_{L_1}/p\Gamma_{L_1} \oplus \Gamma_{L_2}/p\Gamma_{L_2} & \to 0
\end{array}
$$

The middle map β is injective as $\mu_p \subseteq F$ and $F = L_1 \cap L_2$; that is, $B_1 \cap B_2 = F^{*p}$. Clearly the bottom row of $(*)$ is exact. Since $v_1|_F$ and $v_2|_F$ are independent, the approximation theorem shows F^* maps onto $\Gamma_1 \oplus \Gamma_2$; hence, the top row of $(*)$ is exact. Because (L_i, v_i) is p-Henselian we have $U_{L_i}/U_{L_i}^p \cong \bar{L}_i^*/\bar{L}_i^{*p}$ (see Lemma 1.8(ii)). It follows that α is surjective by the approximation theorem and the hypothesis that $\bar{F}_i \cong \bar{L}_i$. By hypothesis, γ is also surjective. Thus, the snake lemma [**Bo**$_1$, §1, Proposition 2] implies that β and γ are isomorphisms. Hence, $B_i/F^{*p} \cong L_i^*/L_i^{*p}$, $i = 1, 2$, $B_1 \cdot B_2 = F^*$, and $p\Gamma_{L_i} \cap \Gamma_i = p\Gamma_i$, $i = 1, 2$. In cohomological terms, the isomorphism β reads: $H^1(F) \cong H^1(L_1) \oplus H^1(L_2)$.

Let C_{ij} denote the subgroup of $H^2(F)$ generated by the cup products $\{(a) \cup (b) | a \in B_i, b \in B_j\}$ for $i = 1, 2$, $j = 1, 2$. Since $B_1 \cdot B_2 = F^*$ the Merkurjev-Suslin Theorem 1.3 and the remarks after (1.7) show that $H^2(F) = C_{11} + C_{12} + C_{22}$. We will prove that $C_{12} = 0$ and $H^2(F) = C_{11} \oplus C_{22}$, with $C_{ii} \cong H^2(L_i)$ via the restriction map. Since clearly $\operatorname{res}_{F \to L_1}(C_{22}) = \operatorname{res}_{F \to L_2}(C_{11}) = 0$ it follows that res: $H^2(F) \to H^2(L_1) \oplus H^2(L_2)$ is an isomorphism. Then the desired conclusion $G_p(F) \cong G_p(L_1) *_p G_p(L_2)$ follows by Neukirch's Theorem 4.1.

Consider any generator $(a) \cup (b)$ of C_{12} with $a \in B_1$, $b \in B_2$. As $a \in L_2^p$, using $p\Gamma_{L_2} \cap \Gamma_2 = p\Gamma_2$, the surjectivity of $\bar{F}_2 \to \bar{L}_2$, and the approximation theorem we may find an $a' \in F^*$ with $a' \equiv a \bmod F^{*p}$, $v_2(a') = 0$, $\overline{a'} = 1$ in $\bar{F}_2$, and $v_1(a') > 0$. Likewise, there is a $b' \equiv b \bmod F^{*p}$ with $v_1(b') = 0$, $\overline{b'} = 1$ in $\bar{F}_1$, and $v_2(b') > 0$. Consequently $v_i(a' + b') = 0$ and $\overline{a' + b'} = 1$ in $\bar{L}_i$ for $i = 1$ and $i = 2$. Since the L_i are p-Henselian it follows by Lemma 1.8(i) that $a' + b' \in L_1^p \cap L_2^p \cap F = F^p$. Thus, $(a') \otimes (b')$ lies in the Steinberg relation subgroup of $H^1(F) \otimes H^1(F)$ (cf. Theorem 1.3). From this we see that $(a) \cup (b) = (a') \cup (b') = 0$ in $H^2(F)$. Thus, $C_{12} = 0$.

To complete the proof we must show $H^2(F) = C_{11} \oplus C_{22} \cong H^2(L_1) \oplus H^2(L_2)$. This is immediate from the following

CLAIM. There exist homomorphisms ε_i: $H^2(L_i) \to H^2(F)$, with $\operatorname{im}(\varepsilon_i) = C_{ii}$ and $\operatorname{res}_{F \to L_i} \circ \varepsilon_i$: $H^2(L_i) \to H^2(L_i)$ the identity map, $i = 1, 2$.

To prove the claim, observe first that the isomorphism $B_i/F^{*p} \cong L_i^*/L_i^{*p}$ yields an injection $\hat{\varepsilon}_i$: $H^1(L_i) \to H^1(F)$ which is the composite of

$$
H^1(L_i) \xrightarrow{\cong} L_i^*/L_i^{*p} \xrightarrow{\cong} B_i/F^{*p} \hookrightarrow F^*/F^{*p} \xrightarrow{\cong} H^1(F).
$$

Note that $\hat{\varepsilon}_i((a)_{L_i}) = (a)_F$ for every $a \in B_i$. The map $\hat{\varepsilon}_i \otimes \hat{\varepsilon}_i$ composed with the cup product yields a homomorphism

$$
\varepsilon_i'\colon H^1(L_i) \otimes H^1(L_i) \to H^2(F)
$$

defined on generators by $\varepsilon_i'((a)_{L_i} \otimes (b)_{L_i}) = (a)_F \cup (b)_F$ for all $a, b \in B_i$. Since $\operatorname{im}(\varepsilon_i') = C_{ii}$ and the composition $\operatorname{res}_{F \to L_i} \circ \hat{\varepsilon}_i$: $H^1(L_i) \to H^1(L_i)$ is identity, to prove the claim it suffices to show that ε_i' induces a well-defined homomorphism ε_i: $H^2(L_i) \to H^2(F)$. In view of the Merkurjev-Suslin Theorem 1.3 we must show that $S_i \subseteq \ker \varepsilon_i'$, where S_i is the Steinberg relation subgroup of $H^1(L_i) \otimes H^1(L_i)$. That is, Steinberg relations can be "lifted" from L_i to F.

Take any generator $(a)_{L_i} \otimes (b)_{L_i}$ of S_i, $a, b \in B_i$. Then there exist $r, s \in L_i^*$ such that

$$(\dagger) \qquad ar^p + bs^p = 1.$$

In showing $(a)_F \cup (b)_F = 0$ there are four cases to consider:

First, suppose $v_i(ar^p) \neq 0$ and $v_i(bs^p) \neq 0$. Then valuation theory and equation (†) show that $v_i(ar^p) = v_i(bs^p) < 0$ and $-ar^p(bs^p)^{-1} \in 1 + M_{L_i}$. This yields $-ab^{-1} \in L_i^p$ since L_i is p-Henselian. As $L_i^p \cap B_i = F^{*p}$ we find $-ab^{-1} \in F^{*p}$, i.e., $(b)_F = (-a)_F$ in $H^1(F)$. So $\varepsilon_i'((a)_{L_i} \otimes (b)_{L_i}) = (a)_F \cup (b)_F = (a)_F \cup (-a)_F = 0$ in $H^2(F)$ (cf. [**Mi**, p. 319]).

For the next case suppose $v_i(ar^p) = 0$ but $v_i(bs^p) \neq 0$. Then from (†) we have $v_i(bs^p) > 0$ and $ar^p \in 1 + M_{L_i} \subseteq L_i^p$. Thus, $a \in L_i^p \cap B_i = F^{*p}$. So, $(a)_F = 0$ in $H^1(F)$, which assures $(a)_F \cup (b)_F = 0$ in $H^2(F)$. The case where $v_i(ar^p) \neq 0$ but $v_i(bs^p) = 0$ is handled analogously.

In the final case, we have $v_i(ar^p) = v_i(bs^p) = 0$. So, $v_i(a)$, $v_i(b) \in p\Gamma_i$ by the injectivity of the map γ of diagram (*). Modifying a and b by pth powers from F, we may assume that each of a, b, r, s lies in U_{L_i}. Recall that $a \in B_i \subseteq L_j^p$, where $j = 3 - i$. So $v_j(a) \in p\Gamma_{L_j} \cap \Gamma_j = p\Gamma_j$. Applying the approximation theorem and the isomorphism $\overline{F}_i \cong \overline{L}_i$, we can choose $r', s' \in F^*$ with $v_i(r') = 0$, $\overline{r'} = \bar{r}$ in $\overline{L}_i$, $v_j(r'^p) = -v_j(a)$, and $v_i(s') = 0$, $\overline{s'} = \bar{s}$ in $\overline{L}_i$, $v_j(s'^p) > -v_j(b)$. Then $ar'^p + bs'^p$ is a unit with respect to each valuation, and $\overline{ar'^p + bs'^p} = \overline{ar^p + bs^p} = 1$ in $\overline{L}_i$ and $\overline{ar'^p + bs'^p} = \overline{ar'^p}$ in $\overline{L}_j^p$. Since L_1 and L_2 are each p-Henselian, it follows that $ar'^p + bs'^p \in L_1^p \cap L_2^p \cap F = F^p$. Hence, $(a)_F \otimes (b)_F$ lies in the Steinberg relation group of $H^1(F) \otimes H^1(F)$. Thus, $(a)_F \cup (b)_F = 0$ in $H^2(F)$. This establishes the claim and completes the proof of Theorem 4.3. □

REMARK 4.4. Suppose (L_i, v_i) are p-Henselian valued fields, $i = 1, 2$, with $\mu_p \subseteq L_i$ and $\operatorname{char} \overline{L}_i \neq p$ for each i. Let $F = L_1 \cap L_2$, and suppose $v_1|_F$ and $v_2|_F$ are independent valuations. In each of the following two situations we can see that each (L_i, v_i) is an immediate extension of (F, v_i), so the hypotheses of Theorem 4.3 are satisfied:

(i) Each L_i is unramified over F, $\overline{L}_i$ is Galois over $\overline{F}_{v_i}$ and (L_i, v_i) is Henselian.

(ii) Each L_i is unramified over F and $L_i \subseteq \tilde{F}_p$, the pth root closure of F.

In either case, it suffices to check that $\overline{F}_i = \overline{F}_{v_i}$ maps onto $\overline{L}_i$. In case (i) take any $\bar{c} \in \overline{L}_i$, and let $\bar{f}_i \in \overline{F}_i[X]$ be the minimal polynomial of $\bar{c}$ over $\overline{F}_i$. Then $\bar{f}_i$ splits completely over $\overline{L}_i$, as $\overline{L}_i$ is Galois over $\overline{F}_i$. For $j = 3 - i$, pick any monic $\bar{f}_j \in \overline{F}_j[X]$ with $\deg \bar{f}_j = \deg \bar{f}_i$, and such that $\bar{f}_j$ splits completely in $\overline{F}_j[X]$ with no repeated roots. By the approximation theorem applied to the corresponding coefficients of $\bar{f}_i$ and $\bar{f}_j$ there is a monic $f \in V_{F,v_1}[X] \cap V_{F,v_2}[X]$ with $\bar{f} = \bar{f}_1$ in $\overline{F}_1[X]$

and $\bar{f} = \bar{f}_2$ in $\bar{F}_2[X]$. The Henselian assumption implies that f splits in L_1 and L_2. Hence, f splits in $L_1 \cap L_2 = F$. So, $\bar{c} \in \bar{F}_i$ which shows that $\bar{L}_i = \bar{F}_i$. In case (ii) we have $\mu_p \subseteq \bar{F}_i$ and $\bar{L}_i \subseteq \tilde{\bar{F}}_p$. From the theory of p-groups (cf. (1.4)) if $\bar{F}_i \neq \bar{L}_i$, then there is a $\bar{d} \in \bar{L}_i - \bar{F}_i$ with $\bar{d}^p \in \bar{F}_i$. Pick any $\bar{e} \in \bar{F}_j^*$, $j = 3 - i$. By the approximation theorem there is a $b \in F^*$ with $v_1(b) = v_2(b) = 0$ and $\bar{b} = \bar{d}^p$ in $\bar{F}_i$ and $\bar{b} = \bar{e}^p$ in $\bar{F}_j$. Since L_1 and L_2 are p-Henselian, we have $b \in L_1^p \cap L_2^p \cap F = F^p$. Hence $\bar{d}^p = \bar{b} \in \bar{F}_i^p$, contradicting the choice of $\bar{d}$.

We will exploit Theorem 4.3 below to obtain local global principles relating algebras over F to their extensions over L_1 and L_2. The key to moving from cohomological data to information about algebras is provided by some index computations which are consequences of the pro-p version of the famous Kurosch subgroup theorem. This theorem is due to Binz, Neukirch, and Wenzel [**BNW**]—in a more general form than given here. In what follows, we write H^g for the conjugate gHg^{-1} of a group H.

THEOREM 4.5 (BINZ, NEUKIRCH, WENZEL). *Suppose G, $G_1, \ldots, G_k$ are pro-p-groups with $G = G_1 *_p G_2 *_p \cdots *_p G_k$. Let H be an open subgroup of G. Then,*

$$H = \mathop{*_p}_{i=1}^{k} \left(\mathop{*_p}_{j=1}^{n_i} G_i^{g_{ij}} \cap H \right) *_p \mathscr{F},$$

where for each i the $g_{i1}, \ldots, g_{in_i}$ are a full set of representatives for the double cosets HgG_i of H and G_i in G, and $\mathscr{F}$ is a free pro-p-group.

Before turning to central simple algebras we consider the notion of index in a purely cohomological setting:

DEFINITION 4.6. Let G be a pro-p-group and let $\gamma \in H^i(G, M)$, $i \geqslant 2$, for some discrete G-module M. The *p-index* of γ is

$$p\text{-ind}(\gamma) := \min\{|G:H| \mid H \text{ is an open subgroup of } G \text{ and } \operatorname{res}_{G \to H}(\gamma) = 0 \text{ in } H^i(H, M)\}.$$

REMARKS 4.7. (i) p-ind(γ) is always finite. For, as M is discrete and γ is a continuous cohomology class, there is an open normal subgroup N of G with $\gamma \in \operatorname{im}(\inf_{G/N \to G})$. Hence, $\operatorname{res}_{G \to N}(\gamma) = 0$.

(ii) If K is a closed subgroup of G, then p-ind$(\operatorname{res}_{G \to K}(\gamma)) \leqslant p$-ind$(\gamma)$.

(iii) If $\operatorname{res}_{G \to H}(\gamma) = 0$, we say that H *splits* γ. Note that if H splits γ, then every conjugate H^g of H in G also splits γ. For, the conjugation map $H \to H^g$ induces a function $c_{g,H}$: $H^i(H, M) \to H^i(H^g, M)$. Since $c_{g,G}$ is the identity map on $H^i(G, M)$ (cf. [**Se**$_2$, p. 116, Proposition 3; or **We**, p. 65, Proposition 2-3-1]), we have

$$\operatorname{res}_{G \to H^g}(\gamma) = (\operatorname{res}_{G \to H^g} \circ c_{g,G})(\gamma) = (c_{g,H} \circ \operatorname{res}_{G \to H})(\gamma) = 0.$$

THEOREM 4.8. *Suppose $H_1, \ldots, H_k$ are closed subgroups of a pro-p-group G, and suppose $G = H_1 *_p \cdots *_p H_k$. Then, for any discrete G-module M and any $\gamma \in H^i(G, M)$, $i \geqslant 2$,*

$$p\text{-ind}(\gamma) = \max_{1 \leqslant j \leqslant k} \left\{ p\text{-ind}\big(\operatorname{res}_{G \to H_j}(\gamma)\big) \right\}.$$

PROOF. Let $p^m = \max_{1 \leq j \leq k}\{ p\text{-ind}(\text{res}_{G \to H_j}(\gamma))\}$. By Remark 4.7(ii), $p\text{-ind}(\gamma) \geq p^m$. To prove the reverse inequality we proceed by induction on m. If $m = 0$, each H_i splits γ, so as $H^i(G, M) \cong \oplus_{j=1}^k H^i(H_j, M)$ by Theorem 4.2, we find that G splits γ, i.e., $p\text{-ind}(\gamma) = 1 = p^0$.

Now, suppose $m \geq 1$. For each j, choose an open subgroup K_j of H_j such that K_j splits γ and $|H_j : K_j| = p\text{-ind}(\text{res}_{G \to H_j}(\gamma))$. If $K_j \neq H_j$, let N_j be a maximal proper subgroup of H_j containing K_j; so N_j is normal in H_j and $H_j/N_j \cong \mathbf{Z}/p\mathbf{Z}$, as H_j is a pro-p-group. If $K_j = H_j$, let $N_j = H_j$. Then for each j there is a homomorphism π_j: $H_j \to \mathbf{Z}/p\mathbf{Z}$ with kernel N_j. At least one π_j is surjective, as $m \geq 1$. By the universal mapping property of the free product there is an epimorphism π: $G \to \mathbf{Z}/p\mathbf{Z}$ with $\pi|_{H_j} = \pi_j$ for each j. Set $N = \ker(\pi)$. Then N is a normal subgroup of G, $|G : N| = p$, and $N \cap H_j = N_j \supseteq K_j$ for $j = 1, 2, \ldots, k$.

Applying Theorem 4.5 we have

$$N = L_1 *_p \cdots *_p L_l *_p \mathscr{F},$$

where $\mathscr{F}$ is a free pro-p-group and each $L_i = N \cap H_{j(i)}^{g_i} = (N \cap H_{j(i)})^{g_i}$ for some $g_i \in G$ and $j(i) \in \{1, 2, \ldots, k\}$. Set $K_i' = K_{j(i)}^{g_i} \subseteq L_i$ and set $\delta = \text{res}_{G \to N}(\gamma)$. Since $K_{j(i)}$ splits γ, K_i' must also split γ (hence δ), by Remark 4.7(iii). Consequently,

$$p\text{-ind}\big(\text{res}_{N \to L_i}(\delta)\big) \leq |L_i : K_i'| = |N_{j(i)} : K_{j(i)}| \leq p^{m-1}.$$

Also, $p\text{-ind}(\text{res}_{N \to \mathscr{F}}(\delta)) = p^0$ as $H^i(\mathscr{F}, M) = 0$, $i \geq 2$. Thus, by induction, $p\text{-ind}(\delta) \leq p^{m-1}$, so that

$$p\text{-ind}(\gamma) \leq |G : N| \cdot p\text{-ind}\big(\text{res}_{G \to N}(\gamma)\big) \leq p \cdot p^{m-1} = p^m.$$

This proves the theorem. □

DEFINITION 4.9. Let A be a central simple F-algebra with $[A] \in \text{Br}_p(F)$. The *p-index* of A is

$$p\text{-ind}(A) := \min\big\{[L : F] \mid L \text{ is a field, } F \subseteq L \subseteq \tilde{F}_p, \text{ and } L \text{ splits } A\big\}.$$

REMARKS 4.10. (i) For every A with $[A] \in \text{Br}_p(F)$, $p\text{-ind}(A)$ is necessarily finite. For, as we observed in §1, every such A is split by $\tilde{F}_p$, so by some finite degree subextension.

(ii) If $\mu_p \subseteq F$, then $G_p(F)$ is a pro-p-group. If $[A]$ has exponent p^n there is a corresponding element γ of $H_p^2(F, \mu_{p^n})$. Then for any field $M \supseteq F$, $\text{res}_{F \to M}(\gamma)$ is the element of $H_p^2(M, \mu_{p^n})$ corresponding to $[M \otimes_F A]$ in $\text{Br}_p(M)$. From this it is clear that $p\text{-ind}(A) = p\text{-ind}(\gamma)$, which is a power of p. However, if $\mu_p \notin F$, it is unknown whether $p\text{-ind}(A)$ is always a p-power.

(iii) For any A with $[A] \in \text{Br}_p(F)$, clearly $\text{index}(A) \leq p\text{-ind}(A)$, but it is an open question whether equality always holds. (Equality means that the underlying division algebra of A has a maximal subfield in $\tilde{F}_p$.) Indeed, if $\mu_p \subseteq F$ and $\text{index}(A) = p$, then $p\text{-ind}(A) = p$ iff the underlying division algebra of A is a cyclic algebra. But for $p \geq 5$ (p prime) it is unknown whether every division algebra of index p is cyclic.

THEOREM 4.11 (LOCAL-GLOBAL PRINCIPLES). *Let L_1 and L_2 be fields with $\mu_p \subseteq L_i$, $i = 1, 2$, and let $F = L_1 \cap L_2$. Suppose the natural map $G_p(L_1) *_p G_p(L_2) \to G_p(F)$ is an isomorphism. Then for any central simple F-algebra A with $[A] \in \mathrm{Br}_p(F)$,*

(i) *F splits A iff L_1 and L_2 each split A;*

(ii) $\mathrm{index}(A) \leqslant p\text{-ind}(A) = \max\{p\text{-ind}(A \otimes_F L_i) | i = 1, 2\}$;

(iii) *if* $\mathrm{index}(A \otimes_F L_i) = p\text{-ind}(A \otimes_F L_i)$, $i = 1, 2$, *then* $\mathrm{index}(A) = p\text{-ind}(A)$;

(iv) *for any field K with $F \subseteq K \subseteq \tilde{F}_p$ and $[K : F] < \infty$, K splits A iff $K \otimes_F L_i$ splits A, $i = 1, 2$;*

(v) *suppose there are finite degree Galois p-extensions M_i of L_i which split A, and suppose G is a finite p-group generated by isomorphic copies of $\mathcal{G}(M_i/L_i)$, $i = 1, 2$; then there is a Galois extension M of F for which $\mathcal{G}(M/F) \cong G$, M splits A and $M \cdot L_i = M_i$, $i = 1, 2$.*

Note that for K as in (iv), K is separable over F, so $K \otimes_F L_i$ is a direct sum of fields. "$K \otimes_F L_i$ splits A" means each summand splits A.

PROOF. Suppose $[A]$ has exponent p^n; let $\gamma \in H_p^2(F, \mu_{p^n})$ be the element corresponding to $[A]$ in ${}_{p^n}\mathrm{Br}(F)$.

Part (i) is immediate from the isomorphism $H_p^2(F, \mu_{p^n}) \cong H_p^2(L_1, \mu_{p^n}) \oplus H_p^2(L_2, \mu_{p^n})$ given by Theorem 4.2. Part (ii) follows from Theorem 4.8 and Remarks 4.10(ii), (iii). Since $\mathrm{index}(A) \geqslant \max\{\mathrm{index}(A \otimes_F L_i) | i = 1, 2\}$, (iii) is immediate from (ii).

For (iv) the "only if" part is clear. For the reverse implication assume that (each summand of) each $K \otimes_F L_i$ splits A. Let $N = G_p(K)$, an open subgroup of $G_p(F)$. Let $H_i = G_p(L_i)$, which we identify with its image in $G_p(F)$. (The free product hypothesis assures that the map $H_i \to G_p(F)$ is injective.) Let

$$N = N_{11} *_p \cdots *_p N_{1n_1} *_p N_{21} *_p \cdots *_p N_{2n_2} *_p \mathcal{F}$$

be the free product decomposition of N given by Theorem 4.5, where $N_{ij} = H_i^{g_{ij}} \cap N$ for suitable $g_{ij} \in G_p(F)$ and $\mathcal{F}$ is a free pro-p-group. For each i, j, $H_i \cap N^{g_{ij}^{-1}}$ is (isomorphic to) $G_p(g_{ij}^{-1}(K) \cdot L_i)$. Since the compositum $g_{ij}^{-1}(K) \cdot L_i$ is isomorphic to a summand of $K \otimes_F L_i$, it splits A. Thus, $\mathrm{res}_{G \to (H_i \cap N^{g_{ij}^{-1}})}(\gamma) = 0$. Let $\delta = \mathrm{res}_{G \to N}(\gamma)$. Since $H_i \cap N^{g_{ij}^{-1}} = N_{ij}^{g_{ij}^{-1}}$, we have $0 = \mathrm{res}_{G \to N_{ij}}(\gamma) = \mathrm{res}_{N \to N_{ij}}(\delta)$ (cf. Remark 4.7(iii)). Because $\mathcal{F}$ is free, $\mathrm{res}_{N \to \mathcal{F}}(\delta) = 0$. Therefore, by Theorem 4.2 $\delta = 0$ in $H^2(N, \mu_{p^n})$, i.e., K splits A, as desired.

(v) Let f_i be the composite homomorphism $G_p(L_i) \to \mathcal{G}(M_i/L_i) \hookrightarrow G$, with kernel $G_p(M_i)$; we have an induced epimorphism f: $G_p(F) \xrightarrow{\cong} G_p(L_1) *_p G_p(L_2) \to G$. Let M be the fixed field of $\ker f$. Then M is Galois over F and $\mathcal{G}(M/F) \cong G_p(F)/\ker f \cong G$. When we identify $G_p(F)$ with $G_p(L_1) *_p G_p(L_2)$, $\ker f \cap G_p(L_i) = \ker f_i = G_p(M_i)$. Consequently, $M \cdot L_i = M_i$. Since M is Galois over F every summand of $M \otimes_F L_i$ is isomorphic to $M \cdot L_i$. Hence, $M \otimes_F L_i$ splits A. By (iv) M splits A, as desired. □

REMARK. Theorems 4.3 and 4.11 which were stated for $F = L_1 \cap L_2$ clearly hold as well for $F = L_1 \cap L_2 \cap \cdots \cap L_k$ for any integer $k \geqslant 2$.

5. Noncrossed products of exponent p^n, $n \geq 3$. Fix a prime number p and integers $m \geq n \geq 3$. In this section we will construct a noncrossed product division algebra D of exponent p^n and index p^m over a field F of any characteristic $\neq p$.

To begin, fix any field k containing p distinct pth roots of unity (so $\operatorname{char} k \neq p$). Set $F_0 = k(x_1, x_2, y_1, y_2, y_3, \ldots, y_{2m})$, where $x_1, x_2, y_1, \ldots, y_{2m}$ are algebraically independent over k. Let v_1 be the valuation on F_0 with residue field $k(y_1, \ldots, y_{2m})$ and value group $\mathbf{Z} \times \mathbf{Z}$, ordered lexicographically, with $v_1(x_1) = (1,0)$ and $v_1(x_2) = (0,1)$. (This is the valuation described in Example 2.7, viewing $F_0 = K(x_1, x_2)$, with $K = k(y_1, \ldots, y_{2m})$.) Let v_2 be the valuation on F_0 with residue field $k(x_1, x_2)$ and value group $\prod_{i=1}^{2m} \mathbf{Z}$, ordered lexicographically, with $v_2(y_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$ (the 1 in the ith place). (This is another case of Example 2.7, viewing $F_0 = K(y_1, \ldots, y_{2m})$ with $K = k(x_1, x_2)$.) Clearly v_1 and v_2 are independent valuations on F_0. Within some fixed algebraic closure of F_0 let (L_1, v_1) be a strict p-Henselization of (F_0, v_1) and let (L_2, v_2) be a strict p-Henselization of (F_0, v_2), as described in §1.

Let $F = L_1 \cap L_2$. Note that F contains a primitive p^nth root of unity ω as $\mu_{p^l} \subseteq L_i$ for all l, $i = 1, 2$. Let $\rho = \omega^{p^{n-1}}$, a primitive pth root of unity. Using the notation of §1 we define central simple F-algebras A_1 and A_2 by

$$A_1 = A_\omega(x_1, x_2; F) \quad \text{and} \quad A_2 = \bigotimes_{j=1}^{m} A_\rho(y_{2j-1}, y_{2j}; F).$$

Set $A = A_1 \otimes_F A_2$. By Wedderburn's theorem $A \cong M_l(D)$, where D is a division algebra with center F. The notation defined here will remain fixed throughout this section. We will show in Theorem 5.4 that D is not a crossed product. But first we summarize the nice properties of F given by our earlier theorems.

THEOREM 5.1. *With F, L_1, L_2, and p as above, we have*

(i) $G_p(L_1) \cong \hat{\mathbf{Z}}_p \oplus \hat{\mathbf{Z}}_p$ *and* $G_p(L_2) \cong (\hat{\mathbf{Z}}_p)^m$;

(ii) $G_p(F) \cong G_p(L_1) *_p G_p(L_2)$;

(iii) $\operatorname{Br}_p(F) \cong \operatorname{Br}_p(L_1) \oplus \operatorname{Br}_p(L_2)$;

(iv) *the local global principles (Theorem* 4.11*) apply from L_1 and L_2 to F.*

PROOF. Since the value group $\Gamma_{L_i} = \Gamma_{F_0, v_i}$, (i) follows from Lemma 1.9(iv). The valuations v_1 and v_2 are independent on F since they are independent on F_0 and F is algebraic over F_0. Thus, (ii) follows from Remark 4.4(ii) and Theorem 4.3. Then (iii) follows by Theorem 4.2, taking $M = \mu_{p^l}$, $l = 1, 2, \ldots$. Finally, (ii) implies (iv). □

REMARK 5.2. It can be shown (though we will not) that over a strictly p-Henselian field L every central simple division algebra B with $[B] \in \operatorname{Br}_p(L)$ is isomorphic to a tensor product of cyclic algebras. Hence, $\operatorname{index}(B) = p\text{-ind}(B)$. Using this and Theorem 4.11(iii) we can add the following properties of F to the list in 5.1: Let C be any central simple F-algebra with $[C] \in \operatorname{Br}_p(F)$; then

(v) $\operatorname{index}(C) = p\text{-ind}(C) = \max\{ p\text{-ind}(C \otimes_F L_i) | i = 1, 2\}$;

(vi) if C is a division algebra, then $C \otimes_F L_1$ is a division algebra or $C \otimes_F L_2$ is a division algebra.

LEMMA 5.3. (i) *$A_1 \otimes_F L_1$ is a division algebra of exponent, index, and p-index p^n, while L_2 splits A_1.*

(ii) *$A_2 \otimes_F L_2$ is a division algebra of index and p-index p^m, while L_1 splits A_2. If M is a Galois extension of L_2 which splits A_2 and $[M : L_2]$ is a power of p, then $(\mathbf{Z}/p\mathbf{Z})^m$ is a homomorphic image of $\mathcal{G}(M/L_2)$.*

PROOF. (i) Note that $A_1 \otimes_F L_1 \cong A_\omega(x_1, x_2; L_1) \cong A_1' \otimes_{F_0} L_1$, where $A_1' = A_\omega(x_1, x_2; F_0)$. Example 2.7 with the valuation v_1 on F_0 shows that A_1' is a division algebra, and that $A_1' \otimes_{F_0} L_1$ is also a division algebra, as (L_1, v_1) is unramified over (F_0, v_1). Since $A_1 \otimes_F L_1$ is a crossed product division algebra, $p\text{-ind}(A \otimes_F L_1) = \text{index}(A \otimes_F L_1) = p^n$. The valuation v_1 on L_1 extends uniquely to $L_1' := L_1(x_1^{1/p^n})$ with value group $p^{-n}\mathbf{Z} \times \mathbf{Z}$. So, v_1 maps the norm group $N_{L_1'/L_1}(L_1'^*)$ into $\mathbf{Z} \times p^n\mathbf{Z}$. Since $v_1(x_2) = (0, 1)$, x_2^l is not a norm from L_1' for $l < p^n$; hence the cyclic algebra $A_1 \otimes_F L_1$ has exponent at least p^n (cf. [**R**, p. 261, Corollary 30.7]). The exponent divides the index, so equals p^n. Turning to L_2, we have $x_1 \in L_2^{*p^n}$ by Lemma 1.9(ii) since x_1 is a unit of (L_2, v_2) which is strictly p-Henselian; hence L_2 splits A_1.

(ii) The arguments of (i) for A_1 apply to A_2 with the valuations reversed, yielding the first part of (ii). Now, $A_2 \otimes_F L_2$ corresponds to $(y_1) \cup (y_2) + \cdots + (y_{2m-1}) \cup (y_{2m})$ in $H_p^2(L_2, \mu_p) \cong H^2(P_{2m}, \mathbf{Z}/p\mathbf{Z})$. Thus, Theorem 3.4 establishes the final assertion of (ii). □

THEOREM 5.4. *Let D be the F-central division algebra defined at the beginning of this section. Then D has exponent p^n and index p^m where $m \geq n \geq 3$. Further,*

(i) *D is not a crossed product.*

(ii) *The matrix algebra $M_{p^r}(D)$ is not a crossed product for all integers $r \leq n - 3$.*

(iii) *$M_{p^{n-2}}(D)$ is a crossed product but is not isomorphic to a tensor product of cyclic algebras.*

(iv) *$M_{p^{n-1}}(D)$ is isomorphic to the tensor product of a cyclic algebra of index p^n and $(m - 1)$ cyclic algebras of index p.*

(v) *D has a maximal subfield whose normal closure over F is of degree a power of p.*

PROOF. Recall that D is the underlying division algebra of $A = A_1 \otimes_F A_2$. So, in $\text{Br}(L_i)$, $[D \otimes_F L_i] = [A \otimes_F L_i] = [A_i \otimes_F L_i]$, $i = 1, 2$, by Lemma 5.3. We have $\exp(D) \leq p^n$ by the construction of the A_i, and $\exp(D) \geq \exp(A_1 \otimes_F L_1) = p^n$, by Lemma 5.3. Applying 5.3 and the local global principles Theorem 4.11(iii), (ii), we have $\text{index}(D \otimes_F L_i) = p\text{-ind}(D \otimes_F L_i)$, $i = 1, 2$, hence $\text{index}(D) = p\text{-ind}(D) = \max\{p\text{-ind}(D \otimes_F L_i) | i = 1, 2\} = p^m$. Part (v) is a restatement of the equality $\text{index}(D) = p\text{-ind}(D)$.

Part (i) is a special case of (ii), so we prove (ii). Suppose $M_{p^r}(D)$ is a crossed product for $0 \leq r \leq n - 3$. This means that there is a splitting field K of D with K Galois over F and $[K : F] = p^{m+r}$. Then $K \cdot L_i$ is Galois over L_i and $[K \cdot L_i : L_i] | [K : F]$, so $K \cdot L_i \subseteq (\tilde{L}_i)_p$. Let $G_i = \mathcal{G}(K \cdot L_i / L_i)$. Then G_1 is a homomorphic image of $G_p(L_1) \cong (\hat{\mathbf{Z}}_p)^2$, so G_1 is abelian of rank ($:=$ minimum number of generators) ≤ 2. Hence, the p-torsion group ${}_pG_1$ of G_1 has order equal to $|G_1 / G_1^p| \leq p^2$. Also, since $K \cdot L_1$ splits D and hence splits $A_1 \otimes_F L_1$, we have $|G_1| = [K \cdot L_1 : L_1] \geq \text{index}(A_1 \otimes_F L_1) = p^n$ (cf. (1.1)). On the other hand, as $K \cdot L_2$

splits $A_2 \otimes_F L_2$, the last part of Lemma 5.3 says G_2 has $(\mathbf{Z}/p\mathbf{Z})^m$ as a homomorphic image. Therefore, the abelian group G_2 has a subgroup G_3 with $G_3 \cong (\mathbf{Z}/p\mathbf{Z})^m$. Both G_1 and G_3 may be viewed as subgroups of $\mathcal{G}(K/F)$. Since $|\mathcal{G}(K/F)| = p^{m+r} \leqslant p^{m+n-3}$ while $|G_1| \geqslant p^n$ and $|G_3| = p^m$, we find $|G_1 \cap G_3| \geqslant p^3 > |_pG_1|$. But $G_1 \cap G_3 \subseteq {}_pG_1$. This contradiction proves (ii).

(iii) $A_1 \otimes_F L_1$ has a splitting field $M_1 = L_1(x_1^{1/p^{n-1}}, x_2^{1/p})$ which is Galois over L_1 with $\mathcal{G}(M_1/L_1) \cong \mathbf{Z}/p^{n-1}\mathbf{Z} \oplus \mathbf{Z}/p\mathbf{Z}$. Likewise $A_2 \otimes_F L_2$ has a splitting field $M_2 = L_2(y_1^{1/p}, y_3^{1/p}, \ldots, y_{2m-1}^{1/p})$ which is Galois over L_2 with $\mathcal{G}(M_2/L_2) \cong (\mathbf{Z}/p\mathbf{Z})^m$. Since each M_i splits D, the local global principle (Theorem 4.11) (v) says that there is a splitting field M of D with M Galois over F and $\mathcal{G}(M/F) \cong \mathbf{Z}/p^{n-1}\mathbf{Z} \oplus (\mathbf{Z}/p\mathbf{Z})^{m-1}$. Thus M is a maximal subfield of $M_{p^{n-2}}(D)$, which must therefore be a crossed product.

Suppose $M_{p^{n-2}}(D) \cong C_1 \otimes_F C_2 \otimes_F \cdots \otimes_F C_t$, with each C_i a cyclic algebra. Let N be a compositum of t maximal subfields cyclic over F, one from each C_i. Then $\mathcal{G}(N/F)$ is an abelian p-group, and $t \geqslant \operatorname{rank}(\mathcal{G}(N/F)) \geqslant \operatorname{rank} \mathcal{G}(N \cdot L_2/L_2) \geqslant m$; the last inequality comes from Lemma 5.3 as $N \cdot L_2$ splits $A_2 \otimes_F L_2$. However, at least one of the C_i has exponent (hence index) at least $\exp(D) = p^n$. Thus, $\dim_F(C_1 \otimes_F \cdots \otimes_F C_t) \geqslant (p^n \cdot p^{m-1})^2 > \dim_F M_{p^{n-2}}(D)$, and this contradiction finishes (iii).

For (iv) note that $A_\omega(x_1, y_2^{p^{n-1}}; F)$ and $A_\omega(y_1, x_2; F)$ are split, by Theorem 5.1(iii), since the argument of Lemma 5.3 shows that they are each split by L_1 and by L_2. Also, in $\operatorname{Br}_p(F)$, $[A_\omega(y_1, y_2^{p^{n-1}}; F)] = [A_\rho(y_1, y_2; F)]$ by [**R**, p. 262, Theorem 30.10] as $\rho = \omega^{p^{n-1}}$. Thus, in $\operatorname{Br}_p(F)$, D is similar to $A_1 \otimes_F A_2$ which is similar to

$$A_\omega\left(x_1y_1, x_2y_2^{p^{n-1}}; F\right) \otimes_F A_\rho(y_3, y_4; F) \otimes_F \cdots \otimes_F A_\rho(y_{2m-1}, y_{2m}; F).$$

This yields (iv), completing the proof of the theorem. □

REMARKS 5.5. (i) In case $m = n$ we can see that D is not a crossed product using the valuation theory in §2 without invoking the cohomological machinery in §3. (Indeed, §3 is needed only for working with matrix algebras in proving Theorem 5.4(ii), (iii).) For, suppose K is a maximal subfield of D with K Galois over F. Let $G = \mathcal{G}(K/F)$. Because $D \otimes_F L_i \cong A_i \otimes_F L_i$ is a division algebra by Lemma 5.3 and Example 2.7, K is linearly disjoint to L_i over F, so that $G \cong \mathcal{G}(K \cdot L_i/L_i)$. By 2.7, $\mathcal{G}(K \cdot L_i/L_i)$ is isomorphic to a subgroup of $\Gamma_{A_i \otimes_F L_i}/\Gamma_{L_i}$; but this group is $(\mathbf{Z}/p^m\mathbf{Z})^2$ if $i = 1$ and $(\mathbf{Z}/p\mathbf{Z})^{2m}$ if $i = 2$. Clearly these two groups have no common subgroup of order p^m, as $m \geqslant 3$, so D cannot be a crossed product.

(ii) An explicit example (for any $m \geqslant n \geqslant 3$) of a maximal subfield of D is given by $K = F(\alpha_1, \alpha_2, \ldots, \alpha_m)$, where

$$\alpha_1 = \sqrt[p]{(x_1 + y_{2m})^{p-1} x_1 y_{2m}},$$

$$\alpha_j = \sqrt[p]{(\alpha_{j-1} + y_{2(m-j+1)})^{p-1} \alpha_{j-1} y_{2(m-j+1)}}, \qquad j = 2, 3, \ldots, m.$$

One can check that $K \cdot L_1 = L_1(x_1^{1/p^m})$ and $K \cdot L_2 = L_2(y_2^{1/p}, y_4^{1/p}, \ldots, y_{2m}^{1/p})$. Since $K \cdot L_i$ ($\cong K \otimes_F L_i$) splits A_i, hence D, Theorem 4.11(iv) shows K splits D. This gives a more concrete verification of the index of D and of (v) of the theorem.

(iii) We have focussed here on a single prime p. But if we take the L_i to be strict Henselizations of (F_0, v_i) (not just strict p-Henselizations) and assume k has enough roots of unity, it is clear that we can find over $F = L_1 \cap L_2$ noncrossed products D_q of index q^m and exponent q^n $(m \geqslant n \geqslant 3)$ for every prime $q \neq \operatorname{char} k$. It can be shown that $M_t(D_q)$ is a crossed product iff $q^{n-2} | t$. Furthermore, noncrossed products of composite index can be constructed over such an F.

REMARK 5.6. When $m > n$ the noncrossed product D of Theorem 5.4 is decomposable—one can check that $D \cong D_0 \otimes_F D_1 \otimes_F \cdots \otimes_F D_{m-n}$, where D_0 is a noncrossed product of exponent and index p^n, while $D_1, \ldots, D_{m-n}$ are cyclic of exponent and index p. However, the methods used in constructing D can also be applied to obtain examples of indecomposable division algebras with index exceeding the exponent. Here is a sketch for the case index $= p^4$, exponent $= p^3$ (which is inspired by the examples in [**Sa**$_3$, §2]): Construct fields and valuations (L_1, v_1), (L_2, v_2) and $F = L_1 \cap L_2$ exactly as at the beginning of this section except with four x_i instead of two and four y_i. Let ω_j be a primitive p^jth root of unity in F, $j = 1, 2, 3$, let

$$A_1 = A_{\omega_3}(x_1, x_2; F) \otimes_F A_{\omega_1}(x_3, x_4; F),$$

$$A_2 = A_{\omega_2}(y_1, y_2; F) \otimes_F A_{\omega_2}(y_3, y_4; F),$$

and let D be the underlying division algebra of $A_1 \otimes_F A_2$. One checks as in Lemma 5.3 and Theorem 5.4 that $\operatorname{index}(D) = p^4$, $\exp(D) = p^3$, and that $D_i := D \otimes_F L_i \cong A_i \otimes_F L_i$, $i = 1, 2$. Furthermore, by Corollary 2.6 the valuation v_i on L_i extends to D_i, so D_i is a division algebra totally ramified over L_i, and $\Gamma_{D_1}/\Gamma_{L_1} \cong (\mathbf{Z}/p^3\mathbf{Z})^2 \times (\mathbf{Z}/p\mathbf{Z})^2$ and $\Gamma_{D_2}/\Gamma_{L_2} \cong (\mathbf{Z}/p^2\mathbf{Z})^4$. Suppose $D_i = D_\alpha \otimes_{L_i} D_\beta$. We claim that $\Gamma_{D_\alpha} \cap \Gamma_{D_\beta} = \Gamma_{L_i}$. For, otherwise $(\Gamma_{D_\alpha} \cap \Gamma_{D_\beta})/\Gamma_{L_i}$ would have a nontrivial cyclic subgroup H, and D_α and D_β would each contain a copy of the unique totally ramified field extension K of L_i with $\Gamma_K/\Gamma_{L_i} = H$. But then $D_\alpha \otimes_F D_\beta$ would have zero divisors, contradicting the fact that D_i is a division algebra. This shows that $\Gamma_{D_i}/\Gamma_{L_i} = (\Gamma_{D_\alpha}/\Gamma_{L_i}) \times (\Gamma_{D_\beta}/\Gamma_{L_i})$. Note also that the invariant factors of the finite abelian groups $\Gamma_{D_\gamma}/\Gamma_{L_i}$ occur with even multiplicity, $\gamma = \alpha, \beta$. (For this "local" information, proofs will appear in [**W**$_2$].) Thus, in a nontrivial decomposition of D_1 one of the tensor factors has index p^3 and the other has index p; likewise in a decomposition of D_2 each factor has index p^2. Since the decompositions of D_1 and D_2 are incompatible, D must be indecomposable. This D is a crossed product, since by Theorem 4.11(v) it is split by a Galois extension M of F with $\mathcal{G}(M/F) \cong (\mathbf{Z}/p^2\mathbf{Z}) \times (\mathbf{Z}/p\mathbf{Z})^2$. However, with suitable modifications in the construction, by using three valuations, one can obtain examples of noncrossed product division algebras which are indecomposable of degree p^m and exponent p^n for any of the p^m and p^n given in Saltman's theorem [**Sa**$_3$, p. 811, Theorem 2.6].

6. Noncrossed products of exponent p^2. We will now show that our basic method can be used to construct noncrossed product division algebras of exponent p^2 $(p \neq 2)$ and index p^m for any $m \geqslant 2$. The construction is more delicate than the one in §5, as we must work with a field F not containing pth roots of unity, and must take care to control what happens when μ_p is adjoined to F. (We need to

assure that the local global principles of Theorem 4.11 apply to $F(\mu_p)$, even though they do not apply directly to F itself.) It is still an open question whether there exists a noncrossed product division algebra of index p^2 over a field containing μ_p.

We now fix a prime $p \neq 2$ and an integer $m \geqslant 2$. Fix also a field k, $\operatorname{char} k \neq p$, satisfying

$$\begin{aligned} &\text{(i)} \quad \left[k(\mu_p): k\right] = 2; \\ &\text{(ii)} \quad k \text{ has } m+1 \text{ linearly disjoint cyclic Galois extensions} \\ &\qquad \mathscr{L}, \mathscr{L}_1, \mathscr{L}_2, \ldots, \mathscr{L}_m, \text{ with } [\mathscr{L}: k] = p^2 \text{ and } \left[\mathscr{L}_j : k\right] = p, \\ &\qquad j = 1, 2, \ldots, m. \end{aligned} \tag{6.1}$$

For example, one could set $k_1 = \mathbf{R}(w_1, \ldots, w_{p^2}, z_{ij}, 1 \leqslant i \leqslant p, 1 \leqslant j \leqslant p)$ where all the w_i and z_{ij} are algebraically independent over the real numbers $\mathbf{R}$; then let k be the fixed field of the group $\mathbf{Z}/p^2\mathbf{Z} \times (\mathbf{Z}/p\mathbf{Z})^m$ acting on k_1 by permuting the indeterminates, cf. [**Ri**, §2]. Fields k satisfying (6.1) exist in characteristic 0 and in those prime characteristics $q \neq p$ such that the order of the residue of q in the multiplicative group of the ring $\mathbf{Z}/p\mathbf{Z}$ is even.

Let $F_0 = k(x_1, \ldots, x_m, y_1, \ldots, y_m)$, where $x_1, \ldots, x_m, y_1, \ldots, y_m$ are algebraically independent over k. Let v_1 be the valuation on F_0 as described in Example 2.7, viewing $F_0 = K(x_1, \ldots, x_m)$, where $K = k(y_1, \ldots, y_m)$. So, the value group of (F_0, v_1) is $(\mathbf{Z})^m$ ordered lexicographically and $v_1(x_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$ (the 1 in the ith position) while $v_1(y_i) = 0$, all i. The residue field $\overline{F_{0v_1}}$ is $k(\bar{y}_1, \ldots, \bar{y}_m)$ (where $\bar{y}_i$ is the image of y_i), which is isomorphic to $k(y_1, \ldots, y_m)$. Let v_2 be the same type of valuation on F_0 but with the x_i and y_i interchanged. So, $\Gamma_{F_0, v_2} = (\mathbf{Z})^m$, $v_2(y_i) = (0, \ldots, 0, 1, 0, \ldots, 0)$ (the 1 in the ith position) while $v_2(x_i) = 0$, and $\overline{F_{0v_2}} = k(\bar{x}_1, \ldots, \bar{x}_m) \cong k(x_1, \ldots, x_m)$. It is easy to see that v_1 and v_2 are independent valuations. Next set

$$F_1 = F_0\left(\sqrt[p^2]{x_1 + y_1}, \sqrt[p]{x_2 + y_2}, \ldots, \sqrt[p]{x_m + y_m}\right).$$

Any extension of v_1 to F_1 has residue field containing $k(\bar{y}_1^{1/p^2}, \bar{y}_2^{1/p}, \ldots, \bar{y}_m^{1/p})$, an extension of $\overline{F_{0v_1}}$ of degree p^{m+1}. From the fundamental inequality $\Sigma e_i f_i \leqslant [F_1 : F_0] = p^{m+1}$ we see that v_1 has a unique extension (also called v_1) to F_1 which is inertial, hence unramified, with residue field $k(\bar{y}_1^{1/p^2}, \bar{y}_2^{1/p}, \ldots, \bar{y}_m^{1/p})$. Likewise v_2 has a unique inertial extension to F_1, with residue field $F_0(\bar{x}_1^{1/p^2}, \bar{x}_2^{1/p}, \ldots, \bar{x}_m^{1/p})$.

Now, let F be an algebraic extension of F_1 which is maximal with respect to the property that both valuations v_1 and v_2 have immediate extensions from F_1 to F; these valuations on F are again denoted v_1 and v_2. The existence of such an F follows by Zorn's lemma. This F is the field over which our example will be constructed. Within the pth root closure $\tilde{F}_p$ of F let (L_i, v_i) be a pth root Henselization of (F, v_i), $i = 1, 2$, as described in §1. Since $F \subseteq L_1 \cap L_2$ and each v_i has an immediate extension to $L_1 \cap L_2$, the definition of F guarantees that $F = L_1 \cap L_2$.

Let $F' = F(\mu_p)$ and $L_i' = L_i(\mu_p)$, $i = 1, 2$. Note that $[F' : F] = [L_i' : L_i] = 2$ by (6.1)(i) since the residue fields of the L_i are purely transcendental over k. Furthermore v_i has a unique inertial extension from L_i to L_i' and from F to F', $i = 1, 2$.

The goal of the next few lemmas is to prove that $F' = L_1' \cap L_2'$, so that the machinery of §4 can be invoked. The notation defined thus far will be held fixed throughout this section.

LEMMA 6.2. $F \cap L_1^p \cap L_2^p = F^p$.

PROOF. Take any $a \in F \cap L_1^p \cap L_2^p$, and suppose $a \notin F^p$. Pick $\alpha_i \in L_i$ with $\alpha_i^p = a$, $i = 1, 2$. The pth root Henselization (L_i, v_i) is an immediate extension of (F, v_i), so $v_i|_{F(\alpha_i)}$ is an immediate extension of (F, v_i) to $F(\alpha_i)$. Now, the polynomial $X^p - a \in F[X]$ is irreducible since it has no roots in F and p is prime (cf. [**K**, p. 62]). Therefore, $F(\alpha_1) \cong F(\alpha_2)$. Hence both v_1 and v_2 have immediate extensions to $F(\alpha_1)$, contradicting the maximality of F. Thus, we must have $a \in F^p$. □

LEMMA 6.3. *Pick any $\tau_i \in G_p(L_i) = \mathcal{G}(\tilde{F}_p/L_i)$ such that τ_i restricts to the nontrivial L_i-automorphism of $L_i' = L_i(\mu_p)$. Take any $b \in F' \cap L_1'^p \cap L_2'^p$ and any $\beta \in L_1' \cap L_2'$ with $\beta^p = b$. Then $\tau_1(\beta) = \tau_2(\beta)$.*

PROOF. We have $\beta\tau_i(\beta) = N_{L_i'/L_i}(\beta) \in L_i$, $i = 1, 2$. Thus, $(\beta\tau_i(\beta))^p = b\tau_i(b) = N_{F'/F}(b) \in F \cap L_1^p \cap L_2^p$. The preceding lemma says there is a $c \in F$ with $c^p = (\beta\tau_i(\beta))^p$; then $\beta\tau_i(\beta) = \omega_i c$ for some $\omega_i \in \mu_p$, $i = 1, 2$. So $\omega_i = \beta\tau_i(\beta)c^{-1} \in L_i$. Since $L_i(\mu_p) \neq L_i$ we must have $\omega_1 = \omega_2 = 1$. Therefore, $\tau_1(\beta) = c\beta^{-1} = \tau_2(\beta)$, as desired. □

LEMMA 6.4. *Let G be a profinite group which is generated topologically by closed subgroups G_1 and G_2. Let H be an open subgroup of G with $|G:H| = |G_1 : G_1 \cap H| = |G_2 : G_2 \cap H| = 2$. If $\tau_i \in G_i - H$, then H is generated topologically by its closed subgroups $G_1 \cap H$, $G_2 \cap H$, and $\langle \tau_1\tau_2^{-1} \rangle$.*

PROOF. Let H_0 be the closed subgroup of H generated topologically by $G_1 \cap H$ and $G_2 \cap H$ and by $\langle \tau_1\tau_2^{-1} \rangle$ (which is the closed subgroup of H generated by $\tau_1\tau_2^{-1}$). We must show that $H_0 = H$. Assume first that G is finite. Then, as G is generated by G_1 and G_2 we may express any $h \in H$ as $h = r_1 s_1 r_2 s_2 \cdots r_n s_n$, with $r_1, \ldots, r_n \in G_1$ and $s_1, \ldots, s_n \in G_2$. We show by induction on n that $h \in H_0$. For $n = 1$, if $r_1 \in H$, then also $s_1 \in H$, so $r_1 s_1 \in H_0$. If $r_1 \notin H$, then $s_1 \notin H$, so that $r_1\tau_1^{-1} \in G_1 \cap H$, $\tau_2 s_1 \in G_2 \cap H$, and $h = (r_1\tau_1^{-1})(\tau_1\tau_2^{-1})(\tau_2 s_1) \in H_0$. Now assume $n > 1$. If $r_1 s_1 \in H$, then $r_1 s_1 \in H_0$ and $r_2 s_2 \cdots r_n s_n \in H_0$ by induction, and we are done. If $r_1 s_1 \notin H$, then $r_1(s_1\tau_2^{-1}) \in H$ and $(\tau_1 r_2) s_2 r_3 s_3 \cdots r_n s_n \in H$. By induction both these terms lie in H_0, whence $h = (r_1 s_1 \tau_2^{-1})(\tau_2\tau_1^{-1})(\tau_1 r_2 s_2 \cdots r_n s_n) \in H_0$. This proves the lemma if G is finite.

Now drop the assumption that G is finite. If $H_0 \neq H$, then $H - H_0$ is a nonempty open subset of H. Since a base of open sets of H is given by cosets of open normal subgroups of H, there is an $h \in H$ and an open normal subgroup U of H with $hU \cap H_0 = \varnothing$. We may assume that U is actually normal in G (replacing U if necessary by the finite intersection of conjugates of U). Because U is open, $|G:U| < \infty$. Let $\pi\colon G \to G/U$ be the canonical projection. It is easy to check that the hypotheses relating G, G_1, G_2, H, τ_1, τ_2 all carry over to $\pi(G)$, $\pi(G_1)$, $\pi(G_2)$, $\pi(H)$, $\pi(\tau_1)$, $\pi(\tau_2)$. Clearly $\pi(H_0)$ contains the subgroup of $\pi(H)$ generated by

$\pi(H) \cap \pi(G_1)$, $\pi(H) \cap \pi(G_2)$, and $\langle \pi(\tau_1)\pi(\tau_2)^{-1} \rangle$. But $\pi(h) \in \pi(H) - \pi(H_0)$ which contradicts the finite case of the lemma proved above. Thus, $H_0 = H$, and the lemma is proved in general. □

LEMMA 6.5. *$F' \cap L_1'^p \cap L_2'^p = F'^p$. Consequently, $F' = L_1' \cap L_2'$, $G_p(F') = G_p(L_1') *_p G_p(L_2')$, and the local global principles of Theorem 4.11 hold from L_1' and L_2' to F'.*

PROOF. We have $F \subseteq L_i \subseteq \tilde{F}_p$, $i = 1, 2$, and $F = L_1 \cap L_2$. So, $G_p(F) = \mathcal{G}(\tilde{F}_p/F)$ is generated topologically by its closed subgroups $G_p(L_1)$ and $G_p(L_2)$. We have $|G_p(F) : G_p(F')| = [F' : F] = 2$ and $G_p(F') \cap G_p(L_i) = G_p(L_i')$, which has index 2 in $G_p(L_i)$. Thus, Lemma 6.4 says $G_p(F')$ is generated topologically by $G_p(L_1')$, $G_p(L_2')$, and $\overline{\langle \tau_1\tau_2^{-1} \rangle}$ for any $\tau_i \in G_p(L_i)$ which restricts to the nontrivial L_i-automorphism of L_i'.

Now pick any $b \in F' \cap L_1'^p \cap L_2'^p$, and any $\beta \in \tilde{F}_p$ with $\beta^p = b$. Let $N = G_p(F'(\beta))$, a closed subgroup of $G_p(F')$. Since L_i' contains one, hence all pth roots of b, $\beta \in L_i'$, so $G_p(L_i') \subseteq N$, $i = 1, 2$. But Lemma 6.3 shows $\tau_1\tau_2^{-1} \in N$ also. Since a topological generating set of $G_p(F')$ lies in N, $N = G_p(F')$ which shows that $\beta \in F'$. Thus $F' \cap L_1'^p \cap L_2'^p = F'^p$.

Since $F' \subseteq L_1' \cap L_2' \subseteq \tilde{F}_p$, $L_1' \cap L_2'$ is obtainable from F' by successive adjunctions of pth roots (cf. (1.4)). Thus, the equality proved in the previous paragraph implies $F' = L_1' \cap L_2'$. Because L_i is a pth root Henselization of (F, v_i), the unique extension of v_i to L_i' is p-Henselian and is an immediate extension of (F', v_i). Also, v_1 and v_2 are independent valuations on F' since they are independent on F_0 and F' is algebraic over F_0. Therefore, Theorem 4.3 shows that $G_p(F') = G_p(L_1') *_p G_p(L_2')$, completing the proof. □

For each i the residue field $\overline{F_{v_i}}$ of F with respect to v_i is the same as that of F_1; so $\overline{F_{v_i}}$ is a purely transcendental extension of our original ground field k. Hence, for the fields $\mathcal{L}$, $\mathcal{L}_1$, $\mathcal{L}_2, \ldots, \mathcal{L}_m$ posited in (6.1)(ii), the valuation v_i on F has a unique inertial extension to $\mathcal{L} \cdot F$ (resp. to each $\mathcal{L}_j \cdot F$) with residue field $\mathcal{L} \cdot \overline{F_{v_i}}$ (resp $\mathcal{L}_j \cdot \overline{F_{v_i}}$). So, $\mathcal{L} \cdot F$, $\mathcal{L}_1 \cdot F, \ldots, \mathcal{L}_m \cdot F$ are linearly disjoint cyclic Galois extensions of F. We fix a generator σ of $\mathcal{G}(\mathcal{L} \cdot F/F) \cong \mathbf{Z}/p^2\mathbf{Z}$, and generators σ_j of $\mathcal{G}(\mathcal{L}_j \cdot F/F) \cong \mathbf{Z}/p\mathbf{Z}$, $j = 1, 2, \ldots, m$. Using the cyclic algebra notation described in §1 we set

$$A_1 := A(\mathcal{L} \cdot F/F, \sigma, x_1) \quad \text{and} \quad A_2 := \bigotimes_{j=1}^{m}{}_F \; A(\mathcal{L}_j \cdot F/F, \sigma_j, y_j).$$

The underlying division algebra D of $A_1 \otimes_F A_2$ will provide the counterexample of this section. We first consider the local properties of the A_i.

LEMMA 6.6. (i) *$A_1 \otimes_F L_1$ is a division algebra of index and exponent p^2, while L_2 splits A_1.*

(ii) *$A_2 \otimes_F L_2$ is a division algebra of index p^m and exponent p, while L_1 splits A_2.*

(iii) *$A_i \otimes_F L_i'$ has the same index and exponent as $A_i \otimes_F L_i$, $i = 1, 2$.*

PROOF. (i) Since (L_1, v_1) has the same residue field as (F, v_1), the same argument as given just above shows v_1 has a unique inertial (hence unramified) extension to $\mathscr{L}\cdot L_1$; so $\mathscr{L}\cdot F$ and L_1 are linearly disjoint over F. Hence, $\mathscr{G}(\mathscr{L}\cdot L_1/L_1) \cong \mathscr{G}(\mathscr{L}\cdot F/F) \cong \mathbf{Z}/p^2\mathbf{Z}$ and $A_1 \otimes_F L_1 \cong A(\mathscr{L}\cdot L_1/L_1, \sigma, x_1)$. Since $v_1(x_1) = (1, 0, \ldots, 0)$ in the value group Γ_{L_1} of L_1, the image of $v_1(x_1)$ in $\Gamma_{L_1}/p^2\Gamma_{L_1}$ has order p^2. Therefore, Corollary 2.9 with $k = 1$ and $n_1 = l = p^2$ shows that $A_1 \otimes_F L_1$ is a valued division algebra; its index is clearly p^2. Because v_1 extends uniquely to $\mathscr{L}\cdot L_1$ without ramification, v_1 maps the norm group $N_{\mathscr{L}\cdot L_1/L_1}(\mathscr{L}\cdot L_1^*)$ into $p^2\Gamma_{L_1}$. Thus, x_1^r cannot be a norm from $\mathscr{L}\cdot L_1$ to L_1 for $1 \leqslant r < p^2$; this shows that $A_1 \otimes_F L_1$ has exponent p^2 by [**R**, p. 261, Corollary 30.7].

Now consider $A_1 \otimes_F L_2$. We have again that $\mathscr{L}\cdot F$ is linearly disjoint to L_2 over F, so $A_1 \otimes_F L_2 \cong A(\mathscr{L}\cdot L_2/L_2, \sigma, x_1)$. But $\bar{x}_1$ has a p^2-root in $\bar{L}_2$. Thus, the polynomial $f(X) = X^{p^2} - x_1 \in V_{L_2}[X]$, which splits over $\tilde{F}_p$, has image $\bar{f}$ in $\bar{L}_2[X]$ with a nonrepeated linear factor. Because (L_2, v_2) is pth root Henselian, f must have a linear factor in $V_{L_2}[X]$, i.e., x_1 has a p^2-root in L_2. Therefore, x_1 lies in the norm group $N_{\mathscr{L}\cdot L_2/L_2}(\mathscr{L}\cdot L_2^*)$, which shows that $A_1 \otimes_F L_2$ is split.

(ii) As in (i), but with the valuations reversed, we see that v_2 has a unique inertial extension to $\mathscr{L}_j \cdot L_2$ for $j = 1, 2, \ldots, m$, with residue field $\mathscr{L}_j \cdot \bar{L}_2$. Hence, $A(\mathscr{L}_j \cdot F/F, \sigma_j, y_j) \otimes_F L_2 \cong A(\mathscr{L}_j \cdot L_2/L_2, \sigma_j, y_j)$. Corollary 2.9 applies to the tensor product of these algebras with $k = m$, $n_1 = n_2 = \cdots = n_k = l = p$, showing that $A_2 \otimes_F L_2 \cong \otimes_{j=1}^m A(\mathscr{L}_j \cdot L_2/L_2, \sigma_j, y_j)$ is a valued division algebra with residue ring $\mathscr{L}_1 \cdot \cdots \cdot \mathscr{L}_m \cdot \bar{L}_2$. Clearly the exponent of $A_2 \otimes_F L_2$ is p and the index is p^m. Switching to L_1 we find that $A_2 \otimes_F L_1 \cong \otimes_{j=1}^m A(\mathscr{L}_j \cdot L_1/L_1, \sigma_j, y_j)$. But as each $\bar{y}_j$ has a pth root in $\bar{L}_1$ an argument like that in (i) shows that each y_j has a pth root in L_1. Hence, L_1 splits A_2 as it splits each of the cyclic factors.

(iii) The same arguments just given for $A_i \otimes_F L_i$ apply to $A_i \otimes_F L_i'$. Alternatively, note that $[L_i' : L_i] = [L_i(\mu_p) : L_i] = 2$. Hence, the index reduction formula [**P**, p. 243] shows that for any central simple L_i-algebra B of odd index, $\operatorname{index}(B \otimes_{L_i} L_i') = \operatorname{index}(B)$. So, in particular, the map $\operatorname{Br}_p(L_i) \to \operatorname{Br}_p(L_i')$ is injective. □

Let $A = A_1 \otimes_F A_2$ with the A_i as defined before Lemma 6.6 and the F defined at the beginning of §6. Write $A \cong M_l(D)$, where D is an F-central division algebra.

THEOREM 6.7. *The division algebra D just defined has index p^m and exponent p^2. D is not a crossed product. The $F(\mu_p)$-division algebra $D \otimes_F F(\mu_p)$, with the same index and exponent as D, is a crossed product.*

PROOF. Observe that Lemma 6.6 shows that $[D \otimes_F L_i] = [A_i \otimes_F L_i]$ in $\operatorname{Br}_p(L_i)$ and $[D \otimes_F L_i'] = [A_i \otimes_F L_i']$ in $\operatorname{Br}_p(L_i')$. The construction of the A_i shows that $\exp(D) | p^2$. Then $\exp(D) = p^2$ since $\exp(D \otimes_F L_1) = p^2$ by Lemma 6.6(i). Hence, $\operatorname{index}(D) = p^s$ for some $s \geqslant 2$. By the index reduction formula [**P**, p. 243], $\operatorname{index}(D) = \operatorname{index}(D \otimes_F F')$ as $[F' : F] = 2$ is prime to p. We compute the index of $D \otimes_F F'$ using the local global principles of Theorem 4.11. Since $A_i \otimes_F L_i'$ is a crossed product division algebra, $\operatorname{index}(A_i \otimes_F L_i') = p\text{-ind}(A_i \otimes_F L_i')$. Therefore, by Lemmas 6.6(iii) and 6.5, and Theorem 4.11(ii), (iii),

$$p^m = \max\{\text{index}(A_i \otimes_F L_i') | i = 1,2\} = \max\{\text{index}(D \otimes_F L_i') | i = 1,2\}$$
$$= \text{index}(D \otimes_F F') = \text{index}(D).$$

By comparing indices we see that $D \otimes_F L_2 \cong A_2 \otimes_F L_2$.

Suppose D is a crossed product. Then there exists a maximal subfield K of D with $[K\colon F] = p^m$ and K Galois over F. Let $K_i = K \cdot L_i$, $i = 1, 2$. Then each K_i is Galois over L_i, and we view $\mathcal{G}(K_i/L_i) \subseteq \mathcal{G}(K/L)$ by restriction. In particular, $[K_i\colon L_i]$ is a power of p. Since (L_i, v_i) is p-Henselian, v_i has a unique extension to a valuation of K_i. According to Corollary 2.4, K_i is an inertial extension of L_i with $\mathcal{G}(K_i/L_i) \cong \mathcal{G}(\bar{K}_i/\bar{L}_i)$, $i = 1, 2$.

Since $D \otimes_F L_2 \cong A_2 \otimes_F L_2$ is a division algebra, $K_2 \cong K \otimes_F L_2$, which is isomorphic to a maximal subfield K_3 of $A_2 \otimes_F L_2$. Hence $[K_3\colon L_2] = p^m$ and $\mathcal{G}(K/F) \cong \mathcal{G}(K_3/L_2) \cong \mathcal{G}(\bar{K}_3/\bar{L}_2)$. As we saw in proving Lemma 6.6(ii) $A_2 \otimes_F L_2$ is a valued division algebra with residue ring $\mathcal{L}_1 \cdot \cdots \cdot \mathcal{L}_m \cdot \bar{L}_2$. Thus $\bar{K}_3 \subseteq \mathcal{L}_1 \cdot \cdots \cdot \mathcal{L}_m \cdot \bar{L}_2$, and equality must hold by comparing degrees over $\bar{L}_2$. Since each $\mathcal{L}_i$ was a cyclic extension of k of degree p, $\mathcal{G}(\bar{K}_3/\bar{L}_2) \cong (\mathbf{Z}/p\mathbf{Z})^m$. Putting these isomorphisms together, we have $\mathcal{G}(K/F) \cong (\mathbf{Z}/p\mathbf{Z})^m$. Hence, the subgroup $\mathcal{G}(K_1/L_1)$ is elementary abelian.

Recall now from the proof of Lemma 6.6 that $A_1 \otimes_F L_1 \cong A(\mathcal{L} \cdot L_1/L_1, \sigma, x_1)$, where $\mathcal{L} \cdot L_1$ is a cyclic Galois and inertial extension of L_1 with $\mathcal{G}(\mathcal{L} \cdot L_1/L_1) \cong \mathbf{Z}/p^2\mathbf{Z}$. Because $\mathcal{G}(K_1/L_1)$ is elementary abelian, $\mathcal{L} \cdot L_1 \not\subseteq K_1$. Therefore, $\mathcal{L} \cdot K_1$, which is a cyclic Galois extension of K_1, has degree p or p^2 over K_1. By [**R**, p. 261, Theorem 30.8], $A_1 \otimes_F K_1$ is similar to $A(\mathcal{L} \cdot K_1/K_1, \tau, x_1)$ in $\text{Br}(K_1)$, where $\tau = \sigma$ if $[\mathcal{L} \cdot K_1\colon K_1] = p^2$ and $\tau = \sigma^p$ if $[\mathcal{L} \cdot K_1\colon K_1] = p$. In either case, $\mathcal{L} \cdot K_1$ is an inertial extension of K_1 by Corollary 2.4. ($\mu_p \not\subseteq K_1$, as $[K_1\colon L_1]$ is a power of p.) Therefore, since K_1 has the same value group as L_1 and $v_1(x_1) = (1, 0, \ldots, 0)$ we see from Corollary 2.9 with $k = 1$ and $l = n_1 = p^2$ or p that $A(\mathcal{L} \cdot K_1/K_1, \tau, x_1)$ is a division algebra of index p^2 or p. So, K_1 does not split A_1. Since $[A_1 \otimes_F L_1] = [D \otimes_F L_1]$ in $\text{Br}_p(L_1)$, K_1 cannot split D. But K_1 contains the maximal subfield K of D. This contradiction shows D cannot be a crossed product.

To see that $D \otimes_F F'$ is a crossed product, where $F' = F(\mu_p)$, we first work locally. We have $\mathcal{L} \cdot L_1'$ is cyclic Galois over L_1'. Hence by Kummer theory there is a cyclic subextension $L_1'(\sqrt[p]{l})$ of degree p over L_1'. By [**R**, p. 261, Theorem 30.8], $A_1 \otimes_F L'(\sqrt[p]{l})$ is similar to $A(\mathcal{L} \cdot L_1'(\sqrt[p]{l})/L_1'(\sqrt[p]{l}), \sigma^p, x_1)$ in $\text{Br}_p(L_1'(\sqrt[p]{l}))$, and this algebra is split by $M_1 := L_1'(\sqrt[p]{l}, \sqrt[p]{x_1})$. Invoking Lemma 6.6(i) we see that D is split by M_1. But A_2, and hence D, is split by $M_2 := L_2'(\sqrt[p]{y_1}, \ldots, \sqrt[p]{y_m})$. Each M_i is Galois over L_i' and $\mathcal{G}(M_1/L_1') \cong (\mathbf{Z}/p\mathbf{Z})^2$ while $\mathcal{G}(M_2/L_2') \cong (\mathbf{Z}/p\mathbf{Z})^m$. By Lemma 6.5 and the local global principle Theorem 4.11(v) there is a field M Galois over F' such that M splits D and $\mathcal{G}(M/F') \cong (\mathbf{Z}/p\mathbf{Z})^m$. By dimension count M is a maximal subfield of $D \otimes_F F'$; hence $D \otimes_F F'$ is a crossed product. □

REMARK 6.8. One can show that the p-index of D, as defined in §4, is p^m, the same as its index.

REFERENCES

[**Am**] S. A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972), 408–420.

[**AEJ**] J. Kr. Arason, R. Elman and B. Jacob, *The graded Witt ring and Galois cohomology*. I, Quadratic and Hermitian Forms (C. Riehm and I. Hambleton, eds.), Canad. Math. Soc. Conf. Proc., Vol. 4, Amer. Math. Soc., Providence, R.I., 1984, pp. 17–50.

[**BNW**] E. Binz, J. Neukirch and G. H. Wenzel, *A subgroup theorem for free products of pro-finite groups*, J. Algebra **19** (1971), 104–109.

[$\mathbf{Bo}_1$] N. Bourbaki, *Algèbre commutative*, Chapter I, *Modules plats*, Hermann, Paris, 1961.

[$\mathbf{Bo}_2$] _____, *Algèbre commutative*, Chapter VI, *Valuations*, Hermann, Paris, 1964.

[**Br**] L. Bröcker, *Characterization of fans and hereditarily Pythagorean fields*, Math. Z. **151** (1976), 149–163.

[**CF**] J. W. S. Cassels and A. Fröhlich, eds., *Algebraic number theory*, Academic Press, London, 1967.

[**E**] O. Endler, *Valuation theory*, Springer-Verlag, New York, 1972.

[**Er**] Ju. L. Ershov, *Semilocal fields*, Soviet Math. Dokl. **15** (1974), 424–428.

[**HS**] P. J. Hilton and U. Stammbach, *A course in homological algebra*, Springer-Verlag, New York, 1971.

[**J**] B. Jacob, *On the structure of Pythagorean fields*, J. Algebra **68** (1981), 247–267.

[**Ja**] N. Jacobson, *P.I.-algebras: An introduction*, Lecture Notes in Math., vol. 441, Springer-Verlag, New York, 1975.

[**K**] I. Kaplansky, *Fields and rings*, Univ. of Chicago Press, Chicago, Ill., 1969.

[**MS**] A. S. Merkurjev and A. A. Suslin, *K-cohomology of Severi-Brauer varieties and the norm residue homomorphism*, Math. USSR Izv. **21** (1983), 307–340.

[**Mi**] J. Milnor, *Algebraic K-theory and quadratic forms*, Invent. Math. **9** (1970), 318–344.

[**N**] J. Neukirch, *Freie Produkte proendlichen Gruppen und ihre Kohomologie*, Arch. Math. **22** (1971), 337–357.

[**P**] R. S. Pierce, *Associative algebras*, Springer-Verlag, New York, 1982.

[**R**] I. Reiner, *Maximal orders*, Academic Press, London, 1975.

[**Ri**] L. Risman, *Cyclic algebras, complete fields, and crossed products*, Israel J. Math. **28** (1977), 113–128.

[**Ro**] L. H. Rowen, *Division algebra counterexamples of degree* 8, Israel J. Math. **38** (1981), 51–57.

[$\mathbf{Sa}_1$] D. Saltman, *Noncrossed products of small exponents*, Proc. Amer. Math. Soc. **68** (1978), 165–168.

[$\mathbf{Sa}_2$] _____, *Noncrossed product p-algebras and Galois p-extensions*, J. Algebra **52** (1978), 302–314.

[$\mathbf{Sa}_3$] _____, *Indecomposable division algebras*, Comm. Algebra **7** (1979), 791–817.

[**SS**] M. Schacher and L. Small, *Noncrossed products in characteristic p*, J. Algebra **24** (1973), 100–103.

[**Sch**] W. Scharlau, *Über die Brauer-Gruppe eines Henselkorpers*, Abh. Math. Sem. Univ. Hamburg **33** (1969), 243–249.

[**S**] O. F. G. Schilling, *The theory of valuations*, Math. Surveys, no. 4, Amer. Math. Soc., Providence, R. I., 1950.

[$\mathbf{Se}_1$] J.-P. Serre, *Cohomologie Galoisienne*, Lecture Notes in Math., vol. 5, Springer-Verlag, Berlin, 1965.

[$\mathbf{Se}_2$] _____, *Local fields*, Springer-Verlag, New York, 1979; English transl. of *Corps locaux*.

[**Sh**] S. Shatz, *Profinite groups, arithmetic, and geometry*, Ann. of Math. Studies, no. 67, Princeton Univ. Press, Princeton, N. J., 1974.

[**T**] J. Tate, *Relations between* K_2 *and Galois cohomology*, Invent Math. **36** (1976), 257–274.

[**Ti**] J.-P. Tignol, *Cyclic and elementary abelian subfields of Malcev-Neumann division algebras*, preprint, 1985.

[**TA**] J.-P. Tignol and S. A. Amitsur, *Totally ramified splitting fields of central simple algebras over Henselian fields*, J. Algebra (to appear).

[$\mathbf{W}_1$] A. Wadsworth, *p-Henselian fields: K-theory, Galois cohomology, and Witt rings*, Pacific J. Math. **105** (1983), 473–495.

[$\mathbf{W}_2$] _____, *Totally ramified valuations on finite dimensional division algebras* (in preparation).

[**We**] E. Weiss, *Cohomology of groups*, Academic Press, New York, 1969.

DEPARTMENT OF MATHEMATICS, OREGON STATE UNIVERSITY, CORVALLIS, OREGON 97331

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, SAN DIEGO, LA JOLLA, CALIFORNIA 92093