ISRAEL JOURNAL OF MATHEMATICS 78 (1992), 197-207

PRIME TO p EXTENSIONS OF DIVISION ALGEBRA

BY

LOUIS H. ROWEN*
Department of Mathematics, Bar-Ilan University, Ramat-Gan, Israel

AND

DAVID J. SALTMAN**
Department of Mathematics, University of Texas, Austin, Texas 78712, USA

ABSTRACT

Every division algebra of degree p^t has a prime-to-p extension which is a crossed product, iff $t \leq 2$.

Introduction

Throughout this paper we assume D is a division algebra which is finite dimensional over its center F (a field). Then it is well-known $[D : F] = n^2$ for some integer n called the **degree** of D; furthermore D is isomorphic to a tensor product $D_1 \otimes \cdots \otimes D_u$ over F where each D_i has degree $p_i^{t(i)}$ for a suitable prime p_i and suitable $t(i) \in \mathbb{N}$ (so that $n = p_1^{t(1)} \ldots p_u^{t(u)}$). In this way the structure theory of finite dimensional division algebras often is reduced to the case that the degree n is some prime power p^t, and we shall make this assumption ($n = p^t$) throughout; in particular p is a fixed prime.

Many basic theorems about division algebras have been proved by passing to $D \otimes_F L$ where $[L : F]$ is finite but not divisible by p; we shall call $D \otimes_F L$ a **prime-to-p** extension of D. For example, Albert showed that any division algebra D

* Research of the first author supported in part by the NSA/MSP Grant MDA90-H4001 while the author was on Sabbatical at Yale University
** Second author is grateful for support order NSF grant DMS-8901778
Received May 9, 1991 and in revised form March 26, 1992

of degree p has a prime-to-p extension which is cyclic; taking the corestriction Rosset proved D is similar (in the Brauer group) to a tensor product of cyclics each of degree p. Our main theorems using this technique are:

1. Every division algebra D of degree p^u, $u \geq 2$, has a prime-to-p extension which contains a tensor product of two cyclic extensions of its center (each of dimension p). In particular if $u = 2$ then D has a prime-to-p extension which is a crossed product with respect to the group $\mathbb{Z}_p \times \mathbb{Z}_p$.

2. There are examples of division algebras of degree p^u, $u \geq 3$, such that **no** prime-to-p extension is a crossed product.

3. (for p odd). There is a division algebra of degree p^2 and exponent p, every prime to p extension of which is tensor indecomposable (i.e. cannot be written as a tensor product of central subalgebras). (The referee has pointed out that for $p = 2$, the same techniques yield the analogous results in degree 8 and exponent 2.)

Each section of this paper corresponds to the respective theorem stated above.

1. The "canonical" prime-to-p extension, and crossed products

In this section we set up the standard prime-to-p extension of D (which goes back to Albert), and use it to prove theorem 1.

Suppose D is a division algebra of degree n over its center F, where n is a power of a prime number p. Let $K \supset F$ be a subfield of D which is separable over F. (There exist separable subfields of dimension n, by Koethe's theorem.) Let E be the normal closure of K, and let $G = Gal(E/K)$. Also let $[K : F] = p^u$. Then $|G| = p^v t$ for suitable $v \geq u$ and suitable t prime to p. Let H be a Sylow p-subgroup of G, and let $L = E^H$, the fixed subfield of E under H. Then $[L : F] = [E : F]/[E : L] = t$ is prime to p.

Note $L \subset E$ and $K \subset E$ so $KL \subseteq E$. But $t = [L : F]$ divides $[KL : F]$ and $p^u = [K : F]$ divides $[KL : F]$, implying $[KL : F] = p^u t$.

By Galois theory E/L is Galois with Galois group H. Let $H_1 = \mathrm{Gal}(E/KL)$. Since H is a p-group we can form a chain of subgroups

$$H_1 \subset H_2 \subset \ldots \subset H_v = H$$

with each H_i normal of index p in H_{i+1}. Thus there is a chain:

$$KL = E_0 \supset E_1 \supset E_2 \cdots \supset E_v = L$$

with each E_i/E_{i+1} Galois of degree p.

Looking at E_{v-1} we have:

PROPOSITION 1.1 (Essentially Albert [A, theorem 4.31]): *If* $\deg D = n = p^u$ *and* $K \supset F$ *is a subfield of* D *separable over* F *then there is some extension* $L \supset F$ *with* $[L : F]$ *prime to* p, *such that* KL *contains an element* a *of degree* p *over* L *with* $L(a)/L$ *Galois.*

THEOREM 1.2: *If* $p^2|\deg(D)$ *then some prime-to-p extension* $D \otimes L$ *contains a Galois field extension* $\tilde{K}$ *of* L *of dimension* p^2, *having Galois group* $\mathbb{Z}_p \times \mathbb{Z}_p$.

Proof: By Proposition 1.1 there is a prime-to-p extension L_0 of F such that $D_1 = D \otimes L_0$ contains a Galois extension $L_0(a)$ of L_0 of degree p; let σ be a nontrivial automorphism of $L_0(a)/L_0$. By the Skolem-Noether theorem there is y in D_1 for which $yay^{-1} = \sigma(a)$. Clearly y^p commutes with a, but y does not. Furthermore L_0, y, and a generate a division algebra A of degree p with center $L_0(y^p)$.

Let $D' = C_{D_1}(A)$ be the centralizer of A in D_1. Then $D' \cap L_0(a) = L_0$. (For otherwise $D' \cap L_0(a) = L_0(a)$ since $[L_0(a) : L] = p$ is prime, implying $a \in D'$ and thus commutes with y, contradiction.)

CASE 1: D' contains a proper separable extension K of L_0. Applying proposition 1.1 there is a prime-to-p extension L_1 of L_0 such that L_1K contains an element b with $L_1(b)/L_1$ Galois of dimension p. Furthermore $L_1K \cap L_1(a) = L_1$ seen by matching bases over L_0, so $L_1(b) \cap L_1(a) = L_1$; we conclude by taking $L = L_1$ and $\tilde{K} = L_1(a, b)$, which is Galois over L_1 with Galois group $\mathbb{Z}_p \times \mathbb{Z}_p$.

CASE 2: D' does not contain a proper separable field extension K of L_0, i.e., every subfield of D' is purely inseparable over L_0. Note that $\deg D' = 1$, since otherwise D' has maximal subfields separable over its center, which thus are not purely inseparable over L_0. Hence $A = C_{D_1}(L_0(y^p))$, implying $p[L_0(y^p) : L_0] = \deg D$, and thus $L_0(y)$ is a maximal subfield of D_1, purely inseparable over L_0. By [A, theorem 7.25], D_1 is cyclic. Hence by [S, theorem 1′], D_1 has a Galois field extension $\tilde{K}$ of L of dimension p^2, having Galois group $\mathbb{Z}_p \times \mathbb{Z}_p$. (In fact by the theorem quoted, any group of order $\leq \deg(D_1)$ appears as the Galois group of a suitable maximal subfield.) (We would like to thank Al Sethuraman for pointing out a gap in the original version; he has an alternate proof for this case.) ∎

COROLLARY 1.3: *If* $\deg(D) = p^2$ *then some prime-to-p extension of* D *is a crossed product.*

2. Degrees higher than p^2

In the previous section, we showed that for any division algebra D/F of degree p^2 there is a prime-to-p field extension $L \supseteq F$ such that $D \otimes_F L$ is a crossed product. Of course, if D has degree p the proof is quite easy. The purpose of this section is to show that the above results are best possible. That is, we will show:

THEOREM 2.1: *Suppose* $s \geq 2$, $r \geq 3$, F *is a field of characteristic not* p, *and* $D = UD(F, p^r, s)$ *is the generic division algebra of degree* p^r *in* s *variables over* F. *Let* $Z = Z(D)$, *the center of* D *and* $L \supseteq Z$, *an arbitrary prime-to-p extension. Then* $UD(F, p^r, s) \otimes_Z L$ *is not a crossed product.*

Although the proof of 2.1 will take a few pages, conceptually what we will do is very clear. The main idea is that even after prime-to-p extensions the argument in Amitsur's noncrossed product proof still works in the case degree p^r, $r \geq 3$. For example, assume $UD(F, p^r, s) \otimes_Z L$ is a G-crossed product (i.e. G appears as the Galois group) where $L = Z(a)$ is separable over Z, and let $f \in Z[x]$ be the minimal polynomial of a over Z. One may assume f is monic. Specializing $UD(F, p^r, s)$ to a division ring D would specialize f to a polynomial $\bar{f}$ which may be reducible, so writing $Z(D)[x]/\langle \bar{f} \rangle$ as a direct sum of fields $L_1 \oplus \cdots \oplus L_t$ we see that $D \otimes L_1, \ldots, D \otimes L_t$ each are G-crossed products. But $[L_1 \oplus \cdots \oplus L_t : F] = \sum [L_i : F] = \deg f$, so some $[L_i : F]$ is prime to p, and now the customary comparison technique can be made to work.

In order to provide a comprehensive proof including the inseparable case we turn to the techniques of Azumaya algebras. Let us begin by defining some terminology.

If $\varphi : R \to S$ is a ring homomorphism of commutative rings and M is an R-module, $M \otimes_\varphi S$ is defined as $M \otimes_R S$ where S is viewed as an R module via φ. For commutative rings $R \subseteq T$, recall (e.g. [DI, p.80]) the definition of a G-Galois extension T/R. Given such a T/R, let $c : G \times G \to T^*$ be a 2 cocycle. We can form the G-crossed product $\Delta(T/R, G, c) = \sum T u_\sigma$ where $u_\sigma t = \sigma(t) u_\sigma$ for $t \in T$ and $u_\sigma u_\tau = c(\sigma, \tau) u_{\sigma\tau}$. An algebra A/R is called a G-**crossed product** if $A \cong \Delta(T/R, G, c)$ for some T/R and c. Note that if R is a field, T need not be a field but is a direct sum $L \oplus \cdots \oplus L$ where L/R is H-Galois for some $H \subset G$. The advantage of this definition is that the class of G-crossed products is closed under base extension. For any commutative domain R, we denote its field of fractions by $Q(R)$. Finally, if A is a set, $|A|$ denotes the order of A.

Our approach, not surprisingly, is to modify Amitsur's comparison technique. First we give the consequences of assuming $UD(F,p^r,s)\otimes_Z L$ is a crossed product.

THEOREM 2.2: *Let $D = UD(F,p^r,s)$ where $s \geq 2$, and $Z = Z(D)$. Assume D has a prime-to-p extension $D \otimes_Z L$ which is a G-crossed product. If A/K is any central simple algebra of degree n, where $K \supseteq F$, then A has a prime-to-p extension $A \otimes_K K'$ which is a G-crossed product.*

Proof: Let L'' be the maximal separable subfield of L over Z. View D naturally as the ring of fractions of the ring of generic matrices $F\{Y_1,\ldots,Y_s\}$ at its center $C = Z(F\{Y_1,\ldots,Y_s\})$. Before continuing the proof we need

LEMMA 2.3: *There is $0 \neq t \in C$ and, for $C' = C(1/t)$, there is an Azumaya algebra B/C', a commutative C'-algebra S'', and a commutative S''-algebra S such that:*

1. *S'' is a finitely generated free C'-module and separable over C'.*
2. *S is a finitely generated free S''-module, and $S^q \subseteq S''$ for some power q of char(F). Of course, $S = S''$ if char$(F) = 0$.*
3. *$Q(S'') = L''$.*
4. *$Q(S) = L$.*
5. *$B \otimes_{C'} Z = D$.*
6. *$B \otimes_{C'} S$ is a G-crossed product.*

Proof: Note that properties (1) through (6) are preserved by extension of C' in Z. Also note that it suffices to find $C' \subseteq Z$ finitely generated as an algebra over C, satisfying all the above, since then $C' \subseteq C(1/t)$ for some $0 \neq t \in C$. Thus, at any stage in the argument we are free to add finitely many elements to C' as needed.

To find B/C' Azumaya with $B \otimes_{C'} Z = D$ is standard (e.g. [OS, p.135]). Suppose $L'' = Z(\alpha)$ and $f(x) \in Z[x]$ is the minimal monic polynomial of α over Z. By adding finitely many elements to C', we may assume $f(x) \in C'[x]$. Set $S'' = C'[x]/\langle f(x)\rangle$. If $e \in L'' \otimes_Z L''$ is the separating idempotent (e.g. [DI, p.40]), adding finitely many more elements to C' will insure $e \in S'' \otimes_{C'} S''$, and so S''/C' is separable. Next, suppose $L_0 = L'' \subseteq L_1 \subseteq \cdots \subseteq L_n = L$ is such that L_i/L_{i-1} has degree q_i and $L_i = L_{i-1}(\alpha_i)$ where $(\alpha_i)^{q_i} = a_i \in L_{i-1}$. Adding finitely many elements to C' will insure $a_i \in S''$ and inductively we set $S_i = S_{i-1}[x]/(x^{q_i} - a_i)$ (where $S_0 = S''$). Proceeding by induction we can set $S = S_n$.

We have assumed $D \otimes_Z L \cong \Delta(M/L, G, c)$ where M/L is G-Galois. In the same spirit as the above paragraph, we can add finitely many elements to C' so that there is a G-Galois T/S with $T \otimes_S L \cong M$ as G-Galois extensions and such that all values of $c : G \times G \to M$ are units in T (we can quote [S1, p.528] here). Forming the crossed product $\Delta(T/S, G, c)$, we obtain an isomorphism φ : $(B \otimes_{C'} S) \otimes_S L \cong \Delta(T/S, G, c) \otimes_S L$. Adjoining the final finite batch of elements to C' will insure that φ restricts to an isomorphism $B \otimes_{C'} S \cong \Delta(T/S, G, c)$. This proves the lemma. ∎

We can now complete the proof of 2.2. Suppose A/K is as given, and $C' = C(1/t)$, S'', S, B are as in the lemma. There is a $\varphi : C \to K$ such that $\varphi(t) \neq 0$, and extending φ to C', we have $B \otimes_\varphi K \cong A$. Let $K'' = S'' \otimes_\varphi K$. Then K'' is a separable K-algebra so $K'' = K_1'' \oplus \cdots \oplus K_t''$ where each K_i'' is a separable field extension of K. Let $V = S \otimes_\varphi K$. Then V is a commutative K''-algebra and $V^q \subseteq K''$. If J is the Jacobson radical of V, then $V/J \cong K_1' \oplus \cdots \oplus K_t'$ where each K_i' is a purely inseparable field extension of K_i''.

Since $B \otimes_{C'} S$ is a G-crossed product, the same holds for $A \otimes_K V$. It follows that $A \otimes_K V/J$ is a G-crossed product and so all $A \otimes_K K_i'$ are G-crossed products. But $[L : Z]$ is prime to p, so the same is true of $[L'' : Z]$ and thus of $[K' : K]$. It follows that some K_i'' has degree prime to p over K. If $L = L''$ then $K_i' = K_i''$ and we are done. If not, char$(F) \neq p$ implying that $[K_i' : K_i'']$ is prime to p and so $[K_i' : K]$ is prime to p, proving 2.2. ∎

With 2.2 as our tool, we proceed to prove 2.1 by showing no group G can arise for all A/K as in 2.2. To this end, we require examples of division algebras in which we understand the groups appearing as Galois groups of maximal subfields and their behavior under prime to p extensions. It is very convenient to use totally and tamely ramified division algebras for our purpose. We will recall some basic definitions in this area, but we refer the reader to [TW], and [TA] for more details.

Let D be a division algebra with (Krull) valuation v: $D \to \Gamma$ where Γ is an ordered abelian group. Associated to v is its valuation ring $R \subseteq D$ with unique maximal ideal $M \subsetneq R$ and residue division algebra $\bar{D} = R/M$. If $F = Z(D)$ then v induces a valuation (also called v) on F and we let $e(D/F)$ denote the finite index $[v(D^*) : v(F^*)]$. We say D is **totally and tamely ramified** with respect to v if $e(D/F) = [D : F]$ and $[D : F]$ is prime to the residue characteristic. Note that in this case $\bar{D} = \bar{F}$.

Assume that D is a totally and tamely ramified division algebra with center F, with respect to a valuation v. We will quote some known results about D. Let $A = v(D^*)/v(F^*)$, an abelian group of order $[D : F]$. D defines a **nondegenerate symplectic pairing** $\gamma : A \times A \to \mu$ [TW, p. 232] where $\mu \subseteq \bar{F}$ is the group of roots of 1, by which we mean:

(1) γ is bilinear
(2) $\gamma(a, a) = 1$ for all $a \in A$
(3) γ induces an isomorphism $A \cong \mathrm{Hom}_Z(A, \mu)$.

Recall that if $a, b \in v(D)$ and $d, e \in D$ satisfy $v(d) = a$, $v(e) = b$, then:

$$\gamma(a,b) = (ded^{-1}e^{-1}) + M \in \bar{D} = \bar{F}. \tag{2.4}$$

A subgroup $B \subseteq A$ is called **Lagrangian** if $\gamma(B, B) = 1$ and $|B|^2 = |A|$. The key result in this whole business is:

THEOREM 2.5 (TW, theorem 3.8): *A group G is isomorphic to the Galois group of a maximal subfield of D over a henselian field F if and only if G is isomorphic to a Lagrangian subgroup of A.*

Paired with 2.5 is the existence theorem.

THEOREM 2.6 (TA, p. 133): *Suppose A' is a finite abelian group with a nondegenerate symplectic pairing $\gamma' : A' \times A' \to \mathbb{Q}/\mathbb{Z}$. For any field F' of characteristic prime to $|A'|$, there is a division algebra D/F and a valuation $v : D \to \Gamma$ such that:*

a) *F is Henselian with respect to the restriction of v,*
b) *D is totally and tamely ramified with respect to v and*
c) *The symplectic pairing defined by D can be identified with A', γ'.*

Totally and tamely ramified division algebras behave well with respect to prime-to-p extensions as the following shows.

LEMMA 2.7: *Suppose D/F and $v : D \to \Gamma$ are such that 2.6 a) and b) hold. If L/F is a field extension of degree prime to $[D : F]$, the division algebra $E = D \otimes_F L$ has a valuation extending v with respect to which it is totally and tamely ramified. Moreover, D and E define isomorphic symplectic pairings.*

Proof: (Follows from [M, theorem 1] but we provide a short, self-contained proof) Since F is Henselian, v extends to a unique valuation (also called v) on L, and L is Henselian. It follows that v extends to some valuation $v : E \to \Gamma'$. Set $A = v(D)/v(F)$ and $A' = v(E)/v(L)$. The inclusion $D \subseteq E$ induces a homomorphism $\psi : A \to A'$ which by (2.4) is easily seen to be compatible with the symplectic pairings. We claim ψ is injective. Indeed suppose $a \in v(D) \cap v(L)$. Write $a = v(g)$ for $g \in L$. Let $N_{L/F} : L \to F$ be the norm map and let $f = N_{L/F}(g)$. Then $v(f) = [L : F]v(g)$, implying $a + v(F)$ has order dividing $[L : F]$ in A. But $|A|$ and $[L : F]$ are relatively prime so $a \in v(F)$, as desired.

Now $[v(E) : v(L)] = |A'| \geq |A| = [v(D) : v(F)] = [D : F] = [E : L]$ and E is totally and tamely ramified. Consequently $|A'| = |A|$, so $A \to A'$ is an isomorphism and 2.7 is proved. ∎

We are ready to prove 2.1 using Amitsur's incompatibility argument. Suppose, on the contrary, that $UD(F, p^r, s) \otimes_Z L$ is a G-crossed product for $[L : Z]$ of degree prime to p. Let A' be the elementary abelian p group of order p^{2r} with basis $a_1, \ldots, a_r, b_1, \ldots, b_r$. For convenience we identify μ with a subgroup of $\mathbb{Q}/\mathbb{Z}$, by fixing the various primitive roots of 1. Let $\gamma' : A' \times A' \to \mathbb{Q}/\mathbb{Z}$ be the nondegenerate symplectic pairing defined by $\gamma'(a_i, a_j) = \gamma'(b_i, b_j) = \gamma'(a_i, b_j) = 0$ if $i \neq j$, $\gamma'(a_i, a_i) = \gamma'(b_i, b_i) = 0$, and $\gamma'(a_i, b_i) = \frac{1}{p} + \mathbb{Z}$. Take D/F as in 2.6. By 2.2, $D \otimes_F L'$ is a G-crossed product for some $L' \supseteq F$ of degree prime to p. By 2.7 and 2.5, G is isomorphic to a Lagrangian of A' and hence to an elementary abelian p-group of order p^r. On the other hand, let A' be the direct sum of two cyclic groups of order p^r with basis a, b. Define the nondegenerate symplectic pairing $\gamma' : A' \times A' \to \mathbb{Q}/\mathbb{Z}$ by setting $\gamma'(a, b) = (1/p^r) + \mathbb{Z}$. Arguing as above, G must be isomorphic to a Lagrangian of A and so is either cyclic or metacyclic. When $r \geq 3$ this is a contradiction, and 2.1 is proved.

3. Indecomposable division algebras and prime-to-p extensions

In this section we will show that there is a division algebra D/F of odd degree p^2 and exponent p, for p odd, such that every prime-to-p extension of $D \otimes_F L$ is indecomposable. More specifically, we will show that the indecomposable division algebra constructed in [T] has this property. The referee has pointed out that using [TW] and [M], one can generalize this example to include an arbitrary inertially split division algebra D of exponent p and degree p^r ($r \geq 2$) over a Henselian field, for p odd, and degree $r \geq 3$ for $p = 2$. In this whole section, the field F' will contain a primitive p^{th} root ρ of 1.

The argument in [T] starts by constructing a division algebra A/F' of degree p^2 and a field $M = F'(a^{1/p}, b^{1/p})$ such that:

(1) M splits A

(2) A cannot be written as $(a, f)_{p,F'} \otimes (b, g)_{p,F'}$

where in general $(x, y)_{p,F'}$, of course, is generated over F' by α, β subject to the relations $\alpha^p = x$, $\beta^p = y$, and $\alpha\beta = \rho\beta\alpha$. We do not have to duplicate the construction of A but can simply note that (1) and (2) are preserved by prime-to-p extensions, as follows.

LEMMA 3.1: *Suppose $L' \supseteq F'$ is a finite field extension with $[L' : F']$ prime to p. Write $A' = A \otimes_{F'} L'$ and $M' = L'(a^{1/p}, b^{1/p})$. Then M' splits A'; but A' cannot be written as $(a, f')_{p,L'} \otimes (b, g')_{p,L'}$ for any $f', g' \in L'$.*

Proof: Clearly M' splits A'. Suppose $A' \cong (a, f')_{p,L'} \otimes (b, g')_{p,L'}$ and $r = [L' : F']$. Taking the corestriction from L' to F',

$$[\mathrm{cor}_{L'/F'}(A')] = [\mathrm{cor}_{L'/F'}(a, f')][\mathrm{cor}_{L'/F'}(b, g')].$$

By [B, p. 112] this last expression is $[(a, N_{L'/F'}(f'))][(b, N_{L'/F'}(g'))]$. Finally, note $[\mathrm{cor}_{L'/F'}(A')] = [A]^r$. If rs is congruent to 1 mod p, then

$$A \cong (a, N_{L'/F'}(f')^s)_{p,F'} \otimes (b, N_{L'/F'}(g')^s)_{p,F'}.$$

This contradiction proves the lemma. ∎

The next step in the proof of [T] was to set $F = F'(x, y)$ and D/F the division algebra in the class of $(A \otimes_{F'} F) \otimes_F (x, a)_{p,F} \otimes_F (y, b)_{p,F}$. If $K = F(a^{1/p}, b^{1/p})$, then K splits D and so D has degree p^2. Tignol in [T] showed that D is indecomposable. We wish to show:

THEOREM 3.2: *Suppose $L \supseteq F$ is a finite field extension and $[L : F]$ is prime to p. Then $D \otimes_F L$ is indecomposable.*

Of course, 3.2 is a consequence of 3.1 and:

PROPOSITION 3.3: *Suppose $L \supseteq F$ is a finite field extension and $[L : F]$ is prime to p. If $D \otimes_F L$ is decomposable, there is a finite prime-to-p extension $L' \supseteq F'$ such that $A \otimes_{F'} L' \cong (a, f)_{p,L'} \otimes (b, g)_{p,L'}$.*

Proof: Let $K = F'((x, y))$ be the iterated power series field, $F' \supseteq F$. $L \otimes_F K$ is a direct sum of fields $\oplus L_i$. One such L_i, say L_1, must have degree prime to p over K. The discrete valuation on K defined by y extends uniquely to L_1 and we may view $L \subseteq L_1$. If $L'' = \bar{L}_1$ is the residue field, $L'' \supseteq F'((x))$ is a finite field extension of degree prime to p. The discrete valuation defined by x on $F'((x))$ extends uniquely to L'' and $L' = \bar{L}''$ has degree prime to p over F'.

Now suppose $D \otimes_F L$ is decomposable. Then $(D \otimes_F K) \otimes_K L_1 = B_1 \otimes B_2$ where the B_i are central over L_1 of degree p. By [T, p. 212], one of the B_i, say B_1, can be assumed to be unramified with respect to the (extension of the) y- valuation. Thus B_2 defines the same ramification character over $\bar{L}_1 = L''$ as (y, b). By the argument of [T, p. 212] $B_2 \cong (yu, b)$ for $u \in L_1$ a unit with respect to the y-valuation. The residue $\bar{u} \in L''$ can be written $\pi^r w$ where π is a prime element of L'' with respect to the x-valuation and w is a unit. Let s be the valuation of the image of x in L''. Now $[B_1][(yu, b)] = [D \otimes_F L_1] = [A \otimes_{F'} L_1][(x, a)][(y, b)]$, so we have $[B_1][(u, b)] = [A \otimes_{F'} L_1][(x, a)]$. Both sides of this equation are unramified so we can equate their images in $Br(\bar{L}_1)$. That is,

$$[\bar{B}_1][(\pi^r w, b)] = [A \otimes_{F'} L''][(x, a)] \tag{3}$$

It follows that with respect to the x-valuation, B_1 has the same character over $L'' = \bar{L}'$ as $(\pi, a^s b^{-r})$, or as (x, ab^{-rt}) where st is congruent to 1 modulo p. As with B_2, it follows that the residue algebra $\bar{B}_1 \cong (xv', ab^{-rt})_{p,L''}$ for some unit $v' \in L''$. Substituting this into (3) we have

$$[A \otimes_F L''] = [(xv', ab^{-rt})][(\pi^r w, b)][(x, a^{-1})].$$

Writing $x = \pi^s z$ for some unit z we have $[A \otimes_F L''] =$

$$[(\pi^s, ab^{-rt})][(z, ab^{-rt})][(v', ab^{-rt})][(\pi^r w, b)][(\pi^s z, a^{-1})] =$$

$$[(\pi, a^s b^{-rst})][(v', ab^{-rt})][(z, ab^{-rt})][(\pi, b^r)][(w, b)][(z, a^{-1})][(\pi, a^{-s})] =$$

$$[(v', a)][(v'^{-rt} z^{-rt} w, b)].$$

Taking images in $Br(L')$ and renaming variables we have

$$[A \otimes_{F'} L'] = [(a, f)][(b, g)].$$

This proves 3.3. ∎

Of course, 3.3 and 3.1 imply the main theorem 3.2 and we are done.

References

[A] A. A. Albert, *Structure of Algebras,* AMS Coll. Publ. 24, Providence RI, 1961

[B] K. S. Brown, *Cohomology of Groups,* Springer-Verlag, New York, 1982.

[DI] I. Demeyer and E. Ingraham, *Separable Algebras over Commutative Rings,* Springer Lecture Notes in Math. 181, 1971.

[JW] B. Jacob and A. Wadsworth, *Division Algebras over Henselian Fields,* J. Algebra **128** (1990), 126–179.

[M] P. Morandi, *The Henselization of a Valued Division Algebra,* J. Algebra **122** (1989), 232–243.

[OS] M. Orzech and C. Small, *The Brauer Group of Commutative Rings,* Marcel Dekker, New York, 1975.

[R] L. H. Rowen, *Cyclic Division Algebras,* Israel J. Math. **41** (1982), 213–234. Correction, ibid. **43** (1982), 277–280.

[S1] D. J. Saltman, *Azumaya algebras with involution,* J of Algebra **52(2)** (1978), 526–539.

[S] D. Saltman, *Splittings of cyclic p-algebras,* Proc. Amer. Math. Soc. **62** (1977), 223–228.

[T] J.-P. Tignol, *Algebres indecomposables d'exponent premier,* Adv. in Math. **65(3)** (1987), 205–228.

[TA] J.-P. Tignol and S. A. Amitsur, *Kummer subfields of Malcev–Neumann division algebras,* Isr. J. of Math. **50(1-2)** (1985), 114–144.

[TW] T.-P. Tignol and A. R. Wadsworth, *Totally ramified valuations on finite dimensional division algebras,* Trans AMS **302(1)** (1987), 223–250.