The First Two Cohomology Groups of Some Galois Groups

J. Mináč *† A. Wadsworth†

Abstract

We investigate the first two Galois cohomology groups of p-extensions over a base field which does not necessarily contain a primitive pth root of unity. We use twisted coefficients in a systematic way. We describe field extensions which are classified by certain residue classes modulo p^nth powers of a related field, and we obtain transparent proofs and slight generalizations of some classical results of Albert. The potential application to the cyclicity question for division algebras of degree p is outlined.

Introduction

Let p be a prime number, let F be a field with $char(F) \neq p$, and let $\mathcal{G}_F = \mathcal{G}(F_{sep}/F)$ be the absolute Galois group of F. It is well known that for any $n \in \mathbb{N}$, the continuous cohomology group $H^1(\mathcal{G}_F, \mathbb{Z}/p^n\mathbb{Z})$ classifies the cyclic Galois extensions of F of degree dividing p^n, while $H^1(\mathcal{G}_F, \mu_{p^n}) \cong F^*/F^{*p^n}$, where μ_{p^n} denotes the group of p^n-th roots of unity in the separable closure F_{sep} of F; also, $H^2(\mathcal{G}_F, \mu_{p^n}) \cong {}_{p^n}Br(F)$, the p^n-torsion in the Brauer group of F. When $\mu_{p^n} \subseteq F$, then $\mu_{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}$ as trivial $\mathcal{G}_F$-modules, and the resulting isomorphism $H^1(\mathcal{G}_F, \mathbb{Z}/p\mathbb{Z}) \cong H^1(\mathcal{G}_F, \mu_{p^n})$ is the homological formulation of the classical Kummer correspondence between cyclic Galois extensions of F of degree dividing p^n and cyclic subgroups of F^*/F^{*p^n}. Then also, the Merkurjev-Suslin Theorem describes ${}_{p^n}Br(F)$; this depends on the isomorphism $H^2(\mathcal{G}_F, \mu_{p^n}) \cong H^2(\mathcal{G}_F, \mu_{p^n}^{\otimes 2})$, which is available because of the trivial action of $\mathcal{G}_F$ on μ_{p^n}.

We consider here questions concerning first and second cohomology groups with μ_{p^n} coefficients and concerning F^*/F^{*p^n} and ${}_{p^n}Br(F)$ when F does not contain a primitive p-th root of unity (so $p \neq 2$), so that the isomorphisms just mentioned are not available. In particular, we will give an answer to the question: What field extensions does F^*/F^{*p^n} classify when $\mu_{p^n} \not\subseteq F$?

Since the full absolute Galois group is often too large to work with conveniently, and we are interested in field extensions of degree a power of p, we prefer to work with a pro-p-group instead of $\mathcal{G}_F$. For this, let $F(p)$ be the maximal p-extension of F, which is the compositum of all the Galois field extensions of F of degree a power of p, and let G_F be the Galois group $\mathcal{G}(F(p)/F)$; so, G_F is the maximal pro-p homomorphic image of $\mathcal{G}_F$. Then, $H^1(G_F, \mathbb{Z}/p\mathbb{Z}) \cong H^1(\mathcal{G}_F, \mathbb{Z}/p\mathbb{Z})$, but

*Supported in part by NSERC grant R0370A01.

†The authors would like to thank MSRI in Berkeley for its hospitality while part of the research for this paper was carried out. We also thank the organizers of the exciting Galois theory program held at MSRI in Fall of 1999.

"$H^1(G_F, \mu_{p^n})$" is undefined since $\mu_{p^n} \not\subseteq F(p)$. We will given an interpretation of "$H^1(G_F, \mu_{p^n})$" in this context, and show that once again it classifies a certain family of field extensions. However, these are field extensions of $M = F(\mu_{p^n})$, rather than those of F. Indeed, our general approach is to relate objects over F to those over $L = F(\mu_p)$ and over $M = F(\mu_{p^n})$, since the latter are easier to understand because of the presence of enough roots of unity. Passage from F to L is particularly tractable because $p \nmid [L : F]$.

Indications of what happens are provided by Albert's work in [A_1] for the case $n = 1$. Albert showed that the cyclic degree p field extensions S of F correspond to certain cyclic degree p extensions T of L. For, if $T = S \cdot L$, then S is the unique extension of F of degree p within T (corresponding to the prime-to-p part of the abelian Galois group $\mathcal{G}(T/F)$). Since T is a p-Kummer extension of L, we have $T = L(\sqrt[p]{b})$ for some $b \in L^*$ whose class $[b] \in L^*/L^{*p}$ generates the cyclic subgroup associated to T in the Kummer correspondence. The question of classifying cyclic extensions of F of degree p reduces to determining which cyclic extension of L they generate. For this, Albert showed that a Kummer p-extension $T' = L(\sqrt[p]{b'})$ has the form $S' \cdot L$ for some cyclic degree p extension S' of F iff $\mathcal{G}(L/F)$ acts on $[b']$ in L^*/L^{*p} the same way it acts on μ_p. A nice way of expressing this is as follows: Let $H = \mathcal{G}(L/F)$. For each character $\chi\colon H \to (\mathbb{Z}/p\mathbb{Z})^*$ (= group of units of the ring $\mathbb{Z}/p\mathbb{Z}$) and each p-torsion H-module A, there is the χ-eigenmodule of A for the H action: $A^{(\chi)} = \{a \in A \mid h \cdot a = \chi(h)a \text{ for all } h \in H\}$. Then, Albert's result can be rephrased: Cyclic p-extensions of F correspond to cyclic subgroups of $(L^*/L^{*p})^{(\alpha)}$, where $\alpha\colon H \to (\mathbb{Z}/p\mathbb{Z})^*$ is the cyclotomic character defined by $h \cdot \omega = \omega^{\alpha(h)}$ for each $h \in H$, $\omega \in \mu_p$.

We consider here F^*/F^{*p^n} and cyclic Galois extensions of F of degree p^n for arbitrary n. For this, we work with the field $M = F(\mu_{p^n})$ instead of L. We show in Cor. 1.11 that $F^*/F^{*p^n} \cong (M^*/M^{*p^n})^{\mathcal{G}(M/F)}$ (which is the eigenmodule of M^*/M^{*p^n} for the trivial character of $\mathcal{G}(M/F)$). We show further in Th. 1.13 that the cyclic extensions K of M of degree dividing p^n that correspond to cyclic subgroups of F^*/F^{*p^n} are those K which are Galois over F with $\mathcal{G}(M/F)$ acting on $\mathcal{G}(K/F)$ by the cyclotomic character $\alpha\colon \mathcal{G}(M/F) \to (\mathbb{Z}/p^n\mathbb{Z})^*$ for μ_{p^n}. In addition, when $M = L$, we give in Prop. 1.7 a small generalization of Albert's result, by showing that then the cyclic field extensions of F of degree dividing p^n correspond to the cyclic subgroups of $(M^*/M^{*p^n})^{(\alpha)}$. (This correspondence breaks down whenever $M \neq L$, however—see Remark 1.8(a).)

Characters on Galois groups can also be used to define twisted actions for their modules: For any profinite group G, any continuous character $\chi\colon G \to (\mathbb{Z}/p\mathbb{Z})^*$, and any p^n-torsion discrete G-module A, define the action of G on A twisted by χ to be the new action given by $g * a = \chi(g)(g \cdot a)$ (where $g \cdot a$ denotes the original G-action). We use such a twisted action in §2 to give an interpretation to "$H^i(G_F, \mu_{p^n})$", which as written is not well-defined. We define this to mean $H^i(G_F, \widetilde{\mu_{p^n}})$, where $\widetilde{\mu_{p^n}}$ denotes μ_{p^n}, but with the action of $\mathcal{G} = \mathcal{G}(L(p)/F)$ on it twisted by a character θ^{-1} so that $\mathcal{G}(L(p)/F(p))$ acts trivially on $\widetilde{\mu_{p^n}}$; hence, G_F acts on $\widetilde{\mu_{p^n}}$, even though not on μ_{p^n}. For H^1, we give a more specific interpretation in Th. 2.3, by showing that $H^1(G_F, \widetilde{\mu_{p^n}}) \cong (L^*/L^{*p^n})^{(\theta)}$. It follows easily (see Cor. 2.5) that the canonical map $H^1(G_F, \widetilde{\mu_{p^n}}) \to H^1(G_F, \widetilde{\mu_p})$ is surjective. This result was needed for the paper [MW_1], which was the initial impetus for the work given here. We also show that $H^1(G_F, \widetilde{\mu_{p^n}})$ is isomorphic to an eigenmodule of $H^1(G_M, \mathbb{Z}/p^n\mathbb{Z})$,

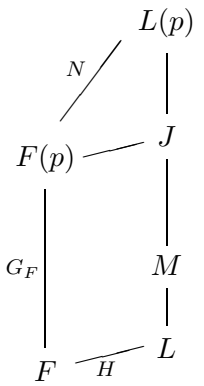
so that the cyclic subgroups of $H^1(G_F, \widetilde{\mu_{p^n}})$ classify certain cyclic field extensions of M of degree dividing p^n; we give in Th. 2.7 a Galois theoretic characterization of those field extensions of M.

In §3 we consider second cohomology groups with μ_{p^n} coefficients, or, equivalently, the p^n-torsion of the Brauer group. We have the standard isomorphisms ${}_{p^n}Br(F) \cong H^2(\mathcal{G}(L(p)/F), \mu_{p^n})$ and ${}_{p^n}Br(L) \cong H^2(G_L, \mu_{p^n})$. When $\mu_{p^n} \subseteq L$, the Merkurjev-Suslin Theorem gives a very useful presentation of ${}_{p^n}Br(L)$ by generators (namely symbol algebras) and relations. The Merkurjev-Suslin Theorem does not apply to ${}_{p^n}Br(F)$ since $\mu_{p^n} \not\subseteq F$, but the easy isomorphism ${}_{p^n}Br(F) \cong ({}_{p^n}Br(L))^{\mathcal{G}(L/F)}$ allows one to analyze ${}_{p^n}Br(F)$ in terms of the more readily understood ${}_{p^n}Br(L)$. This approach was used by Albert in [A_1] in proving his cyclicity criterion for algebras of degree p, and by Merkurjev in [M] in proving that ${}_pBr(F)$ is generated by algebras of degree p. We give here in Th. 3.6 a generalization of Albert's result, by showing that when $\mu_{p^n} \subseteq L$, a division algebra D of degree p^n over F is a cyclic algebra iff there is $d \in D$ with $d^{p^n} \in F^* - F^{*p}$.

But, what we find most tantalizing here is the potential application to the cyclicity question for division algebras of degree p. If B is a central division algebra of degree p over$L$ with $[B] \in ({}_pBr(L))^{\mathcal{G}(L/F)}$, then there is a unique central division algebra A over F of degree p with $A \otimes_F L \cong B$. When B is a cyclic algebra, it is actually a symbol algebra, i.e., it has a presentation by generators i, j such that $i^p = b$, $j^p = c$, $ij = \omega ji$, where $b, c \in L^*$ and $\omega \in \mu_p$, $\omega \neq 1$. We prove in Prop. 3.4 that if A is a cyclic algebra, then not only is B cyclic, but it must have a presentation as above with b and c mapping to specified eigencomponents of L^*/L^{*p} with respect to the $\mathcal{G}(L/F)$ action. Thus, B could very well be cyclic without satisfying the more stringent conditions which correspond to cyclicity of A. Then A would be a counterexample to the decades-old question whether all central simple algebras of degree p must be cyclic algebras (which is still unsettled for all $p \geq 5$). Regrettably, we have not found such a counterexample, but we feel that the approach merits further investigation.

An interesting extreme case of this is for the field $J = F(p) \cdot L = F(p)(\mu_p)$. We have ${}_pBr(F(p)) \cong ({}_pBr(J))^{\mathcal{G}(J/F(p))}$. If this group is nonzero, then Merkurjev's result says that there is a division algebra of degree p over $F(p)$; but such an algebra cannot be cyclic, as $F(p)$ has no cyclic field extensions of degree p. This observation led us to attempt do find division algebras of degree p in $({}_pBr(J))^{\mathcal{G}(J/F(p))}$, by using valuation theory. In §4, we describe how valuations on F with residue characteristic not p extend to $F(p)$ and to J. This makes it easy to see that ${}_pBr(J)$ can have some nontrivial eigencomponents for the action of $\mathcal{G}(J/F(p))$ (see Ex. 4.2). But the question whether $({}_pBr(J))^{\mathcal{G}(J/F(p))} \neq 0$ remains open.

We fix throughout the paper the notation mentioned in this Introduction. The most relevant fields are shown in the diagram below; the names of the Galois groups given here will also be fixed throughout. We write μ_m for the group of m-th roots of unity (in an algebraic closure of the relevant field) and μ_m^* for the primitive m-th roots of unity. Also, for any profinite group G, let $X(G) = Hom(G, \mathbb{Q}/\mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z})$, the (continuous) character group of G. If G is a group of automorphisms of some field, we write $\mathcal{F}(G)$ for the fixed field of G.



$$
\begin{aligned}
L &= F(\mu_p)\\
M &= F(\mu_{p^n})\\
J &= F(p)\cdot L = F(p)(\mu_p)\\
\mathcal{G} &= \mathcal{G}(L(p)/F)\\
G_F &= \mathcal{G}(F(p)/F)\\
G_L &= \mathcal{G}(L(p)/L)\\
\Gamma_F &= \mathcal{G}(J/L) \cong G_F\\
N &= \mathcal{G}(L(p)/F(p))\\
H &= \mathcal{G}(L/F) \cong \mathcal{G}(J/F(p))
\end{aligned}
$$

While we were in the last stages of writing this paper we learned of the interesting recent preprint by U. Vishne [V]. There is some overlap between this paper and Vishne's (most notably in our Th. 3.6), but it is not great, since Vishne is concerned primarily with the situation that $\mu_{p^n} \subseteq F(\mu_p)$.

We would like to thank Bruno Kahn for very helpful discussions at an early stage of this work, particularly for pointing out to us the significance of group actions twisted by characters.

1 Extension fields of F and L, and an interpretation of F^*/F^{*p^n}

In this section, we recall some known properties of p-extensions, then give characterizations of the Galois p-extensions of $L = F(\mu_p)$ which correspond to such extensions of F. We then look at group actions on p^n-torsion modules, and examine eigenspace decompositions of such modules. This is applied to various structures associated to the abelian p^n-extensions of F and L. This leads to Kummer-like characterization of F^*/F^{*p^n} and L^*/L^{*p^n} in terms of certain abelian p^n-extensions, but the extensions are of $M = F(\mu_{p^n})$, not of F and in general not of L. For Prop. 1.1 through Cor. 1.3, p may be any prime number. After Cor. 1.3 we will assume further that p is odd.

We first consider the subfields of $F(p)$. By definition, $F(p)$ is the compositum of all the Galois field extensions of F of degree a power of p (in some algebraic closure of F). Recall that if K_1 and K_2 are Galois extensions of F with $[K_i : F] = p^{k_i}$, then $K_1 \cdot K_2$ is also Galois over F and $[K_1 \cdot K_2 : F] \,|\, p^{k_1+k_2}$. Consequently, $F(p)$ can also be described as the union of of all the Galois extensions of F of degree a power of p. So, $F(p)$ is the maximal Galois extension of F such that $\mathcal{G}(F(p)/F)$ is a pro-p-group. Also, if T is a field extension of F with $[T : F] < \infty$ and K is the normal closure of T over F, then $T \subseteq F(p)$ iff T is separable over F and $[K : F]$ is a power of p. We give next a characterization of such fields T which is well-known, but we could find no reference for it. It is an easy consequence of the property of p-groups that every maximal proper subgroup is a normal subgroup of index p. The proof will be omitted.

Proposition 1.1 *Let S be a field of any characteristic, and let T be a field, $T \supseteq S$, $[T : S] < \infty$. Then the following are equivalent:*

(i) *The normal closure of T over S is Galois over S of degree a power of p, i.e., $T \subseteq S(p)$.*

(ii) *There is a chain of fields $S = S_0 \subseteq S_1 \subseteq S_2 \subseteq \ldots \subseteq S_k = T$ with each S_i Galois over S_{i-1}, and $[S_i : S_{i-1}] = p$.*

We record two important corollaries of Prop. 1.1, which are also well-known, and whose easy proofs are omitted. The second is an immediate consequence of the first.

Corollary 1.2 *For fields S and T of any characteristic, if $S \subseteq T \subseteq S(p)$, then $T(p) = S(p)$. In particular, $S(p)(p) = S(p)$.*

Corollary 1.3 *If T is a field with $char(T) \neq p$ and $\mu_p \subseteq T$, then $T(p)^p = T(p)$.*

From now on, throughout the rest of the paper, we assume that the prime number p is odd.

We now return to the basic setting of this paper, with F a field, $char(F) \neq p$, $L = F(\mu_p)$, $J = F(p) \cdot L = F(p)(\mu_p)$. Since $[L : F] \,\big|\, (p-1)$, we have $L \cap F(p) = F$ and $\mathcal{G}(J/L) \cong \mathcal{G}(F(p)/F) = G_F$. Therefore, there is a canonical inclusion and index preserving one-to-one correspondence between the p-extensions S of F (i.e., $F \subseteq S \subseteq F(p)$) and those p-extensions T of L with $T \subseteq J$. When $S \leftrightarrow T$ we have $T = S \cdot LS(\mu_p)$ and $S = T \cap F(p)$. Furthermore, S is Galois over F iff T is Galois over L; when this occurs, $\mathcal{G}(S/F) \cong \mathcal{G}(T/L)$. Of course $L(p)$ may be much larger than J (as in Ex. 4.2 below), so we next characterize those Galois p-extensions of L which lie in J. Let $H = \mathcal{G}(L/F)$, so H is cyclic and $|H| \,\big|\, p-1$. Let $s = |H| = [L : F]$.

Proposition 1.4 *Let T be a Galois extension of L with $L \subseteq T \subseteq L(p)$. Then, the following are equivalent:*

(i) *$T \subseteq J$.*

(ii) *$T = S \cdot L$ for a field S, $F \subseteq S \subseteq F(p)$, with S Galois over F.*

(iii) *T is Galois over F and $\mathcal{G}(T/F) \simeq \mathcal{G}(T/L) \times \mathcal{H}$ for some group $\mathcal{H}$. (Then necessarily $\mathcal{H} \cong H$.)*

(iv) *T is Galois over F and $\mathcal{G}(T/F)$ has a normal subgroup $\mathcal{H}$ of order s.*

If $\mathcal{G}(T/L)$ is abelian, then (i)–(iv) are equivalent to:

(v) *T is Galois over F and $\mathcal{G}(L/F)$ acts trivially on $\mathcal{G}(T/L)$.*

Proof. Note that $[T : L]$ could be finite or infinite. (i) $\Leftrightarrow$ (ii) was noted above. (ii) $\Rightarrow$ (iii) Let $\mathcal{H} = \mathcal{G}(T/S)$. Note that S and L are each Galois over F, and $S \cap L = F$ as $gcd([S_0 : F], [L : F]) = 1$ for each finite degree subextension S_0 of F in S. Therefore, S and L are linearly disjoint over F, and $\mathcal{G}(T/F) = \mathcal{G}(T/L) \times \mathcal{H}$. Note that $|\mathcal{H}| = [S \cdot L : S] = [L : F] = s$. (iii) $\Rightarrow$ (iv) For $\mathcal{H}$ as in (iii), we have $\mathcal{H} \cong \mathcal{G}(T/F)/\mathcal{G}(T/L) \cong \mathcal{G}(L/F) = H$. Clearly, $\mathcal{H}$ is a normal subgroup of $\mathcal{G}(T/F)$. (iv) $\Rightarrow$ (ii) For $\mathcal{H}$ as in (iv), let $S = \mathcal{F}(\mathcal{H})$. Then S is Galois over F and $[T : S] = |\mathcal{H}| = s$. We have $[T : S \cdot L] \,\big|\, [T : S] = s$ and $[T : S \cdot L]$ is a power of p, as $S \cdot L \subseteq T \subseteq L(p) = (S \cdot L)(p)$ (see Cor. 1.2). Hence, $S \cdot L = T$. Since L is Galois over $L \cap S$, we have $[L : L \cap S] = [L \cdot S : S] = [T : S] = s = [L : F]$;

hence, $L \cap S = F$. Since $T = S \cdot L$ is a compositum of Galois p-extensions of L and $\mathcal{G}(T/L) \cong \mathcal{G}(S/F)$, this S is a compositum of such extensions of F. Hence, $S \subseteq F(p)$, proving (ii).

Now assume $\mathcal{G}(T/L)$ is abelian. Then (iii) implies that $\mathcal{G}(T/F)$ is abelian, so (v) holds. Conversely, assume (v). Let $G = \mathcal{G}(T/F)$ and let $P = \mathcal{G}(T/L)$. Since G/P acts trivially on the abelian group P, this P must be central in G. Since further $G/P \cong \mathcal{G}(L/F)$, which is cyclic, an elementary exercise in group theory shows that G is abelian. Let T_0 be any finite degree subextension of L lying in T. Then, $[T_0 : L] = p^k$, for some $k \in \mathbb{N}$, and T_0 is abelian Galois over F, with $|\mathcal{G}(T_0/F)| = s p^k$. The primary decomposition of $\mathcal{G}(T_0/F)$ gives $T_0 = S_0 \cdot L_0$, where S_0 is the unique subfield of T_0 with $[T_0 : S_0] = s$ and $[T_0 : L_0] = p^k$. Since S_0 is Galois over F with $[S_0 : F] = p^k$, we have $S \subseteq F(p)$. Also, $[T_0 : L] = [T_0 : L_0]$, so $L = L_0$. Thus, $T_0 = (T_0 \cap F(p)) \cdot L$ for every finite degree subextension T_0 of L in T. Hence, $T = (T \cap F(p)) \cdot L$, proving (ii). □

In proving the following corollary, we will use supernatural numbers. Recall (cf. [S_2, p. 5]) that a supernatural number is a formal product $\prod_{i=1}^{\infty} p_i^{r_i}$ where the p_i are distinct prime numbers and each $r_i \in \{0, 1, 2, \ldots\} \cup \{\infty\}$. Supernatural numbers can be multiplied in the obvious way, and likewise the notions of divisibility, gcd's , and lcm's of supernatural numbers have the obvious interpretation. For fields $F \subseteq K$ with K algebraic over F, we define $[K : F]$ to be the supernatural number $lcm\{\, dim_F N \mid N \text{ is a field, } F \subseteq N \subseteq K, \text{ and } dim_F N < \infty \,\}$. (Of course, this agrees with the usual definition when $dim_F N < \infty$.) The reader can check that for any field E with $F \subseteq E \subseteq K$, we have

$$[K : F] \;=\; [K : E][E : F]\,. \tag{1.1}$$

Corollary 1.5 *Let T/F be a Galois subextension of $L(p)/F$ such that there is a normal subgroup $\mathcal{H}$ of $\mathcal{G}(T/F)$ with $|\mathcal{H}| = s = [L : F]$. Then, $L \subseteq T \subseteq J$. Hence, the Galois group $\mathcal{G}(L(p)/J)$ is the smallest closed normal subgroup B of $\mathcal{G} = \mathcal{G}(L(p)/F)$ such that $\mathcal{G}/B$ contains a normal subgroup of order s.*

Proof. We have $[L(p) : F] = s\, p^r$ for $0 \le r \le \infty$. Since $s = |\mathcal{H}| \;\big|\; [T : F]$, we have $[L(p) : T] = p^t$ for $t \le \infty$, by (1.1). So, $[T(\mu_p) : T]$ is a power of p; hence, $\mu_p \subseteq T$, so $L \subseteq T$. Then, Prop. 1.4 shows that $T \subseteq J$, so of course $\mathcal{G}(L(p)/J) \subseteq \mathcal{G}(L(p)/T)$.

Now, $\mathcal{G}/(\mathcal{G}(L(p)/J) \cong \mathcal{G}(J/F)$, which contains the normal subgroup $\mathcal{G}(J/F(p))$ of order s. The inclusion $T \subseteq J$ just proved shows that $\mathcal{G}(L(p)/J)$ is minimal with this property. □

We want to describe the abelian p^n-extensions of L in J as an eigencomponent of the family of all such extensions of L. For this, we first need some facts about p^n-torsion G-modules.

Fix a positive integer n. Let G be any profinite group, and let A be a discrete G-module (written additively), which is p^n-torsion as an abelian group. Let $\chi\colon G \to (\mathbb{Z}/p^n\mathbb{Z})^*$ be any continuous group homomorphism. (The continuity of the character χ is equivalent to $ker(\chi)$ being an open subgroup of G.) Note that since $(\mathbb{Z}/p^n\mathbb{Z})^* \cong Aut(\mathbb{Z}/p^n\mathbb{Z}, +)$ canonically, defining such a χ is equivalent to giving $\mathbb{Z}/p^n\mathbb{Z}$ the structure of a discrete G-module. Because A is p^n-torsion, it is a $\mathbb{Z}/p^n\mathbb{Z}$-module.

Let $A^{(\chi)}$ denote the χ-*eigenmodule* of A, i.e.

$$A^{(\chi)} = \{a \in A \mid g \cdot a = \chi(g) \cdot a, \text{ for all } g \in G\}. \tag{1.2}$$

Note that $A^{(\chi)}$ is a G-submodule of A. If $A^{(\chi)} = A$, we say that G *acts on* A *via* χ. Whatever the original action of G on A, we can use χ to twist the action, obtaining a new G-module, denoted A_χ, such that $A_\chi = A$ as abelian groups, but if we denote by $\cdot$ the original action of G on A and $*$ the action of G on A_χ, then

$$g * a = \chi(g)(g \cdot a) \qquad \text{for all } g \in G, a \in A.$$

Another way of saying this is that the map $a \mapsto a \otimes 1$ is a G-module isomorphism

$$A_\chi \cong A \otimes_{\mathbb{Z}} \mathbb{Z}/p^n\mathbb{Z}, \tag{1.3}$$

where G acts on $\mathbb{Z}/p^n\mathbb{Z}$ via χ (so $g \cdot (a \otimes k) = (g \cdot a) \otimes \chi(g)k$). We will frequently use the obvious identity

$$(A_\chi)^G = A^{(\chi^{-1})}, \tag{1.4}$$

where $\chi^{-1}(g) = \chi(g)^{-1}$.

Now assume p is odd, and suppose H acts on A, where $H = \mathcal{G}(L/F)$. Since A is p^n-torsion this is equivalent to A being a module for the group ring $\mathbb{Z}/p^n\mathbb{Z}[H]$. Now, H is a cyclic group of order s, where $s \mid p-1$, so

$$\mathbb{Z}/p^n\mathbb{Z}[H] \cong \mathbb{Z}/p^n\mathbb{Z}[x]/(x^s - 1). \tag{1.5}$$

Since $(\mathbb{Z}/p^n\mathbb{Z})^*$ is cyclic of order $\varphi(p^n) = (p-1)p^{n-1}$, it contains a cyclic subgroup of order s. The elements $\gamma_1, \ldots, \gamma_s$ of this group are distinct roots of $x^s - 1$, so $x^s - 1 = (x - \gamma_1)\ldots(x - \gamma_s)$ in $\mathbb{Z}/p^n\mathbb{Z}$. Moreover, since the map $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ has kernel of order p^{n-1}, which is prime to s, the subgroup of order s intersects this kernel trivially. Hence, for $i \neq j$, $\gamma_i - \gamma_j$ maps to a nonzero element of $\mathbb{Z}/p\mathbb{Z}$; so $\gamma_i - \gamma_j \in (\mathbb{Z}/p^n\mathbb{Z})^*$. Therefore, the ideals $(x-\gamma_i)\mathbb{Z}/p^n\mathbb{Z}[x]$ and $(x-\gamma_j)\mathbb{Z}/p^n\mathbb{Z}[x]$ comaximal since their sum contains the unit $\gamma_i - \gamma_j$. It follows by the Chinese Remainder Theorem that

$$\mathbb{Z}/p^n\mathbb{Z}[x]/(x^s - 1) \;\cong\; \bigoplus_{i=1}^{s} \mathbb{Z}/p^n\mathbb{Z}[x]/(x - \gamma_i).$$

Hence, $\mathbb{Z}/p^n\mathbb{Z}[H]$ has s mutually orthogonal primitive idempotents $e_1, \ldots, e_s$, such that each $e_j\mathbb{Z}/p^n\mathbb{Z}[H] \cong \mathbb{Z}/p^n\mathbb{Z}$, and if h is a designated generator of H corresponding to the image of x in (1.5), then $he_i = \gamma_i e_i$. One can check that if $ts \equiv 1 \ mod\ p^n$, then

$$e_i \;=\; t \sum_{j=0}^{s-1} \gamma_i^{-j} h^j \,. \tag{1.6}$$

If $\chi_i \colon H \to (\mathbb{Z}/p^n\mathbb{Z})^*$ is the character given by $h^j \mapsto \gamma_i^j$, then in the left multiplicative action on $e_i\mathbb{Z}/p^n\mathbb{Z}[H]$, H acts by χ_i. Therefore, for our H-module A, we have $A = \bigoplus_{i=1}^{s} e_i A$, and H acts on $e_i A$ by χ_i; it follows easily that $e_i A = A^{(\chi_i)}$, and

$$A = \bigoplus_{i=1}^{s} A^{(\chi_i)}, \tag{1.7}$$

which is a canonical decomposition of A into a direct sum of eigenmodules.

Now, let $\check{L}$ be the compositum of all the Galois field extensions of L with cyclic Galois group of order dividing p^n. Then $\check{L}$ is clearly Galois over L, and over F, and $\check{L}$ is the maximal abelian p^n-extension of L, i.e., the unique maximal Galois extension of L such that the Galois group is abelian p^n-torsion. Let $X(\check{L}/L) = X(\mathcal{G}(\check{L}/L))$ denote the continuous character group of $\mathcal{G}(\check{L}/L)$,

$$X(\check{L}/L) = \mathit{Hom}(\mathcal{G}(\check{L}/L), \mathbb{Q}/\mathbb{Z}) \qquad \text{(continuous homomorphisms)}.$$

Note that $X(\check{L}/L) \cong \mathit{Hom}(G_L, p^{-n}\mathbb{Z}/\mathbb{Z})$, and that $\mathcal{G}(\check{L}/L) \cong G_L/\cap\{\ker\psi \mid \psi \in \mathit{Hom}(G_L, p^{-n}\mathbb{Z}/\mathbb{Z})\}$.

Because $\check{L}$ is Galois over F and $\mathcal{G}(\check{L}/L)$ is abelian, there is a well-defined group action of $H = \mathcal{G}(L/F)$ on $\mathcal{G}(\check{L}/L)$ given by, for $\tau \in \mathcal{G}(\check{L}/F)$, $\overline{\tau}$ the image of τ in $\mathcal{G}(L/F)$, $\sigma \in \mathcal{G}(\check{L}/L)$, $\overline{\tau} \cdot \sigma = \tau\sigma\tau^{-1}$. This in turn induces a (left) action of H on $X(\check{L}/L)$ given by, for $\psi \in X(\check{L}/L)$,

$$(\overline{\tau} \cdot \psi)(\sigma) = \psi(\overline{\tau}^{-1} \cdot \sigma) = \psi(\tau^{-1}\sigma\tau). \tag{1.8}$$

Since $\mathcal{G}(\check{L}/L)$ and $X(\check{L}/L)$ are p^n-torsion H-modules, each has an eigenmodule decomposition as described in (1.7):

$$\mathcal{G}(\check{L}/L) = \prod_{i=1}^{s} \mathcal{G}(\check{L}/L)^{(\chi_i)} \qquad \text{and} \qquad X(\check{L}/L) = \bigoplus_{i=1}^{s} X(\check{L}/L)^{(\chi_i)}. \tag{1.9}$$

These eigendecompositions are related to each other. Consider the canonical $\mathbb{Z}$-bilinear pairing,

$$B\colon \mathcal{G}(\check{L}/L) \times X(\check{L}/L) \to p^{-n}\mathbb{Z}/\mathbb{Z} \qquad \text{given by } B(\sigma, \psi) = \psi(\sigma). \tag{1.10}$$

If Y is any subgroup of $X(\check{L}/L)$, let $Y^{\perp} = \bigcap_{\psi \in Y} \ker(\psi)$ a closed subgroup of $\mathcal{G}(\check{L}/L)$. Note that B induces an isomorphism $Y \cong X(\mathcal{G}(\check{L}/L)/Y^{\perp})$. Now the pairing in (1.10) is H-equivariant, i.e.,

$$B(h \cdot \sigma, h \cdot \psi) = h \cdot B(\sigma, \psi) = B(\sigma, \psi), \quad \text{for all } h \in H, \sigma \in \mathcal{G}(\check{L}/L), \psi \in X(\check{L}/L). \tag{1.11}$$

For any $\chi \in \{\chi_1, \ldots, \chi_s\}$, let

$$_{\chi}L = \mathcal{F}(\mathcal{N}), \text{ where } \mathcal{N} = \left(X(\check{L}/L)^{(\chi^{-1})}\right)^{\perp}. \tag{1.12}$$

Then, $\mathcal{G}(_{\chi}L/L) \cong \mathcal{G}(\check{L}/L)/\mathcal{N}$, hence $X(_{\chi}L/L) \cong X(\check{L}/L)^{(\chi^{-1})}$. Because H acts by χ^{-1} on $X(_{\chi}L/L)$, it follows from the H-equivariance of the pairing (1.10) that H acts by χ on $\mathcal{G}(_{\chi}L/L)$, i.e., $\mathcal{G}(_{\chi}L/L) = \left(\mathcal{G}(_{\chi}L/L)\right)^{(\chi)}$. Moreover, $_{\chi}L$ is the largest subfield of $\check{L}$ with this property.

Now, look back at the eigendecompositions of $\mathcal{G}(\check{L}/L)$ and $X(\check{L}/L)$ in (1.9). Because the pairing in (1.10) is H-equivariant (and $1 - \chi_i(h)\chi_j(h) \in (\mathbb{Z}/p^n\mathbb{Z})^*$ whenever $\chi_i(h)\chi_j(h) \neq 1$) we have $B(\mathcal{G}(\check{L}/L)^{(\chi_i)}, X(\check{L}/L)^{(\chi_j)}) = 0$ unless $\chi_j = \chi_i^{-1}$, and B induces a nondegenerate pairing between $\mathcal{G}(\check{L}/L)^{(\chi)}$ and $X(\check{L}/L)^{(\chi^{-1})}$ for each $\chi \in \{\chi_1, \ldots, \chi_s\}$. Hence, $\left(X(\check{L}/L^{(\chi_i)})\right)^{\perp} = \bigoplus_{j \neq i} \mathcal{G}(\check{L}/L)^{(\chi_j)}$, so that

$$\mathcal{G}(_{\chi}L/L) \cong \mathcal{G}(\check{L}/L)^{(\chi)} \qquad \text{and} \qquad \check{L} \cong {}_{\chi_1}L \otimes_L \ldots \otimes_L {}_{\chi_s}L\,. \tag{1.13}$$

Corollary 1.6 *Let χ_1 be the trivial character $H \to (\mathbb{Z}/p^n\mathbb{Z})^*$. Then*

$$J \cap \check{L} = {}_{\chi_1}L \qquad \text{and} \qquad \mathcal{G}((J \cap \check{L})/L) \cong \mathcal{G}(\check{L}/L)^H.$$

Furthermore, there is a one-to-one correspondence between the abelian p^n-extensions S of F and the abelian p^n-extensions T of L such that T is Galois over F and H acts trivially on $\mathcal{G}(T/L)$.

PROOF. This is immediate from Prop. 1.4. □

Because $\mu_{p^n} \not\subseteq F$ in general, the abelian p^n-Galois extensions are not classified by subgroups of F^*/F^{*p^n}. We will show in Th. 1.13 below that instead F^*/F^{*p^n} classifies certain abelian p^n-extensions of M, where $M = F(\mu_{p^n})$. This will require some preliminary results. We first make some basic observations about M and group actions of $\mathcal{G}(M/F)$. Note that $M \subseteq J$, by Prop. 1.4, since M is Galois over F with $\mathcal{G}(M/F)$ abelian.

Let $\check{M}$ be the maximal abelian p^n-extension of M; by Kummer theory, $\check{M} = M(\{\sqrt[p^n]{m} \mid m \in M\})$. Then, $\mathcal{G}(M/F)$ acts on the p^n-torsion groups $\mathcal{G}(\check{M}/M)$ and $X(\check{M}/M)$ (analogous to the action described in (1.8) above). So, for each character $\chi\colon \mathcal{G}(M/F) \to (\mathbb{Z}/p^n\mathbb{Z})^*$ we have the eigenmodules $\mathcal{G}(\check{M}/M)^{(\chi)}$ and $X(\check{M}/M)^{(\chi)}$, though the eigenmodules together do not yield a direct sum decomposition of the whole module, since the groupring $\mathbb{Z}/p^n\mathbb{Z}[\mathcal{G}(M/F)]$ is not semisimple when $M \supsetneq L$. Just as for the ${}_\chi L$ defined in (1.12) above, we have the field ${}_\chi M$ which is maximal in $\check{M}$ such that $\mathcal{G}(M/F)$ acts on $\mathcal{G}({}_\chi M/M)$ by χ; also $X({}_\chi M/M) \cong X(\check{M}/M)^{(\chi^{-1})}$.

We can relate these eigenmodules to those of M^*/M^{*p^n}. For $m \in M^*$, we write $[m]$ for its image in M^*/M^{*p^n}. From Kummer theory, we have the following isomorphisms,

$$M^*/M^{*p^n} \to \mathit{Hom}(\mathcal{G}(\check{M}/M), \mu_{p^n}) \cong X(\check{M}/M) \otimes_{\mathbb{Z}} \mu_{p^n}\,, \tag{1.14}$$

where the first map is given by $[m] \mapsto (\sigma \mapsto \sigma(a)/a)$, for any $a \in \check{M}^*$ such that $a^{p^n} = m$. Now, $\mathcal{G}(M/F)$ acts on each of the groups in (1.14) (it acts on $\gamma \in \mathit{Hom}(\mathcal{G}(\check{M}/M), \mu_{p^n})$ by $(\overline{g} \cdot \gamma)(\sigma) = \overline{g}(\gamma(g^{-1}\sigma g))$, for any $g \in \mathcal{G}(L(p)/F)$ restricting to $\overline{g} \in \mathcal{G}(M/F)$); it is easy to check that each of the isomorphisms in (1.14) is compatible with the $\mathcal{G}(M/F)$-action. Thus, if we let α be the cyclotomic character, which corresponds to the action of $\mathcal{G}(M/F)$ on μ_{p^n}, i.e.

$$\alpha\colon \mathcal{G}(M/F) \to (\mathbb{Z}/p^n\mathbb{Z})^* \text{ is given by } g(\omega) = \omega^{\alpha(g)} \text{ for all } g \in \mathcal{G}(M/F) \text{ and } \omega \in \mu_{p^n}, \tag{1.15}$$

then (1.14) shows that as $\mathcal{G}$-modules,

$$M^*/M^{*p^n} \cong X(\check{M}/M)_\alpha\,. \tag{1.16}$$

It follows that for any character $\chi\colon H \to (\mathbb{Z}/p^n\mathbb{Z})^*$, we have

$${}_\chi M = M(\{\sqrt[p^n]{m} \mid [m] \in (M^*/M^{*p^n})^{(\alpha\chi^{-1})}\}), \tag{1.17}$$

since $X({}_\chi M/M) \cong X(\check{M}/M)^{(\chi^{-1})} = (X(\check{M}/M)_\alpha)^{(\alpha\chi^{-1})} \cong (M^*/M^{*p^n})^{(\alpha\chi^{-1})}$. (One can also deduce (1.17) from the $\mathcal{G}(M/F)$-equivariant Kummer pairing $\mathcal{G}(\check{M}/M) \times M^*/M^{*p^n} \to \mu_{p^n}$.) Note that if $[m] \in (M^*/M^{*p^n})^{(\alpha\chi^{-1})}$, then $M(\sqrt[p^n]{m})$ is Galois over F, since the cyclic subgroup $\langle [m] \rangle \subseteq$

M^*/M^{*p^n} is stable under the action of $\mathcal{G}(M/F)$. Conversely, if $M(\sqrt[p^n]{m})$ is Galois over F, then $\langle[m]\rangle$ must be $\mathcal{G}(M/F)$-stable, so $[m] \in (M^*/M^{*p^n})^{(\varphi)}$ for some character φ. However, $M(\sqrt[p^n]{m})$ is *abelian* Galois over M iff $\mathcal{G}(M/F)$ acts trivially on $\mathcal{G}(M(\sqrt[p^n]{m})/M)$, iff $M(\sqrt[p^n]{m}) \subseteq {}_{\chi_1}M$, where χ_1 is the trivial character, iff (by (1.17)) $[m] \in (M^*/M^{*p^n})^{(\alpha)}$.

We will relate this to F^*/F^{*p^n} below. But first, let us observe how it yields a slight generalization of Albert's characterization of the cyclic extensions of F of degree p (see [A_1, Th. 2] or [A_2, p. 211, Th. 15]).

Proposition 1.7 *Suppose $p \nmid [F(\mu_{p^n}) : F]$. Let $M = F(\mu_{p^n})$, $m \in M^* - M^{*p}$, and $T = M(\sqrt[p^n]{m})$. Then, $T = S \cdot M$ for some cyclic field extension S of F of degree p^n iff $T \subseteq J$, iff $g \cdot [m] = [m^{\alpha(g)}]$ in M^*/M^{*p^n} for each $g \in \mathcal{G}(M/F)$, where $\alpha\colon \mathcal{G}(M/F) \to (\mathbb{Z}/p\mathbb{Z})^*$ is the cyclotomic character described in* (1.15) *above.*

Proof. Since $[M : L]$ is a power of p, the assumption that $p \nmid [F(\mu_{p^n}) : F]$ is equivalent to: $M = L$, i.e., $\mu_{p^n} \subseteq F(\mu_p)$. For $T = M(\sqrt[p^n]{m})$, we have $T = S \cdot M$ for some cyclic Galois extension S of F with $[S : F] = [T : M] = p^n$ iff $T \subseteq J \cap \check{M}$ (see Prop. 1.4). But, by Cor. 1.6, $J \cap \check{M} = {}_{\chi_1}M$, where $\chi_1\colon \mathcal{G}(M/F) \to (\mathbb{Z}/p^n\mathbb{Z})^*$ is the trivial character. As noted in (1.17), ${}_{\chi_1}M = M(\{\sqrt[p^n]{c} \mid [c] \in (M^*/M^{*p^n})^{(\alpha)}\}$ So, $T = S \cdot M$ iff $T \subseteq {}_{\chi_1}M$ iff (by Kummer theory) $[m] \in (M^*/M^{*p^n})^{(\alpha)}$, as desired. □

Remarks 1.8 (a) Albert's result is the case $n = 1$ of Prop. 1.7, for which the assumption that $p \nmid [F(\mu_p) : F]$ always holds. Note that the hypothesis that $p \nmid [F(\mu_{p^n}) : F]$ is needed for Prop. 1.7. For, when $M = F(\mu_{p^n}) \supsetneq F(\mu_p)$, we do have $X(\check{M}/M)^{\mathcal{G}(M/F)} \cong (M^*/M^{*p^n})^{(\alpha)}$ as $\mathcal{G}(M/F)$-modules (see (1.16)). But the abelian p^n-extensions of M coming from such extensions of F correspond to the image of $X(\check{F}/F)$ in $X(\check{M}/M)$, which is properly smaller than $X(\check{M}/M)^{\mathcal{G}(M/F)}$. Specifically, if we take $\omega \in \mu_{p^{n^*}} \subseteq M^*$, then clearly $[\omega] \in (M^*/M^{*p^n})^{(\alpha)}$ and $[\omega]$ has order p^n in M^*/M^{*p^n} (see Lemma 1.9 below). Then, for $\psi \in X(\check{M}/M)$ with $ker(\psi) = \mathcal{G}(\check{M}/M(\sqrt[p^n]{\omega}))$, we have $\psi \in X(\check{M}/M)^{\mathcal{G}(M/F)}$, but ψ is not in the image of $X(\check{F}/F)$, since there is no cyclic p^n-extension S of F with $S \cdot M = M(\sqrt[p^n]{\omega})$. (For, $M(\sqrt[p^n]{\omega}) \cap F(p)$ is cyclic over F, but of degree greater than p^n.) However, this example is, roughly speaking, the only obstruction when $M \supsetneq L$. For, one can check that $\check{F} \cdot M(\sqrt[p^n]{\omega}) = {}_{\chi_1}M$, which is is the subfield of $\check{M}$ corresponding to $X(\check{M}/M)^{\mathcal{G}(M/F)}$. (This follows from the observations that if $[M : L] = p^{n-c}$ as in Lemma 1.9 below, then $\left|X(\check{M}/M)^{\mathcal{G}(M/F)} : im(X(\check{F}/F))\right| \leq \left|H^2(\mathcal{G}(M/F), \mathbb{Z}/p^n\mathbb{Z})\right| = p^{n-c}$ while $[\check{F} \cdot M(\sqrt[p^n]{\omega}) : \check{F} \cdot M] = p^{n-c}$.)

(b) For a closely related description of the cyclic extensions of F of degree p^n, see [Sa, Th. 2.3]. Saltman's description does not require the hypothesis that $\mu_{p^n} \subseteq F(\mu_p)$.

We want to relate F^*/F^{*p^n} to M^*/M^{*p^n}, and use F^*/F^{*p^n} to parametrize certain field extensions of M. For this, we first need the following two lemmas.

Lemma 1.9 *Let $d = \sup\{k \mid \mu_{p^k} \subseteq L\} \in \mathbb{N} \cup \infty$ and let $c = min(d, n)$. Then, $[M : L] = p^{n-c}$.*

Proof. We can assume that $n > c$, since otherwise there is nothing to prove. Let ω be a primitive p^n-th root of unity, and let $\nu = \omega^p$ and $\varepsilon = \omega^{p^{n-c}} \in L$. Let $M_0 = L(\mu_{p^{n-1}}) = L(\nu)$. By induction

on n we may assume that $[M_0 : L] = p^{n-c-1}$. Then $f(x) = x^{p^{n-c-1}} - \varepsilon$ is the minimal polynomial of ν over L, since it has the right degree and $f(\nu) = 0$. Hence, for the norm from M_0 to L, we have $N_{M_0/L}(\nu) = (-1)^{p^{n-c-1}}(-\varepsilon) = \varepsilon$ (as p is odd).

Since $M = M_0(\omega) = M_0(\nu^{1/p})$ and $\mu_p \subseteq M_0$, M is a p-Kummer extension of M_0. So $[M : M_0] = p$ or $= 1$. If $[M : M_0] = 1$, then $\omega \in M_0$, so $\varepsilon = (N_{M_0/L}(\omega))^p$, so $N_{M_0/L}(\omega)$ is a primitive p^{c+1} root of unity in L, contradicting the definition of c (as $n > c$). Thus, we must have $[M : M_0] = p$, so $[M : L] = [M : M_0][M_0 : L] = p^{n-c}$ as desired. □

Lemma 1.10 $H^1(\mathcal{G}(M/L), \mu_{p^n}) = H^2(\mathcal{G}(M/L), \mu_{p^n}) = 1$.

Proof. Because $\mathcal{G}(M/L)$ is cyclic (as p is odd), $H^2(\mathcal{G}(M/L), \mu_{p^n}) \cong (\mu_{p^n})^{\mathcal{G}(M/L)}/N_{M/L}(\mu_{p^n})$. Now $(\mu_{p^n})^{\mathcal{G}(M/L)} = \mu_{p^n} \cap L = \mu_{p^c}$. Let $\omega \in \mu_{p^{n^*}}$, and let $\varepsilon = \omega^{p^{n-c}} \in \mu_{p^{c^*}} \subseteq L$. Since $M = L(\omega)$ and $[M : L] = p^{n-c}$ by Lemma 1.9, ω has minimal polynomial $x^{p^{n-c}} - \varepsilon$ over L, so $N_{M/L}(\omega) = (-1)^{p^{n-c}}(-\varepsilon) = \varepsilon$. Thus, $N_{M/L}(\mu_{p^n}) = \langle N_{M/L}(\omega)\rangle = \langle\varepsilon\rangle = \mu_{p^c} = (\mu_{p^n})^{\mathcal{G}(M/L)}$. Hence $H^2(\mathcal{G}(M/L), \mu_{p^n}) = 1$, and, as $\mathcal{G}(M/L)$ is cyclic and μ_{p^n} is finite, the Herbrand quotient [S_1, p. 134, Prop. 8] shows that $\big|H^1(\mathcal{G}(M/L), \mu_{p^n})\big| = \big|H^2(\mathcal{G}(M/L), \mu_{p^n})\big|$. □

Corollary 1.11

(i) $L^*/L^{*p^n} \cong (M^*/M^{*p^n})^{\mathcal{G}(M/L)}$.

(ii) $F^*/F^{*p^n} \cong (L^*/L^{*p^n})^{\mathcal{G}(L/F)} \cong (M^*/M^{*p^n})^{\mathcal{G}(M/F)}$.

Proof. (i) From the 5-term exact sequence of low degree terms associated with the Hochschild-Serre spectral sequence (cf. [R, p. 307, Th. 11.5], the following is exact:

$$H^1(\mathcal{G}(M/L), \mu_{p^n}^{G_M}) \to H^1(G_L, \mu_{p^n}) \to H^1(G_M, \mu_{p^n})^{G(M/L)} \to H^2(\mathcal{G}(M/L), \mu_{p^n}^{G_M}).$$

Since $\mu_{p^n}^{G_M} = \mu_{p^n}$, Lemma 1.10 applies, yielding

$$H^1(G_L, \mu_{p^n}) \cong H^1(G_M, \mu_{p^n})^{\mathcal{G}(M/L)}. \tag{1.18}$$

The long exact cohomology sequence arising from the short exact sequence of G_L-modules

$$1 \longrightarrow \mu_{p^n} \longrightarrow L(p)^* \xrightarrow{(\ )^{p^n}} L(p)^* \longrightarrow 1 \tag{1.19}$$

(the p^n-power map $L(p) \to L(p)$ is onto by Cor. 1.3), yields $H^1(G_L, \mu_{p^n}) \cong L^*/L^{*p^n}$; likewise $H^1(G_M, \mu_{p^n}) \cong M^*/M^{*p^n}$. Thus, the isomorphism in (1.18) translates to $L^*/L^{*p^n} \cong (M^*/M^{*p^n})^{\mathcal{G}(M/L)}$, as desired.

(ii) The first isomorphism in (ii) can be proved in the same way as (i), using that $H^i(\mathcal{G}(L/F), (\mu_{p^n})^{G_L}) = 1$ for $i = 1, 2$; this is clear, as $gcd(|\mathcal{G}(L/F)|, |(\mu_{p^n})^{G_L}|) = 1$. But the desired isomorphism can also be obtained easily nonhomologically: Injectivity of the map $F^*/F^{*p^n} \to (L^*/L^{*p^n})^{\mathcal{G}(L/F)}$ follows by an evident norm argument; surjectivity of this map follows using Hilbert's Th. 90. The second isomorphism in (ii) follows from the isomorphism in part (i). □

Remarks 1.12 (a) Lemma 1.10 and Cor. 1.11 are special to n where $M = L(\mu_{p^n})$. One can compute analogously to Lemma 1.10 that for $k \le n$ and any $i \ge 1$

$$\left|H^i(\mathcal{G}(M/L), \mu_{p^k})\right| = |\mu_{p^a}/\mu_{p^b}| = p^{a-b},$$

where $a = min(k, c)$ and $b = max(k + c - n, 0)$. So, for $0 < k < n$, $\left|H^i(\mathcal{G}(M/L), \mu_{p^k})\right| > 0$ and the map $L^*/L^{*p^k} \to (M^*/M^{*p^k})^{\mathcal{G}(M/L)}$ is neither 1-1 nor onto.

(b) On the other hand, for every $k \ge n$, the map $L^*/L^{*p^k} \to M^*/M^{*p^k}$ is injective. More generally, for any field $K \supseteq L$, if the map $L^*/L^{*p^n} \to K^*/K^{*p^n}$ is injective, then the map $L^*/L^{*p^k} \to K^*/K^{*p^k}$ is injective for every $k \ge n$. This is a special case of the following group theoretic observation: If $A \subseteq B$ are abelian groups such that the map $A/p^nA \to B/p^nB$ is injective and if $p^{k-2}({}_{p^{k-1}}B) \subseteq A$ for all $k > n$, then the map $A/p^kA \to B/p^kB$ is injective for all $k > n$. (Here ${}_{p^{k-1}}B$ denotes the p^{k-1}-torsion subgroup of B.) This is easily proved by induction on k. One can also check that $L^*/L^{*p^k} \cong (M^*/M^{*p^k})^{\mathcal{G}(M/L)}$ for every $k \ge n$.

We can now give an answer to the question: What do F^*/F^{*p^n} and L^*/L^{*p^n} classify when $\mu_p \not\subseteq F$? The answer, a kind of generalized Kummer theory, is given not in terms of field extensions of F or L, but those of $M = F(\mu_{p^n})$. In the following Theorem 1.13 we are no longer assuming that $\mu_p \not\subseteq F$. Hence, the F appearing there could be either the F or the L of the preceding results.

Theorem 1.13 *Let p be an odd prime number. Let F be any field with $char(F) \neq p$, and let $M = F(\mu_{p^n})$. Let $\alpha\colon \mathcal{G}(M/F) \to (\mathbb{Z}/p^n\mathbb{Z})^*$ be the cyclotomic character, as in* (1.15)*. Then, there is a one-to-one correspondence between the subgroups U of F^*/F^{*p^n} and the abelian Galois extensions K of M such that $exp(\mathcal{G}(K/M)) \mid p^n$, K is Galois over F, and $\mathcal{G}(M/F)$ acts on $\mathcal{G}(K/M)$ via α.*

Proof. One lemma needed for this proof is deferred until the end of this section for ease of exposition. Let $\mathcal{G} = \mathcal{G}(F(\mu_p)(p)/F)$, and let α denote also the composition $\mathcal{G} \to \mathcal{G}(M/F) \xrightarrow{\alpha} (\mathbb{Z}/p^n\mathbb{Z})^*$, which is the cyclotomic character for the action of $\mathcal{G}$ on μ_{p^n}.

We have $\mathcal{G}$-module isomorphisms

$$M^*/M^{*p^n} \to Hom(\mathcal{G}(\check{M}/M), \mu_{p^n}) \to X(\check{M}/M) \otimes \mu_{p^n} \to X(\check{M}/M)_\alpha, \tag{1.20}$$

where the first map is the one in Kummer theory: $[m] \to (\sigma \mapsto \sigma(a)/a)$ for any $a \in \check{M}$ with $a^{p^n} = m$. The last map depends on a choice of generator ω of μ_{p^n}, and is given by $\psi \otimes \omega^j \mapsto j\psi$. By composing these isomorphisms with the identity map $\iota\colon X(\check{M}/M)_\alpha \to X(\check{M}/M)$ (not a $\mathcal{G}$-homomorphism), we have a bijective function $f\colon M^*/M^{*p^n} \to X(\check{M}/M)$. By Cor. 1.11 (i) or (ii), the isomorphisms of (1.20) map F^*/F^{*p^n} onto $(X(\check{M}/\check{M})_\alpha)^{\mathcal{G}(M/F)}$ which ι sends onto $X(\check{M}/M)^{(\alpha^{-1})}$. Thus, f yields a one-to-one correspondence between subgroups of F^*/F^{*p^n} and subgroups of $X(\check{M}/M)^{(\alpha^{-1})}$.

Now, the subgroups Y of $X(\check{M}/M)$ are in one-to-one correspondence with the closed subgroups C of $\mathcal{G}(\check{M}/M)$, where $Y = \{\psi \in X(\check{M}/M) \mid ker(\psi) \supseteq C\}$ and $C = \bigcap_{\psi \in Y} ker(\psi)$. In the Galois correspondence, every closed subgroup C of $\mathcal{G}(\check{M}/M)$ corresponds to an intermediate field K, $M \subseteq K \subseteq \check{M}$, where $K = \mathcal{F}(C)$, the fixed field of C, and $C = \mathcal{G}(\check{M}/K) \cong G_K/G_{\check{M}}$. Suppose

$Y \leftrightarrow C \leftrightarrow K$ (so $Y = X(K/M) \subseteq X(\check{M}/M)$). We have seen that Y corresponds to a subgroup of F^*/F^{*p^n} iff $Y \subseteq X(\check{M}/M)^{(\alpha^{-1})}$; by Lemma 1.15 below (with $G = \mathcal{G}$, $P = G_{\check{M}}$, $Q = G_M$, $R = G_K$), this occurs iff G_K is normal in $\mathcal{G}$ (i.e., K is Galois over F) and $\mathcal{G}$ acts on $\mathcal{G}(K/M)$ via α. The last condition is equivalent to: $\mathcal{G}(M/F)$ acts on $\mathcal{G}(K/M)$ via α. □

Remarks 1.14 (a) In the correspondence of Th. 1.13, a subgroup U of F^*/F^{*p^n} corresponds to the field $K = M(\{\sqrt[p^n]{b} \mid [b] \in U\})$. Conversely, for a given field K, the corresponding subgroup of F^*/F^{*p^n} is $\{[b] \mid b \in K^{p^n} \cap F^*\}$. As usual in Kummer Theory, the correspondence is a lattice isomorphism, so it preserves inclusions, intersection and joins; when $U \leftrightarrow K$ we have $|U| = [K : M]$, and U and $\mathcal{G}(K/M)$ are (Pontrjagin) dual to each other. In particular, $|U| < \infty$ iff $|\mathcal{G}(K/M)| < \infty$, and when this occurs, $U \cong \mathcal{G}(K/M)$ (noncanonically).

(b) One would prefer a correspondence between cyclic subgroups of F^*/F^{*p^n} and simple radical extensions of F of degree dividing p^n. But this does not work when $\mu_{p^n} \nsubseteq F$. For example take any $b \in F^*$ with $[b]$ of order p^n in F^*/F^{*p^n}. Let $K = F(a)$ for some choice of a with $a^{p^n} = b$. Then (as $b \notin F^{*p}$ with p odd, so $x^{p^n} - b$ is irreducible in $F[x]$), $[K : F] = p^n$, and also $[K \cdot M : M] = p^n$, by Cor. 1.11. Hence, K and M are linearly disjoint over F. So, when $M \neq F$, i.e., $\mu_{p^n} \nsubseteq F$, then $\mu_{p^n} \nsubseteq K$, so K does not contain all the p^n-th roots of b. Thus, the field K depends on the choice of a among the p^n-th roots of b, but $K \cdot M$ does not depend on such a choice. For another example, for $L = F(\mu_p)$, assume $\mu_{p^n} \nsubseteq L$ and let $\varepsilon \in \mu_{p^c}^* \subseteq L$ with c as large as possible, as in Lemma 1.9. Then $[L(\sqrt[p^n]{\varepsilon}) : L] = p^n$, by Lemma 1.9, but $[M(\sqrt[p^n]{\varepsilon}) : M] = p^c$, so $[\varepsilon]$ has order p^c in L^*/L^{*p^n} by Cor 1.11.

(c) Theorem 1.13 indicates the divergence between p^n-th power classes and cyclic p^n field extensions of F when $\mu_{p^n} \nsubseteq F$: We have $F^*/F^{*p^n} \cong (M^*/M^{*p^n})^{\mathcal{G}(M/F)}$, while cyclic field extensions of F of degree dividing p^n correspond to cyclic subgroups of $X(\check{F}/F)$, which map (not quite isomorphically) to $X(\check{M}/M)^{\mathcal{G}(M/F)} \cong (H^1(G_M, \mu_{p^n})_{\alpha^{-1}})^{\mathcal{G}(M/F)} \cong (M^*/M^{*p^n})^{(\alpha)}$. So the p^n-th power classes of F and cyclic extensions of F correspond to different eigenspaces for the $\mathcal{G}(M/F)$ action on M^*/M^{*p^n}.

(d) For Th. 1.13 we required that p be odd. For $p = 2$ the theorem is valid, with the same proof, for any field F ($char(F) \neq 2$) such that $\mu_4 \subseteq F$, and $M = F(\mu_{2^n})$ for any n. But if $\mu_4 \nsubseteq F$, the theorem fails already for $n = 2$, since then $-4 \notin F^{*4}$ but $-4 \in F(\mu_4)^{*4}$ (as $(1 + \sqrt{-1})^4 = -4$), so the map $F^*/F^{*4} \to F(\mu_4)^*/F(\mu_4)^{*4}$ is not injective.

The following lemma will complete the proof of Theorem 1.13. For the lemma, let G be a profinite group and let P and Q be closed normal subgroups of G with $P \subseteq Q$. Suppose Q/P is an abelian torsion group of exponent dividing some $e \in \mathbb{N}$. Let $\chi\colon G \to (\mathbb{Z}/e\mathbb{Z})^*$ be any continuous group homomorphism.

Lemma 1.15 *Let R be a closed subgroup of G with $P \subseteq R \subseteq Q$. Then, $X(Q/R) \subseteq X(Q/P)^{(\chi)}$ iff R is normal in G and G acts on Q/R via χ^{-1}.*

Proof. The action of G on Q by conjugation induces the action of G on Q/P; then G acts on $X(Q/P)$ by $(g \cdot \psi)(qP) = \psi(g^{-1} \cdot (qP)) = \psi(g^{-1}qg)P)$, for all $g \in G$, $\psi \in X(Q/P)$, $q \in Q$. For

every closed subgroup R of G with $P \subseteq R \subseteq Q$, the character group $X(Q/R)$ embeds in $X(Q/P)$ using the surjection $Q/P \to Q/R$; we use this embedding to view $X(Q/R) \subseteq X(Q/P)$.

Now, suppose $X(Q/R) \subseteq X(Q/P)^{(\chi)}$. This means that

$$\psi'(g^{-1} \cdot (qP)) = \psi'(q^{\chi(g)}P) \qquad \text{for all} \qquad q \in Q,\ g \in G,\ \psi \in X(Q/R), \tag{1.21}$$

where ψ' denotes the image of ψ in $X(Q/P)$. Observe that $\bigcap_{\psi \in X(Q/R)} ker(\psi') = R/P$. It follows from (1.21) that for each $r \in R$ and $g \in G$ we have $(g^{-1}rg)P = r^{\chi(g)}P \in R/P$. Hence, R is a normal subgroup of G. So, G acts on Q/R, and (1.21) translates to

$$\psi(g^{-1} \cdot (qR)) = \psi(q^{\chi(g)}R) \qquad \text{for all} \qquad q \in Q,\ g \in G,\ \psi \in X(Q/R). \tag{1.22}$$

Because $\bigcap_{\psi \in X(Q/R)} ker(\psi)$ is trivial, it follows that $g \cdot (qR) = (qR)^{\chi(g^{-1})}$ for all $q \in Q$, $g \in G$, i.e., G acts on Q/R via χ^{-1}, as desired.

Conversely, if R is normal in G and G acts on Q/R via χ^{-1}, then $g \cdot (qR) = (qR)^{\chi^{-1}(g)}$ for all $g \in G$, $q \in Q$; so (1.22) holds, and this shows that G acts on $X(Q/R)$ via χ. □

2 "$H^1(G_F, \mu_{p^n})$"

In the analysis of Demushkin groups as Galois groups in [MW$_1$] and [MW$_2$], the authors needed to show that for any field F ($char(F) \neq p$) there is an action of G_F on $\mathbb{Z}/p^n\mathbb{Z}$ so that the map $H^1(G_F, \mathbb{Z}/p^n\mathbb{Z}) \to H^1(G_F, \mathbb{Z}/p\mathbb{Z})$ is surjective. This does not hold in general for the trivial action on $\mathbb{Z}/p^n\mathbb{Z}$ (see Remark 2.6 below) but the authors pointed out in [MW$_2$, proof of Th. 2.2] that this does hold if we replace $\mathbb{Z}/p^n\mathbb{Z}$ by μ_{p^n}. Of course $\mathbb{Z}/p^n\mathbb{Z} \cong \mu_{p^n}$ as abstract groups, but they have different G_F-actions, and the action of G_F on μ_{p^n} is defined iff $\mu_{p^n} \subseteq F(p)$, iff $\mu_p \subseteq F$. The present paper was originally motivated by the need to handle the case where $\mu_p \nsubseteq F$ (so p is odd). We will do this in Cor. 2.5 below, by realizing "$H^1(G_F, \mu_{p^n})$" as an eigenmodule of L^*/L^{*p^n}, where $L = F(\mu_p)$ (see Th. 2.3). We also show in Th. 2.7 that the subgroups of "$H^1(G_F, \mu_{p^n})$" classify certain abelian p^n-extensions of $F(\mu_{p^n})$ and such extensions of $F(\mu_{p^n}) \cap F(p)$.

We assume throughout this section that p is an odd prime number, and that F is a field with $char(F) \neq p$ and that $\mu_p \nsubseteq F$. Then let $L = F(\mu_p)$, and let J, G_F, $\mathcal{G}$, and H be as defined in the Introduction. Let $\Gamma_F = \mathcal{G}(J/L)$. We need to give meaning to "$H^1(G_F, \mu_{p^n})$", since μ_{p^n} is not a G_F-module. One approach would be to take this to mean $H^1(\Gamma_F, \mu_{p^n})$ since $\Gamma_F \cong G_F$ and Γ_F does act on μ_{p^n}. But we will take a somewhat different approach by replacing μ_{p^n} by a twisted version $\widetilde{\mu_{p^n}}$ on which G_F does act; then "$H^1(G_F, \mu_{p^n})$" will be replaced by $H^1(G_F, \widetilde{\mu_{p^n}})$, which is in fact isomorphic to $H^1(\Gamma_F, \mu_{p^n})$—see Th. 2.3(iii). We will need to keep track of how twisting a module by a character affects the action of the Galois group on the cohomology groups of a normal subgroup, and this is described by our first lemma.

Lemma 2.1 *Let G be a profinite group, and let K be a closed normal subgroup of G. Let A be a discrete p^n-torsion G-module, and let $\chi\colon G \to (\mathbb{Z}/p^n\mathbb{Z})^*$ be a continuous character such that $K \subseteq ker(\chi)$. Then, for the χ-twisted G-module A_χ as in* (1.3) *above,*

$$H^i(K, A_\chi) \cong H^i(K, A)_\chi$$

as G-(i.e., G/K-) modules.

Proof. Let $\cdot$ denote the action of G on A and on $Z^i(K, A)$. Let $*$ denote the action of G on A_χ and on $Z^i(K, A)_\chi$. So for the identity map $j\colon A_\chi \to A$ given by $a \mapsto a$, we have $j(g * a) = \chi(g)(g \cdot j(a))$ for all $g \in G$, $a \in A$. Since j is a K-module isomorphism, it induces a group isomorphism on continuous cocycles, $j^*\colon Z^i(K, A_\chi) \to Z^i(K, A)$, given by $j^*(f) = j \circ f$. For $k \in K$, $g \in G$, write k^g for $g^{-1}kg$. Then, for all $g \in G$, $f \in Z^i(K, A_\chi)$, $k_1, \ldots, k_i \in K$, we have

$$\begin{aligned}[j^*(g \cdot f)](k_1, \ldots, k_i) &= j(g * f(k_1^g, \ldots, k_i^g)) \\ &= \chi(g)(g \cdot j(f(k_1^g, \ldots, k_i^g))) \\ &= \chi(g)[(g \cdot j^*(f))(k_1, \ldots, k_i)].\end{aligned}$$

So, $j^*(g \cdot f) = \chi(g)g \cdot j^*(f) = g * j^*(f)$, showing that j^*, viewed as a (bijective) mapping $Z^i(K, A_\chi)$ to $Z^i(K, A)_\chi$ is a G-module homomorphism. Thus, j^* induces a G-module isomorphism $H^i(K, A_\chi) \to H^i(K, A)_\chi$. □

We now return to our specific setting where $\mathcal{G} = \mathcal{G}(L(p)/F)$, $N = \mathcal{G}(L(p)/F(p))$, etc.

Lemma 2.2 *Let A be any p-primary torsion abelian group which is a discrete $\mathcal{G}$-module on which N acts trivially (i.e., A is a G_F-module). Then, there are $\mathcal{G}$-module maps*

$$\begin{aligned}&H^1(G_F, A) \cong H^1(\Gamma_F, A) \cong H^1(G_L, A)^H, \qquad \textit{and} \\ &H^2(G_F, A) \cong H^2(\Gamma_F, A) \hookrightarrow H^2(G_L, A).\end{aligned}$$

Proof. Consider the commutative diagram of $\mathcal{G}$-module maps

$$\begin{array}{ccc} H^i(G_F, A) & \xrightarrow{inf} & H^i(\mathcal{G}, A) \\ \downarrow & & \downarrow{\scriptstyle res} \\ H^i(\Gamma_F, A) & \xrightarrow{inf} & H^i(G_L, A) \end{array} \tag{2.1}$$

Here the left vertical map is the isomorphism induced by the isomorphism $G_F \to \Gamma_F$, which is compatible with the actions of these groups on A, and with the action of $\mathcal{G}$ on these groups. The right vertical restriction map in (2.1) has image lying in $H^1(G_L, A)^{\mathcal{G}} = H^1(G_L, A)^H$ (as $H \cong \mathcal{G}/G_L$), and G_L acts trivially on $H^i(G_L, -)$). Indeed, this map is injective with image all of $H^i(G_L, A)^H$ as A is p-primary and G_L is the p-Sylow subgroup of $\mathcal{G}$. (For, the map $cor \circ res\colon H^i(\mathcal{G}, A) \to H^i(\mathcal{G}, A)$ is multiplication by $|\mathcal{G}/G_L| = |H|$ on the p-primary group $H^i(\mathcal{G}, A)$, so it is an isomorphism. This shows res is injective. On the other hand, $res \circ cor\colon H^i(G_L, A) \to H^i(G_L, A)$ is multiplication by $|H|$ on $H^i(G_L, A)^H$, so it maps this p-primary subgroup to itself.)

Now, recall the five term exact sequence of low degree terms on cohomology associated with the short exact sequence $1 \to N \to \mathcal{G} \to G_F \to 1$:

$$0 \to H^1(G_F, A^N) \xrightarrow{inf} H^1(\mathcal{G}, A) \xrightarrow{res} H^1(N, A)^{G_F} \to H^2(G_F, A^N) \xrightarrow{inf} H^2(\mathcal{G}, A) \tag{2.2}$$

Since N acts trivially on A, we have $H^1(N, A) = Hom(N, A)$ (continuous homomorphisms); but $Hom(N, A) = 0$ as A is p-primary torsion and N has no cyclic factor groups of order p (as $F(p)$ is p-closed). Thus (2.2) shows that the inflation map $H^1(G_F, A) \to H^1(\mathcal{G}, A)$ is an isomorphism, hence (2.1) shows $H^1(\Gamma_F, A) \to H^1(G_L, A)^H$ is an isomorphism. Similarly, (2.2) shows that $H^2(G_F, A^N) \to H^2(\mathcal{G}, A)$ is injective, so (2.1) yields the injectivity of $H^2(\Gamma_F, A) \to H^2(G_L, A)$. □

We now apply these lemmas to the $\mathcal{G}$-module μ_{p^n}. We need the following characters: First let $\alpha\colon \mathcal{G} \to (\mathbb{Z}/p^n\mathbb{Z})^*$ be the cyclotomic character for the action of $\mathcal{G}$ on μ_{p^n}; that is, for all $\omega \in \mu_{p^n}$ and all $g \in \mathcal{G}$

$$g(\omega) = \omega^{\alpha(g)}, \tag{2.3}$$

analogous to (1.15) above. Then, let $\theta\colon \mathcal{G} \to (\mathbb{Z}/p^n\mathbb{Z})^*$ be the unique character such that

$$\theta|_N = \alpha \qquad \text{and} \qquad \theta|_{G_L} = 1. \tag{2.4}$$

(Such a θ is unique because $\mathcal{G} = N \cdot \mathcal{G}_L$ and it exists since $\alpha|_{N \cap G_L} = \alpha|_{\mathcal{G}(L(p)/J)} = 1$.) Indeed, observe that $\theta = \alpha^{p^{n-1}}$ has the properties specified in (2.4). For, since $(\mathbb{Z}/p^n\mathbb{Z})^* \cong (\mathbb{Z}/p^{n-1}\mathbb{Z}) \times (\mathbb{Z}/(p-1)\mathbb{Z})$, our α must map the pro-p group G_L into $\mathbb{Z}/p^{n-1}\mathbb{Z}$, so $\alpha^{p^{n-1}}|_{G_L} = 1$; also, as $|N/G_J| = |\mathcal{H}|$ and $|\mathcal{H}| \mid (p-1)$, this α maps N into $\mathbb{Z}/(p-1)\mathbb{Z}$, so $\alpha^{p^{n-1}}|_N = \alpha|_N$. Note, in fact that θ coincides with the prime-to-p part of α, i.e., the composition of α with the projection $(\mathbb{Z}/p^n\mathbb{Z})^* \to \mathbb{Z}/(p-1)\mathbb{Z}$. Likewise, $\alpha\theta^{-1}$ is the p-primary part of α. To get a G_F-module structure from μ_{p^n}, we need to twist μ_{p^n} by a character to get a trivial N-action. But we use θ^{-1} rather than α^{-1} in order to have a character trivial on G_L, so that we can invoke Lemma 2.1.

Theorem 2.3 *Let $\widetilde{\mu_{p^n}} = (\mu_{p^n})_{\theta^{-1}}$ for the character θ defined in* (2.4) *above. Then $\widetilde{\mu_{p^n}}$ is a G_F-module, and*

(i) $H^1(G_F, \widetilde{\mu_{p^n}}) \cong H^1(G_L, \mu_{p^n})^{(\theta)} \cong (L^*/L^{*p^n})^{(\theta)}$;

(ii) $H^2(G_F, \widetilde{\mu_{p^n}}) \hookrightarrow H^2(G_L, \mu_{p^n})^{(\theta)}$;

(iii) *For all $i \geq 0$, $H^i(G_F, \widetilde{\mu_{p^n}}) \cong H^i(\Gamma_F, \mu_{p^n})$ as groups, but $\mathcal{G}$ acts trivially on $H^i(G_F, \widetilde{\mu_{p^n}})$, while $\mathcal{G}$ acts via θ on $H^1(\Gamma_F, \mu_{p^n})$.*

Proof. Since N acts on μ_{p^n} via α and $\theta|_N = \alpha$, N acts trivially on the θ^{-1}-twist $\widetilde{\mu_{p^n}}$ of μ_{p^n}. Hence, there is a well-defined action of $G_F \cong \mathcal{G}/N$ on $\widetilde{\mu_{p^n}}$. Because $G_F \cong \Gamma_F$, with the isomorphism compatible with the action of $\mathcal{G}$ on these groups, and with the action of these groups on $\widetilde{\mu_{p^n}}$, we have the $\mathcal{G}$-module isomorphism $H^i(G_F, \widetilde{\mu_{p^n}}) \cong H^i(\Gamma_F, \widetilde{\mu_{p^n}})$, for all $i \geq 0$. To prove (i), we have the isomorphisms

$$\begin{aligned} H^1(G_F, \widetilde{\mu_{p^n}}) &\cong H^1(\Gamma_F, \widetilde{\mu_{p^n}}) \cong H^1(G_L, \widetilde{\mu_{p^n}})^H \\ &\cong (H^1(G_L, \mu_{p^n})_{\theta^{-1}})^H = H^1(G_L, \mu_{p^n})^{(\theta)} \cong (L^*/L^{*p^n})^{(\theta)}, \end{aligned} \tag{2.5}$$

where the first isomorphism was just noted, the second is by Lemma 2.2, the third by Lemma 2.1 (since $\theta|_{G_L}$ is trivial). For (ii), likewise, we have $H^2(G_F, \widetilde{\mu_{p^n}}) \hookrightarrow H^2(G_L, \widetilde{\mu_{p^n}})^H \cong H^2(G_L, \mu_{p^n})^{(\theta)}$.

(iii) We have noted already that $H^i(G_F, \widetilde{\mu_{p^n}}) \cong H^i(\Gamma_F, \widetilde{\mu_{p^n}})$ as $\mathcal{G}$-modules. Since $\theta|_{G_L} = 1$, we have $\widetilde{\mu_{p^n}} \cong \mu_{p^n}$ as Γ_F-modules, so $H^i(\Gamma_F, \widetilde{\mu_{p^n}}) \cong H^i(\Gamma_F, \mu_{p^n})$ as abelian groups. It remains to check the $\mathcal{G}$-actions. For this, note that as $\mathcal{H} = \mathcal{G}(J/F(p))$ acts trivially on Γ_F and trivially on $\widetilde{\mu_{p^n}}$, it must act trivially on $H^i(\Gamma_F, \widetilde{\mu_{p^n}})$. Since Γ_F also acts trivially on $H^i(\Gamma_F, \widetilde{\mu_{p^n}})$, $\mathcal{G}(J/F)(\cong \Gamma_F \times \mathcal{H})$ acts trivially on $H^i(\Gamma_F, \widetilde{\mu_{p^n}})$. Because the $\mathcal{G}$-action on $H^i(\Gamma_F, \widetilde{\mu_{p^n}})$ is via $\mathcal{G}(J/F)$, this $\mathcal{G}$-action is also trivial; so $\mathcal{G}$ acts trivially also on $H^i(G_F, \widetilde{\mu_{p^n}})$. On the other hand, the fact that $\mathcal{G}$ acts trivially on $H^i(\Gamma_F, \widetilde{\mu_{p^n}}) \cong H^i(\Gamma_F, \mu_{p^n})_{\theta^{-1}}$ translates to $\mathcal{G}$ acts via θ on $H^i(\Gamma_F, \mu_{p^n})$. □

Remark 2.4 Since $\widetilde{\mu_{p^n}}^{\otimes j} = (\mu_{p^n}{}^{\otimes j})_{\theta^{-j}}$, the analogue to Th. 2.3 holds for every $j \in \mathbb{Z}$ (with the same proof), with $\widetilde{\mu_{p^n}}^{\otimes j}$ replacing $\widetilde{\mu_{p^n}}$ and θ^j replacing θ, except for the second isomorphism in 2.3(i).

We can now prove the result needed for [MW$_1$].

Corollary 2.5 *For any $n \in N$, the map $H^1(G_F, \widetilde{\mu_{p^n}}) \to H^1(G_F, \widetilde{\mu_p})$ induced by the canonical epimorphism $\widetilde{\mu_{p^n}} \to \widetilde{\mu_p}$ is surjective.*

Proof. Let $\alpha' \colon \mathcal{G} \to (\mathbb{Z}/p\mathbb{Z})^*$ be the cyclotomic character given by $\sigma(\omega) = \omega^{\alpha'(\sigma)}$ for all $\sigma \in \mathcal{G}$ and $\omega \in \mu_p$, i.e., α' is the $n = 1$ version of α; let $\theta' = \alpha'$. Note that α' is the composition of $\alpha \colon \mathcal{G} \to (\mathbb{Z}/p^n\mathbb{Z})^*$ with the canonical epimorphism $(\mathbb{Z}/p^n\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$; also θ' is obtainable likewise from θ. Therefore, for any p-torsion $\mathcal{G}$-module A, twisting the $\mathcal{G}$-action on A by θ' is the same as twisting by θ. This applies to $A = \mu_p$ and to $A = L^*/L^{*p}$; in particular, the two possible interpretations of $\widetilde{\mu_p}$ coincide.

Now, consider the diagram

$$\begin{array}{ccc} H^1(G_F, \widetilde{\mu_{p^n}}) & \xrightarrow{\cong} & (L^*/L^{*p^n})^{(\theta)} \\ \downarrow & & \downarrow \\ H^1(G_F, \widetilde{\mu_p}) & \xrightarrow{\cong} & (L^*/L^{*p})^{(\theta')} \end{array} \tag{2.6}$$

The horizontal maps here are the isomorphisms of Th. 2.3(i) for n and for 1. By checking the maps that led to the isomorphisms (see(2.5)), we can see that diagram (2.6) is commutative. Note also that as $\theta|_{G_L} = 1$, θ may be viewed as a character on H. Hence $(L^*/L^{*p^n})^{(\theta)}$ is one of the H-eigenmodules in the direct decomposition of L^*/L^{*p^n} as in (1.5) above, and $(L^*/L^{*p})^{(\theta')}$ is the corresponding H-eigenmodule of L^*/L^{*p}. Since the epimorphism $L^*/L^{*p^n} \to L^*/L^{*p}$ is an H-module map, the right vertical map in (2.6) is onto. Hence the left map in (2.6) is also onto, as desired. □

Remark 2.6 The surjectivity proved in Cor. 2.5 definitely depends on the choice of the group action on the cyclic group of order p^n. Note, by contrast, that for the case of trivial G_F-action the

canonical map

$$H^1(G_F, \mathbb{Z}/p^n\mathbb{Z}) \longrightarrow H^1(G_F, \mathbb{Z}/p\mathbb{Z}) \tag{2.7}$$

is not in general onto. For, surjectivity of the map in (2.7) is equivalent to: every cyclic Galois extension of F of degree p embeds in a cyclic Galois extension of degree p^n. This is not always true, as the following example illustrates: Let S be the rational function field $S = \mathbb{Q}(x_1, \ldots, x_p)$ and let σ be the $\mathbb{Q}$-automorphism of S given by cyclically permuting the indeterminates. Let F be the fixed field of σ; so S is Galois over F of degree p. Let $L = F(\omega)$ where $\omega \in \mu_p^*$, and let $T = S(\omega) = \mathbb{Q}(\omega)(x_1, \ldots, x_p)$, which is a cyclic Galois extension of L of degree p. If T lies in a cyclic Galois extension K of L of degree p^2, then a theorem of Albert [A_2, p. 207, Th. 11] says that there is $\alpha \in T$ such that $N_{T/L}(\alpha) = \omega$. However, using the unique factorization in $\mathbb{Q}(\omega)[x_1, \ldots, , x_n]$, one sees that then there is a constant $\beta \in \mathbb{Q}(\omega)$ such that $N_{T/L}(\beta) = \omega$. But $N_{T/L}(\beta) = \beta^p$ as $\beta \in L$, and ω is clearly not a p-th power in T. So, there can be no such field K, and hence there is no cyclic extension of F of degree p^2 containing S.

The subgroups of $H^1(G_F, \widetilde{\mu_{p^n}})$ classify certain field extensions. To describe this, let $M = F(\mu_{p^n})$, and let $E = M \cap F(p)$, which is a cyclic Galois field extension of F with $E(\mu_p) = M$. Slightly abusing notation, let $\alpha\theta^{-1}$ denote also the character for $\mathcal{G}(E/F)$ and for $\mathcal{G}(M/F)$ induced by $\alpha\theta^{-1}$ on $\mathcal{G}$;likewise, let α denote also the character for $\mathcal{G}(M/F)$ induced by α on $\mathcal{G}$.

Theorem 2.7 *The subgroups of $H^1(G_F, \widetilde{\mu_{p^n}})$ are in one-to-one correspondence with the abelian p^n field extensions S of E such that S is Galois over F and $\mathcal{G}(E/F)$ acts on $\mathcal{G}(S/E)$ via $\alpha\theta^{-1}$. They are also in one-to-one correspondence with the abelian p^n field extensions T of M with T Galois over F, $T \subseteq J$, and $\mathcal{G}(M/L)$ acts on $\mathcal{G}(T/M)$ via α.*

Proof. We have

$$\begin{aligned} H^1(G_F, \widetilde{\mu_{p^n}}) &\cong H^1(G_L, \mu_{p^n})^{(\theta)} \cong H^1(G_M, \mu_{p^n})^{(\theta)} \cong H^1(G_M, (\mathbb{Z}/p^n\mathbb{Z})_\alpha)^{(\theta)} \\ &\cong (H^1(G_M, (\mathbb{Z}/p^n\mathbb{Z})_\alpha)^{(\theta)} = H^1(G_M, \mathbb{Z}/p^n\mathbb{Z})^{(\theta\alpha^{-1})} = X(\check{M}/M)^{(\theta\alpha^{-1})}, \end{aligned}$$

where the first isomorphism is by Th. 2.3(i), the second is the restriction of the $\mathcal{G}$-isomorphism $H^1(G_L, \mu_{p^n}) \cong H^1(G_K, \mu_{p^n})^{\mathcal{G}(M/L)}$ (see (1.18)), the third is from the $\mathcal{G}$-isomorphism $\mu_{p^n} \cong (\mathbb{Z}/p^n\mathbb{Z})_\alpha$, the fourth by the $\mathcal{G}$-isomorphism in Lemma 2.1. By Lemma 1.15, the subgroups of $X(\check{M}/M)^{(\theta\alpha^{-1})}$ are in one-to-one correspondence with the fields T such that $M \subseteq T \subseteq \check{M}$ (i.e., T is an abelian p^n-extension of M), T is Galois over F, and $\mathcal{G}$ (hence also $\mathcal{G}(M/F)$) acts on $\mathcal{G}(T/M)$ via $\alpha\theta^{-1}$. When this occurs, $\mathcal{G}(M/E)$, which lies in $ker(\alpha\theta^{-1})$, acts trivially on $\mathcal{G}(T/M)$, so by Prop. 1.4 (with E replacing F), $T \subseteq J$. Also, since $G_L \subseteq ker(\theta)$, the character $\alpha\theta^{-1}$ agrees with α on $\mathcal{G}(M/L)$. So, the conditions on T are the ones stated in the theorem. Conversely, if T satisfies these conditions, then since $\mathcal{G}(M/L)$ acts on $\mathcal{G}(T/M)$ via α (which agrees with $\alpha\theta^{-1}$ on $\mathcal{G}(M/L)$) and $\mathcal{G}(T/E)$ acts via $\alpha\theta^{-1}$ (i.e., trivially) on $\mathcal{G}(T/M)$, we have $\mathcal{G}(M/F)$ acts on $\mathcal{G}(T/M)$ via $\alpha\theta^{-1}$, so T is involved in the one-to-one correspondence. These fields T, since $T \subseteq J$, correspond by Prop. 1.4 to fields $S \subseteq F(p)$ (where $S = T \cap F(p)$ and $T = S(\mu_p)$) such that S is Galois over F, $\mathcal{G}(S/E) \cong \mathcal{G}(T/M)$, and $\mathcal{G}(E/F)$ acts on $\mathcal{G}(S/E)$ the same way as $\mathcal{G}(M/L)$ acts on $\mathcal{G}(T/M)$, i.e., via $\alpha\theta^{-1}$. □

Remark 2.8 An alternate way of obtaining the first one-to-one correspondence of Th. 2.7 is to observe that

$$H^1(G_F, \widetilde{\mu_{p^n}}) \cong H^1(G_E, \widetilde{\mu_{p^n}})^{\mathcal{G}(E/F)} \cong (H^1(G_E, \mathbb{Z}/p^n\mathbb{Z})_{\alpha\theta^{-1}})^{\mathcal{G}(E/F)}$$
$$= H^1(G_E, \mathbb{Z}/p^n\mathbb{Z})^{(\theta\alpha^{-1})} = X(\check{E}/E)^{(\theta\alpha^{-1})}\,,$$

where the first isomorphism follows as in the proof of Cor. 1.11(i), since $H^i(\mathcal{G}(E/F), \widetilde{\mu_{p^n}}) \cong H^i(\mathcal{G}(M/L), \widetilde{\mu_{p^n}}) \cong H^i(\mathcal{G}(M/L), \mu_{p^n}) = 0$ for $i = 1, 2$, by Lemma 1.9. The subgroups of $X(\check{E}/E)^{(\theta\alpha^{-1})}$ correspond to the specified abelian p^n-extensions of E by Lemma 1.15.

3 Cyclic algebras of degree p

One of the oldest unsettled questions in the theory of central simple algebras is whether every division algebra of prime degree p must be a cyclic algebra. This is known to be true for $p = 2$ and 3, but unsettled for every $p \geq 5$. We now describe a possible approach to finding a counterexample which arises from the analysis of the relations between structures over F and those over $L = F(\mu_p)$. We have not succeeded in using this approach to obtain a counterexample, but feel that it is of sufficient interest to be worth describing. A byproduct of this work is a slight generalization of Albert's characterization of cyclic algebras of prime degree. See Theorem 3.6 below.

We will be working here with cyclic algebras and symbol algebras. Our notation for these is as follows: If T is a cyclic Galois field extension of a field K of degree m with $\mathcal{G}(T/K) = \langle\tau\rangle$ and $a \in K^*$, we write $(T/K, \tau, a)$ for the m^2-dimensional cyclic K-algebra $\bigoplus_{i=0}^{m-1} Tx^i$, where $x^m = a$ and $xcx^{-1} = \tau(c)$ for $c \in T$. If $\mu_m \subseteq K$ (so $char(K) \nmid m$) and $\zeta \in \mu_m^*$ and $a, b \in K^*$ we write $(a, b; K)_\zeta$ for the m^2-dimensional symbol algebra over K with generators i, j and relations $i^m = a$, $j^m = b$, and $ij = \zeta ji$. For any integer k with $gcd(k, m) = 1$, note the isomorphism

$$(a, b; K)_\zeta \;\cong\; (a^k, b; K)_{\zeta^k}\,. \tag{3.1}$$

For, if i, j are standard generators of $(a, b; K)_\zeta$ as above, then i^k, j also generate $(a, b; K)_\zeta$, and they satisfy the relations on generators of $(a^k, b; K)_{\zeta^k}$.

Throughout this section F is a field with $char(F) \neq p$ and $\mu_p \not\subseteq F$, and $L = F(\mu_p)$. Also, $\mathcal{G}$, J, and H are as defined in the Introduction. Let $Br(F)$ denote the Brauer group of equivalence classes of central simple F-algebras, and for a field $K \supseteq F$, let $Br(K/F)$ denote the kernel of the scalar extension map $Br(F) \to Br(K)$; let ${}_{p^n}Br(F)$ (resp. ${}_{p^n}Br(K/F)$) denote the p^n-torsion subgroup of $Br(F)$ (resp. $Br(K/F)$). We have the standard isomorphism $Br(L(p)/F) \cong H^2(\mathcal{G}, L(p)^*)$. The long exact cohomology sequence arising from the short exact sequence of $\mathcal{G}$-modules (1.19) above, together with the cohomological Hilbert 90 [CF, p. 124, Prop. 3], which says that $H^1(\mathcal{G}, L(p)^*) = 0$, yields the familiar fact that ${}_{p^n}Br(L(p)/F) \cong H^2(\mathcal{G}, \mu_{p^n})$. The Merkurjev-Suslin Theorem (see [MS, Th. 11.5] or [Sr, p. 149, Th. 8.5]) says (as $\mu_p \in L(p)$) that ${}_pBr(L(p))$ is generated by symbol algebras of degree p. Since $L(p)$ has no cyclic field extensions of degree p, we must have ${}_pBr(L(p)) = 0$, so

${}_{p^n}Br(L(p)) = 0$; this yields

$$ {}_{p^n}Br(F) \cong H^2(\mathcal{G}, \mu_{p^n}), \qquad \text{and likewise,} \qquad {}_{p^n}Br(L) \cong H^2(G_L, \mu_{p^n}). \tag{3.2} $$

Lemma 3.1 *${}_{p^n}Br(F) \cong ({}_{p^n}Br(L))^H$ where $H = \mathcal{G}(L/F)$. Moreover, this isomorphism preserves the Schur index.*

PROOF. Because G_L is a (in fact, the unique) p-Sylow subgroup of $\mathcal{G}$ and μ_{p^n} is p-primary torsion, the restriction map *res*: $H^2(\mathcal{G}, \mu_{p^n}) \to H^2(G_L, \mu_{p^n})^H$ is an isomorphism. (This can be seen by considering *cor* $\circ$ *res* and *res* $\circ$ *cor*, as noted in the proof of Lemma 2.2.) The isomorphism in the lemma now follows by (3.2), since the second isomorphism in (3.2) is a $\mathcal{G}$-module isomorphism. (See e.g. [D, p. 50] for the action of $\mathcal{G}$ on $Br(L)$.)

The restriction map in cohomology corresponds to the scalar extension map ${}_{p^n}Br(F) \to ({}_{p^n}Br(L))^H$. For a central simple F-algebra A, if $A \cong M_t(D)$, i.e., $t \times t$ matrices over a division ring D, then by definition the Schur index of A is $ind(A) = \sqrt{dim_F(D)}$. If $[A] \in {}_{p^n}Br(F)$, then $ind(A)$ is a power of p, so $dim_F(D)$ is a p-power. Then, $D \otimes_F L$ is a division algebra, since $gcd\big([L:F], dim_F(D)\big) = 1$ (cf. [D, p. 67, Cor. 8]). Thus, $ind(A \otimes_F L) = ind(D \otimes_F L) = ind(D) = ind(A)$, as desired. □

Corollary 3.2 *For $J = F(p)(\mu_p)$, if $({}_pBr(J))^{\mathcal{G}(J/F(p))} \neq 0$, then there exist division algebras of degree p over $F(p)$ which are not cyclic algebras.*

PROOF. By Lemma 3.1, with $F(p)$ replacing F, if $({}_pBr(J))^{\mathcal{G}(J/F(p))} \neq 0$, then ${}_pBr(F(p)) \neq 0$. By a theorem of Merkurjev [M, Th. 2], the group ${}_pBr(F(p))$ is generated by algebras of degree p. No such algebra can be a cyclic algebra, since $F(p)$ has no cyclic field extensions of degree p (see Cor. 1.2 above). □

We will give examples in §4 of fields F such that ${}_pBr(J) \neq 0$, but the far more difficult question of nontriviality of $({}_pBr(J))^{\mathcal{G}(J/F(p))}$ remains unsettled.

Lemma 3.1 suggests a further possibility: There may be a central simple division algebra A over L of degree p with $[A] \in Br(L)^H$, such that A is a cyclic algebra over L, but the inverse image of A in ${}_pBr(F)$ is not a cyclic algebra. This possibility becomes more plausible when we recall that the cyclic field extensions of F of degree p correspond only to a portion of those of L, cf. Prop. 1.4.

We can put this in sharper focus using the H-eigendecomposition of ${}_pBr(L)$ and L^*/L^{*p}, where $H = \mathcal{G}(L/F)$. Let $\chi_1, \ldots, \chi_s$ be the distinct characters $\chi_i \colon H \to (\mathbb{Z}/p\mathbb{Z})^*$, with χ_1 the trivial character; let $\alpha \colon H \to (\mathbb{Z}/p\mathbb{Z})^*$ be the cyclotomic character, as in (1.15) above. Since H acts on the p-torsion abelian group ${}_pBr(L)$, we have ${}_pBr(L) = \bigoplus_{i=1}^{s} {}_pBr(L)^{(\chi_i)}$ as in (1.7) above. Lemma 3.1 shows that ${}_pBr(F) \cong {}_pBr(L)^{(\chi_1)}$. A central simple L-algebra A of degree p which is a cyclic algebra is a symbol algebra, $A \cong (a, b; L)_\omega$, where $\omega \in \mu_p^*$. For $\sigma \in H$, we have $\sigma[(a, b; L)_\omega] = [(\sigma(a), \sigma(b); L)_{\sigma(\omega)}]$. Note the complication introduced because σ acts on ω, as well as on a and b. If $[a]$ and $[b]$ lie in eigencomponents of L^*/L^{*p}, then $[A]$ lies in an eigencomponent of ${}_pBr(L)$, as we now describe. The next lemma appears in [M]. We include a short proof for the convenience of the reader.

Lemma 3.3 *Let χ, ψ be characters: $H \to (\mathbb{Z}/p\mathbb{Z})^*$. If $[a] \in (L^*/L^{*p})^{(\chi)}$ and $[b] \in (L^*/L^{*p})^{(\psi)}$, then $[(a,b;L)_\omega] \in {}_pBr(L)^{(\chi\psi\alpha^{-1})}$.*

Proof. Recall [D, p. 80, Lemma 4] that the symbol algebra $(a,b;L)_\omega$ depends up to isomorphism only on the classes $[a]$ and $[b]$ of a and b in L^*/L^{*p}. With (3.1) above, this yields that for any $\sigma \in H$,

$$\sigma(a,b;L)_\omega \;\cong\; (\sigma(a),\sigma(b);L)_{\sigma(\omega)} \;\cong\; (a^{\chi(\sigma)}, b^{\psi(\sigma)};L)_{\omega^{\alpha(\sigma)}} \;\cong\; (a^{\chi(\sigma)\alpha(\sigma)^{-1}}, b^{\psi(\sigma)};L)_\omega\,.$$

Because the class $[(a,b;L)_\omega]$ in ${}_pBr(L)$ is bimultiplicative in a and b [D, p. 80, Lemma 4], this yields $\sigma[(a,b;L)_\omega] = [(a,b;L)_\omega]^{\chi(\sigma)\psi(\sigma)\alpha(\sigma)^{-1}}$ in ${}_pBr(L)$, as desired. □

Proposition 3.4 *Let $\chi\colon H \to (\mathbb{Z}/p\mathbb{Z})^*$ be a character. Take any $a, b \in L^*$ with $[a] \in (L^*/L^{*p})^{(\chi)}$ and $[b] \in (L^*/L^{*p})^{(\alpha\chi^{-1})}$, and let $A = (a,b;L)_\omega$. Then, there is central simple algebra B of degree p over F with $B \otimes_F L \cong A$. Furthermore, B is a cyclic algebra iff there exist $a', b' \in L^*$ with $[a'] \in (L^*/L^{*p})^{(\alpha)}$ and $[b'] \in (L^*/L^{*p})^H$ such that $A \cong (a', b';L)_\omega$.*

Proof. By Lemma 3.3 and Lemma 3.1, $[A] \in ({}_pBr(L))^{(\alpha^{-1}\chi(\alpha\chi^{-1}))} = ({}_pBr(L))^H = im({}_pBr(F))$. Because the scalar extension map ${}_pBr(F) \to {}_pBr(L)$ is index-preserving (see Lemma 3.1), there is a central simple F-algebra B of degree p with $B \otimes_F L \cong A$. Suppose B is a cyclic algebra, say $B \cong (S/F, \sigma, c)$ where S is a cyclic field extension of F of degree p, $\mathcal{G}(S/F) = \langle\sigma\rangle$, and $c \in F^*$. Let $T = S \cdot L$ which is a cyclic field extension of L of degree p, and let $\sigma' \in \mathcal{G}(T/L)$ be the generator such that $\sigma'|_S = \sigma$. We have $T = L(\sqrt[p]{a'})$ for some $a' \in L^*$, and a' can be chosen so that $\sigma'(\sqrt[p]{a'}) = \omega^{-1}\sqrt[p]{a'}$. By Prop. 1.7, $[a'] \in (L^*/L^{*p})^{(\alpha)}$, while $[c] \in F^*/F^{*p} \cong (L^*/L^{*p})^H$. Thus, we have $A \cong B \otimes_F L \cong (T/L, \sigma', c) \cong (a', c; L)_\omega$, as desired.

Conversely, suppose $A \cong (a', b'; L)_\omega$, as in the Prop. Since $a' \in (L^*/L^{*p})^{(\alpha)}$, we know by Prop. 1.7 that there is a cyclic field extension S of F of degree p, such that $S \cdot L = L(\sqrt[p]{a'})$. Let σ' be the generator of $\mathcal{G}(S \cdot L/L)$ such that $\sigma'(\sqrt[p]{a'}) = \omega^{-1}\sqrt[p]{a'}$, and let $\sigma = \sigma'|_S$. Since $[b'] \in (L^*/L^{*p})^H \cong F^*/F^{*p}$, there is $c \in F^*$ with $[c] = [b']$ in L^*/L^{*p}. Then, $B \otimes_F L \cong A \cong (S/F, \sigma, c) \otimes_F L$, so $B \cong (S/F, \sigma, c)$ since the map $Br(F) \to Br(L)$ is injective by Lemma 3.1. □

Remark 3.5 Prop. 3.4 suggests a way of obtaining a noncyclic algebra of degree p over F, but we must necessarily start with a character $\chi\colon H \to (\mathbb{Z}/p\mathbb{Z})^*$ different from α and the trivial character χ_1. We would need $[a] \in (L^*/L^{*p})^{(\chi)}$ and $[b] \in (L^*/L^{*p})^{\alpha\chi^{-1}}$ such that $A = (a,b;L)_\omega$ is a division algebra, but A is not expressible as $(a', b'; L)_\omega$ for any $[a'] \in (L^*/L^{*p})^{(\alpha)}$ and $[b'] \in (L^*/L^{*p})^H$. If $[L : F] \leq 2$ then there are not enough different characters, and the Prop. is of no help. In this connection, recall Merkurjev's result [M, Th. 1, Lemma 2] that if $[L : F] \leq 3$, then ${}_pBr(F)$ is generated by cyclic algebras of degree p.

The approach in Prop. 3.4 leads to a slight generalization of Albert's characterization of cyclic algebras of prime degree. This theorem has recently been proved independently by U. Vishne, see [V, Th. 11.4].

Theorem 3.6 *Suppose $p \nmid [F(\mu_{p^n}) : F]$. Let D be a division algebra of degree p^n over F. Then, D is a cyclic algebra over F if and only if there is a $\gamma \in D$ with $\gamma^{p^n} \in F^* - F^{*p}$.*

PROOF. Suppose first that D is a cyclic algebra, say $D \cong (C/F, \sigma, b)$. Then, there is $\gamma \in D$ with $\gamma^{p^n} = b$. If $b \in F^{*p}$, say $b = d^p$, then for $\delta = \gamma^{p^{n-1}} d^{-1}$ we have $\delta \in D - F$ and $\delta^p = 1$. So, $1 < [F(\delta) : F] < p$, contradicting $[F(\delta) : F] \,\big|\, dim_F(D)$. Hence, $b \in F^* - F^{*p}$.

Conversely, suppose there is $\gamma \in D$ with $\gamma^{p^n} \in F^* - F^{*p}$, say $\gamma^{p^n} = c$. Let $M = F(\mu_{p^n})$. The assumption that $p \nmid [M : F]$ implies that $M = F(\mu_p)$ (see Lemma 1.9). Let $E = D \otimes_F M$. Since E contains the cyclic Galois field extension $M(\gamma)$ of degree p^n over M, this E must be a cyclic M-algebra; hence, $E \cong (a, c; M)_\omega$ for some $a \in M^*$ and $\omega \in \mu_{p^n}^*$. Let $\chi_1, \ldots, \chi_s$ be the distinct characters mapping $H = \mathcal{G}(M/F) \to (\mathbb{Z}/p^n\mathbb{Z})^*$, with χ_1 the trivial character, and let α be the cyclotomic character (see (1.15)). So we have, as $p \nmid [M : F]$, the eigendecompositions

$$M^*/M^{*p^n} \cong \prod_{i=1}^{s} (M^*/M^{*p^n})^{(\chi_i)} \quad \text{and} \quad {}_{p^n}Br(M) \cong \bigoplus_{i=1}^{s} ({}_{p^n}Br(M))^{(\chi_i)} \tag{3.3}$$

by (1.7) above. Write $[a] = \prod_{i=1}^{s} [a_i]$ in M^*/M^{*p^n}, where $[a_i] \in (M^*/M^{*p^n})^{(\chi_i)}$. Then, in ${}_{p^n}Br(M)$, we have $E \cong (a, c; M)_\omega \sim \bigotimes_{i=1}^{s} (a_i, c; M)_\omega$. Also, $[c] \in (M^*/M^{*p^n})^{(\chi_1)}$ as $c \in F^*$; so each $(a_i, c; M)_\omega \in {}_{p^n}Br(M)^{(\chi_i \alpha^{-1})}$ by the p^n analogue to Lemma 3.3. Thus, each $(a_i, c; M)_\omega$ lies in a different direct summand of ${}_{p^n}Br(M)$ in the eigendecomposition of (3.3). Since $[E] \in {}_{p^n}Br(M)^H = {}_{p^n}Br(M)^{(\chi_1)}$, we must have $E \sim (a_j, c; M)_\omega$ in ${}_{p^n}Br(M)$, where $\chi_j \alpha^{-1} = \chi_1$, i.e., $\chi_j = \alpha$; dimension count shows that $E \cong (a_j, c; M)_\omega$. But, since $[a_j] \in (M^*/M^{*p^n})^{(\alpha)}$, the field extension $M(\sqrt[p^n]{a_j}) = S \cdot M$ for some cyclic field extension S of F of degree p^n, by Prop. 1.7. Then, $E \cong (S/F, \tau, c) \otimes_F M$ for some generator τ of $\mathcal{G}(S/F)$. Since the map ${}_{p^n}Br(F) \to {}_{p^n}Br(M)$ is injective by Lemma 3.1 (as $M = L$), we have $D \cong (S/F, \tau, c)$, as desired. □

Remark 3.7 Albert's result is the $n = 1$ case of Theorem 3.6 (see [A_1, Th. 5] or [A_4, p. 177, Th. 4], for which the condition $p \nmid [F(\mu_p) : F]$ always holds. Our proof of Theorem 3.6 is similar to Albert's, though Albert used different terminology, which somewhat veiled his use of eigendecompositions. The theorem is false without the assumption that $p \nmid [F(\mu_{p^n}) : F]$. Albert gave in [$A_3$] a counterexample with $p^n = 4$, and there are presumably examples with odd p also.

4 Valuations on J

As usual, let $L = F(\mu_p)$, with $L \neq F$ (so $p \neq 2$), let $H = \mathcal{G}(L/F)$, and let $J = F(p)(\mu_p)$. In this section we will look at some of the mod p arithmetic of J in order to investigate ${}_pBr(J)$. This is motivated by the question discussed in §3, whether ${}_pBr(J)^H$ can be nontrivial. We will use valuation theory, which is sometimes a useful tool in verifying that central simple algebras are division algebras.

Remark 4.1 Take any field K with $L \subseteq K \subseteq J$ and $[K : L] = p$. Then, by Albert's theorem (see Prop. 1.7 above), $K = L(\sqrt[p]{c})$, for $c \in L^*$ with $[c] \in (L^*/L^{*p})^{(\alpha)}$, where α: $H \to (\mathbb{Z}/p\mathbb{Z})^*$ is the cyclotomic character, as in (1.15) above (with $n = 1$). By Kummer theory, the map $L^*/L^{*p} \to K^*/K^{*p}$ has kernel $\langle [c] \rangle \subseteq (L^*/L^{*p})^{(\alpha)}$. Consequently, for any other character χ: $H \to (\mathbb{Z}/p\mathbb{Z})^*$, $\chi \neq \alpha$, the map $(L^*/L^{*p})^{(\chi)} \to (K^*/K^{*p})^{(\chi)}$ is injective. It follows by iteration and passage to the direct limit that the map $(L^*/L^{*p})^{(\chi)} \to (J^*/J^{*p})^{(\chi)}$ is injective for each $\chi \neq \alpha$. Thus, $(J^*/J^{*p})^{(\chi)}$ can be nonzero for each $\chi \neq \alpha$, though necessarily $(J^*/J^{*p})^{(\alpha)} = 1$ by Albert's theorem, as $F(p)$ has no Galois extensions of degree p. It is a more difficult question when or whether division algebras of degree p over L remain division algebras after scalar extension to J. We will use valuation theory to make some inroads into this question.

We will use the following notation: Suppose K is a field and W is a valuation ring of K. (This means, in particular, that W has quotient field K). Let M_W denote the maximal ideal of W; let $\overline{W} = W/M_W$, the residue field of W; and let Δ_W denote the value group of W (written additively). For a field $K' \supseteq K$, an extension of W to K' is a valuation ring W' of K' such that $W' \cap K = W$.

Example 4.2 Let k be any field with $char(k) \neq p$ and $\mu_p \not\subseteq k$. Let F be the twice iterated Laurent power series field $F = k((x))((y))$. Then, F has the Henselian valuation ring $V = k[[x]] + yk((x))[[y]]$, with $\overline{V} \cong k$. If v: $F^* \to \Delta_V$ is the associated valuation, then $\Delta_V = \mathbb{Z} \times \mathbb{Z}$, with right-to-left lexicographical ordering, with $v(x) = (1, 0)$ and $v(y) = (0, 1)$. Then, $F(p) = k(p)((x))((y))$ and $J = k(p)(\mu_p)((x))((y))$, while $L(p) = \bigcup_{i=1}^{\infty} k(\mu_p)(p)((x^{1/p^i}))((y^{1/p^i}))$. (The description of $F(p)$ and J follows from Th. 4.5 below, but can be seen more directly using the fact that since $\mu_p \not\subseteq k = \overline{V}$ there is no field extension of F of degree a power of p which is totally ramified with respect to V, cf. [E, pp. 161–162, (20.11)] or, more explicitly, [JW, Cor. 2.4] .) The unique extension of V to J is $Z = k(p)(\mu_p)[[x]] + yk(p)(\mu_p)((x))[[y]]$ with $\Delta_Z = \Delta_V = \mathbb{Z} \times \mathbb{Z}$; let z: $J^* \to \Delta_Z$ be the associated valuation. For any $\omega \in \mu_p^*$, let $D = (x, y; J)_\omega$ (see §3 for the notation). Because the images of $z(x)$ and $z(y)$ in $\Delta_Z/p\Delta_Z$ are $\mathbb{Z}/p\mathbb{Z}$-independent, we know by [JW, Cor. 2.6] that z extends to a valuation on D; so, in particular, D is a division ring. Thus, ${}_pBr(J)$ is nontrivial. Since x and y are H-stable, it is tempting to think that $[D]$ should be H-stable. But, in fact, $[D]$ lies in ${}_pBr(J)^{(\alpha^{-1})}$ but not in ${}_pBr(J)^H$ because of the nontrivial action of H on μ_p.

We will consider valuation rings on J as extensions of ones on V. For this, let us now fix a valuation ring V of F with $char(\overline{V}) \neq p$. Let $W_1, \ldots, W_\ell$ be the extensions of V to L. Let $T = W_1 \cap \ldots \cap W_\ell$, which is the integral closure of V in L. This notation will be fixed for the rest of this section. Recall [E, pp. 95–96, Th. (13.4)] that the maximal ideals of T are $N_1, \ldots N_\ell$, where $N_i = M_{W_i} \cap T$, and that each W_i is the localization T_{N_i}.

Proposition 4.3 *Let V be a valuation ring of F with $char(\overline{V}) \neq p$. Let $W_1, W_2, \ldots, W_\ell$ be the valuation rings of L extending V. Then, each $\overline{W_i} \cong \overline{V}(\mu_p)$ and $\Delta_{W_i} = \Delta_V$. Also, $\ell\,[\overline{V}(\mu_p) : \overline{V}] = [L : F]$.*

PROOF. Let $\omega \in \mu_p^* \subseteq L$, and let $f \in F[x]$ be the monic minimal polynomial of ω over F. Then, $f \in V[x]$ as ω is integral over V, which is integrally closed; also, $f \mid \sum_{i=0}^{p-1} x^i$ in $F[x]$, and hence in $V[x]$ by the Division Algorithm, as f is monic. So, the image $\overline{f}$ of f in $\overline{V}[x]$ divides $\sum_{i=0}^{p-1} x^i$ in $\overline{V}[x]$. This shows that the roots of $\overline{f}$ are all primitive p-th roots of unity, and $\overline{f}$ has no repeated roots. So, if $\overline{f} = \prod_{i=1}^{k} g_i$ is the irreducible monic factorization of $\overline{f}$ in $\overline{V}[x]$ then the g_i are distinct and $deg(g_i) = [\overline{V}(\mu_p) : \overline{V}]$. Since $fF[x] \cap V[x] = fV[x]$ by the Division Algorithm, we have $V[\omega] \cong V[x]/fV[x]$, so

$$V[\omega]/M_V V[\omega] \;\cong\; V[x]/(M_V, f) \;\cong\; \overline{V}[x]/(\overline{f}) \;\cong\; \bigoplus_{i=1}^{k} \overline{V}[x]/(g_i)\,,$$

a direct sum of fields. The inverse images in $V[\omega]$ of the k maximal ideals of $V[\omega]/M_V V[\omega]$ are maximal ideals $P_1, \ldots, P_k$ of $V[\omega]$ such that each $P_i \cap V = M_V$ and $V[\omega]/P_i \cong \overline{V}[x]/(g_i) \cong \overline{V}(\mu_p)$. Because T is integral over $V[\omega]$, for each P_i there is a maximal ideal N_i of T with $N_i \cap V[\omega] = P_i$. Then, for $W_i = T_{N_i}$, we have $\overline{W_i} \cong T/N_i \supseteq V[\omega]/P_i \cong \overline{V}(\mu_p)$. By the Fundamental Inequality, [E, p. 128, Cor. (17.8)] or [B, Ch. VI, §8.3, Th. 1], we have

$$\begin{aligned} [L:F] \;&\geq\; \sum_{i=1}^{k} [\overline{W_i} : \overline{V}]\; |\Delta_{W_i} : \Delta_V| \;\geq\; \sum_{i=1}^{k} [\overline{W_i} : \overline{V}] \\ &\geq\; \sum_{i=1}^{k} [\overline{V}(\mu_p) : \overline{V}] \;=\; \sum_{i=1}^{k} deg(g_i) \;=\; deg(f) \;=\; [L:F]\,. \end{aligned} \tag{4.1}$$

Hence, equality must hold throughout (4.1). Therefore, each $\overline{W_i} = \overline{V}(\mu_p)$ and $\Delta_{W_i} = \Delta_V$, and $k = [L:F]/[\overline{V}(\mu_p) : \overline{V}]$. Furthermore, (4.1) and the Fundamental Inequality show that $W_1, \ldots, W_k$ are all the extensions of V to L; so $\ell = k$. □

Remark 4.4 Let S be any Galois extension field of F of degree p, and let U be any extension of V to S. Then, $[\overline{U} : \overline{V}] \mid [S:F] = p$, as S/F is Galois. Consequently, $\overline{U}$ and $\overline{V}(\mu_p)$ are linearly disjoint over $\overline{V}$, and hence $[\overline{U}(\mu_p) : \overline{U}] = [\overline{V}(\mu_p) : \overline{V}]$. It follows by Prop. 4.3 applied to U in S in place of V in F that the number of extensions of U to $S(\mu_p)$ is ℓ. Since any field S' with $F \subseteq S' \subseteq F(p)$ and $[S':F] < \infty$ is obtainable from F by a tower of degree p Galois extensions (see Prop. 1.1) it follows by iteration that every extension of V to S' has exactly ℓ extensions to $S'(\mu_p)$. Because this holds for every finite degree extension S' of F in $F(p)$, it clearly holds for every field S'' with $F \subseteq S'' \subseteq F(p)$.

The main result of this section describes the residue field and value group of any extension of V to J. In case $\mu_p \subseteq \overline{V}$ (i.e., $\ell = [L:F]$, by Prop. 4.3), this will require looking at two pieces of Δ_V. For this, let P be the union of all prime ideals $\mathfrak{P}$ of V such that $V/\mathfrak{P}$ contains no primitive p-th root of unity. Since the prime ideals of V are linearly ordered by inclusion, it is clear that P is a prime ideal of V (possibly $P = (0)$), and P is maximal with the property that $\mu_p \not\subseteq V/P$. (Note also that for every prime ideal $Q \subseteq P$, we have $\mu_p \not\subseteq V/Q$. For, if $\mu_p \subseteq V/Q$, then $\mu_p \subseteq V/P$, as

char$(V/P) \neq p$.) The localization V_P of V at P is a valuation ring of F (a "coarsening" of V); let $\widetilde{V} = V/P$, which is a valuation ring of $\overline{V_P}$. Recall [B, Ch. VI, §4.3, Remark] that there is a canonical short exact sequence of value groups:

$$0 \longrightarrow \Delta_{\widetilde{V}} \longrightarrow \Delta_V \longrightarrow \Delta_{V_P} \longrightarrow 0 \tag{4.2}$$

Theorem 4.5 *Let V be a valuation ring of F with char$(\overline{V}) \neq p$, and let ℓ be the number of extensions of V to L. Let Y be any extension of V to $F(p)$. Then, $\overline{Y} \cong \overline{V}(p)$. If $\mu_p \not\subseteq \overline{V}$, then $\Delta_Y = \Delta_V$. If $\mu_p \subseteq \overline{V}$, let P be the prime ideal of V maximal such that $\mu_p \not\subseteq V/P$, as above, and let Q be the prime ideal of Y with $Q \cap V = P$; let $\widetilde{Y} = Y/Q$. Then, $\Delta_{Y_Q} = \Delta_{V_P}$, while $\Delta_{\widetilde{Y}} = \mathbb{Z}[1/p] \otimes_{\mathbb{Z}} \Delta_{\widetilde{V}}$. Furthermore, Y has exactly ℓ different extensions $Z_1, Z_2, \ldots, Z_\ell$ to J, and each $\overline{Z_i} \cong \overline{Y}(\mu_p)$ and $\Delta_{Z_i} = \Delta_Y$.*

Note that in view of the exact sequence like (4.2) for Δ_Y, the theorem determines Δ_Y completely. It says that when we view Δ_Y as in the divisible hull $\mathbb{Q} \otimes_{\mathbb{Z}} \Delta_V$ of Δ_V, then Δ_Y is the subgroup generated by $\mathbb{Z}[1/p] \otimes_{\mathbb{Z}} \Delta_{\widetilde{V}}$ (the p-divisible hull of $\Delta_{\widetilde{V}}$) and Δ_V.

To prove the theorem we will analyze the range of possibilities for value groups and residue fields of extensions of V to degree p Galois field extensions of F. This will be done in terms of the corresponding extensions of L, where we can invoke Kummer theory. To facilitate the analysis, we need some information on the eigencomponents of induced modules, which is given in the next proposition.

Let $H = \langle\sigma\rangle$ be a cyclic group of finite order s, and let $\overline{H} = \langle\sigma^m\rangle$ for some $m \,|\, s$. Let A be any $\overline{H}$-module, and let B be the induced H-module, $B = Ind_{\overline{H}\to H} A = \mathbb{Z}[H] \otimes_{\mathbb{Z}[\overline{H}]} A$. So, as abelian groups $B = \bigoplus_{i=0}^{m-1} \sigma^i \otimes A$, where each $\sigma^i \otimes A \cong A$. The left action of H on B arises from the multiplication action of H on $\mathbb{Z}[H]$. That is,

$$\begin{aligned} \sigma \cdot \big(id \otimes a_0 + \sigma \otimes a_1 + \ldots + \sigma^{m-1} \otimes a_{m-1}\big) \;=\; \\ id \otimes \sigma^m \cdot a_{m-1} + \sigma \otimes a_0 + \sigma^2 \otimes a_1 + \ldots + \sigma^{m-1} \otimes a_{m-2}\,. \end{aligned} \tag{4.3}$$

Proposition 4.6 *With $H = \langle\sigma\rangle$ and $\overline{H} = \langle\sigma^m\rangle$ as above, let A be an $\overline{H}$-module which is e-torsion for some integer e. Let $B = Ind_{\overline{H}\to H} A$, as above. Let $\chi\colon H \to (\mathbb{Z}/e\mathbb{Z})^*$ be any character. Then the projection map $\pi\colon B \to A$ given by $\sum_{i=0}^{m-1} \sigma^i \otimes a_i \mapsto a_0$ maps $B^{(\chi)}$ bijectively onto $A^{(\chi|_{\overline{H}})}$, where $\chi|_{\overline{H}}$ is the restriction of χ to $\overline{H}$.*

Proof. Let $b = \sum_{i=0}^{m-1} \sigma^i \otimes a_i \in B$. Note that since $\sigma^m \in \overline{H}$, we have $\sigma^m \cdot b = \sum_{i=0}^{m-1} \sigma^i \otimes \sigma^m(a_i)$. Now, $b \in B^{(\chi)}$ iff $\sigma \cdot b = \chi(\sigma)\, b$, iff

$$a_0 = \chi(\sigma)a_1, \quad a_1 = \chi(\sigma)a_2, \quad \ldots, \quad a_{m-2} = \chi(\sigma)a_{m-1}, \quad \text{and} \quad \sigma^m \cdot a_{m-1} = \chi(\sigma)a_0\,. \tag{4.4}$$

If $b \in B^{(\chi)}$, then $\sigma^m(a_0) = \pi(\sigma^m \cdot b) = \pi(\chi(\sigma)^m b) = \chi(\sigma^m)(a_0)$. Hence, $a_0 \in A^{(\chi|_{\overline{H}})}$. Furthermore, if $a_0 = 0$ then (4.4) shows that each $a_i = \chi(\sigma)^{-i} a_0 = 0$; so π maps $B^{(\chi)}$ injectively to $A^{(\chi|_{\overline{H}})}$.

On the other hand, if we take any $a_0 \in A^{(\chi|_{\overline{H}})}$, then $\sigma^m \cdot a_0 = \chi(\sigma^m)a_0 = \chi(\sigma)^m a_0$; so, if we choose $a_1 = \chi(\sigma)^{-1}a_0$, ..., $a_i = \chi(\sigma)^{-i}a_0$, ..., $a_{m-1} = \chi(\sigma)^{-(m-1)}a_0$, then $\sigma^m \cdot a_{m-1} = \sigma^m \cdot (\chi(\sigma)^{-(m-1)}a_0) = \chi(\sigma)^{-(m-1)}\sigma^m \cdot a_0 = \chi(\sigma)a_0$, so the equations in (4.4) are satisfied, showing that $a_0 \in \pi(B^{(\chi)})$. Thus, π: $B^{(\chi)} \to A^{(\chi|_{\overline{H}})}$ is a bijection. □

We can now prove Theorem 4.5.

PROOF *of Theorem 4.5.* It was noted in Remark 4.4 that Y has exactly ℓ extensions to J. The assertions about $\overline{Z_i}$ and Δ_Z follow by applying Prop. 4.3 to Y in $F(p)$ in place of V in F. It remains to analyze $\overline{Y}$ and Δ_Y. For this, we look closely at what can happen with Galois p-extensions of F. These are difficult to get at directly, so we look at the corresponding extensions of L.

Let us now select and fix one of the ℓ extensions of V to L; call it W. Let w: $L^* \to \Delta_W$ be the associated valuation. Now, let $c \in L^* - L^{*p}$ with $[c] \in (L^*/L^{*p})^{(\alpha)}$, and let $K = L(\sqrt[p]{c})$. Let $S = F(p) \cap K$, which we know by Prop. 1.7 is a degree p Galois extension of F. (Moreover, all such Galois extensions of F arise this way.) Let R be a valuation ring of K with $R \cap L = W$; let r: $K^* \to \Delta_R$ be its valuation, and let $U = R \cap S$, which is a valuation ring of S with $U \cap F = V$. The description of R and U breaks down into three possible cases:

Case I. $w(c) \notin p\Delta_W$. Then, since $r(\sqrt[p]{c}) = \frac{1}{p}w(c) \in \Delta_R$, the Fundamental Inequality implies that $\Delta_R = \langle \frac{1}{p}w(c)\rangle + \Delta_W$. By Prop. 4.3 applied to U in S instead of V in F, we have $\Delta_U = \Delta_R = \langle \frac{1}{p}w(c)\rangle + \Delta_V$. So $|\Delta_U : \Delta_V| = p = [S : F]$, and the Fundamental Inequality shows that $\overline{U} = \overline{V}$ and U is the unique extension of V to S.

Case II. $w(c) \in p\Delta_W$. Then, by modifying c by a p-th power in L, we may assume that $w(c) = 0$. Let $\overline{c}$ be the image of c in $\overline{W}$. For this Case II, assume that $\overline{c} \notin \overline{W}^{*p}$. Then $\overline{R}$ contains $\overline{\sqrt[p]{c}} = \sqrt[p]{\overline{c}}$ which is not in $\overline{W}$. So, the Fundamental Inequality implies that $\overline{R} = \overline{W}(\sqrt[p]{\overline{c}})$. Because $p = [\overline{R} : \overline{W}] \mid [\overline{R} : \overline{V}]$ but $p \nmid [\overline{R} : \overline{U}]$ by Prop. 4.3 applied to U in S, we have $p \mid [\overline{U} : \overline{V}]$. The Fundamental Inequality implies that $[\overline{U} : \overline{V}] = p$, $\Delta_U = \Delta_V$, and U is the unique extension of V to S. We noted earlier that $\overline{U}$ is Galois over $\overline{V}$. A comparison of degrees over $\overline{V}$ shows that $\overline{R} = \overline{U} \cdot \overline{W}$ so $\overline{R}$ is abelian Galois over $\overline{V}$. Thus, $\overline{U}$ is the unique cyclic Galois extension of $\overline{V}$ of degree p within $\overline{R}$.

Case III. $w(c) \in p\Delta_W$, so we may assume $w(c) = 0$. For this Case III, assume that $\overline{c} \in \overline{W}^{*p}$. We claim that there are p different valuation rings of K extending W. For, consider the subring $W[\sqrt[p]{c}]$ of K. Since $x^p - c$ is the minimal polynomial of $\sqrt[p]{c}$ over L, we have $W[\sqrt[p]{c}] \cong W[x]/\big(W[x] \cap (x^p - c)L[x]\big) = W[x]/(x^p - c)W[x]$, where the last equality follows by the Division Algorithm for monic polynomials in $W[x]$. Hence, $W[\sqrt[p]{c}]/M_W\, W[\sqrt[p]{c}] \cong W[x]/\big(M_W, x^p - c\ \big) \cong \overline{W}[x]/(x^p - \overline{c})$. Because $\overline{c} \in \overline{W}^{*p}$ and $\mu_p \subseteq \overline{W}$, $x^p - \overline{c}$ factors into distinct linear terms in $\overline{W}[x]$, say $x^p - \overline{c} = (x - d_1)\dots(x - d_p)$. Then, the Chinese Remainder Theorem shows that $\overline{W}[x]/(x^p - \overline{c}) \cong \bigoplus_{i=1}^{p} \overline{W}[x]/(x - d_i)$. Because $W[\sqrt[p]{c}]/M_W W[\sqrt[p]{c}]$ thus has p maximal ideals, $W[\sqrt[p]{c}]$ has at least p maximal ideals. Let C be the integral closure of W in K. Since C is integral over $W[\sqrt[p]{c}]$, C has at least p different maximal ideals, say $N_1, \dots, N_p$. Each localization $R_i = C_{N_i}$ is a different valuation ring of K with $R_i \cap L = W$. The Fundamental Inequality shows that there

must be exactly p of the R_i, as claimed.

Now, since $\mathcal{G}(S/F)$ acts transitively on the valuation rings of S extending V [E, p.105, (14.1)], the number of such extensions is either 1 or p. There are at least p extensions of V to K (namely, the R_i), but every extension of V to S has $\ell \leq p-1$ extensions to K by Prop. 4.3 applied over S. Hence, there must be more than one, so exactly p extensions of V to S, call them $U_1, \ldots, U_p$. The Fundamental Inequality shows that each $\overline{U_i} = \overline{V}$ and $\Delta_{U_i} = \Delta_V$. This completes Case III.

We must still see what constraints are imposed by the condition that $[c] \in (L^*/L^{*p})^{(\alpha)}$. For this, let $H = \mathcal{G}(L/F) = \langle\sigma\rangle$, as usual, and let $\overline{H} = \{\, \tau \in H \mid \tau(W) = W \,\}$, the decomposition group of W over V. Because H acts transitively on the set of extensions of V to L and there ℓ such extensions, $|H : \overline{H}| = \ell$, so $\overline{H} = \langle\sigma^\ell\rangle$. Each $\tau \in \overline{H}$ maps W to itself, so induces an automorphism $\overline{\tau}$ of $\overline{W}$. Recall [E, p. 147, (19.6)] or [ZS, p. 69, Th. 21] that the map $\overline{H} \to \mathcal{G}(\overline{W}/\overline{V})$ given by $\tau \mapsto \overline{\tau}$ is a group epimorphism. By Prop. 4.3 we have $\left|\overline{H}\right| = |H|/\ell = [L:F]/\ell = |\mathcal{G}(\overline{W}/\overline{V})|$, and therefore the map $\overline{H} \to \mathcal{G}(\overline{W}/\overline{V})$ is an isomorphism. Also, because $\overline{\tau}$ acts on the p-th roots of unity in $\overline{W}$ according to the action of τ on the p-th roots of unity in L, the cyclotomic character $\overline{\alpha}$ for $\mathcal{G}(\overline{W}/\overline{V})$ corresponds to the restriction $\alpha|_{\overline{H}}$.

Observe that the distinct extensions of V to L are $\sigma^i(W)$ for $0 \leq i \leq \ell-1$. Each $\Delta_{\sigma^i(W)}$ is canonically identified with Δ_W inside the divisible hull of Δ_V, and for the associated valuation w_i of $\sigma^i(W)$ we have $w_i = w \circ \sigma^{-i}$. Likewise, for $0 \leq i \leq \ell-1$ we identify $\overline{\sigma^i(W)}$ with $\overline{W}$ using the isomorphism $\overline{\sigma^i}\colon \overline{W} \to \overline{\sigma^i(W)}$ induced by $\sigma^i\colon W \to \sigma^i(W)$. So, for $c \in \sigma^i(W)$, we have $\overline{c} \in \overline{\sigma^i(W)}$ corresponds to $\overline{\sigma^{-i}(c)}$ in $\overline{W}$.

We can now determine $\overline{Y}$.

View $\overline{W}^*$ as an $\overline{H}$-module, where $\tau \in \overline{H}$ acts by $\overline{\tau}$. Let $Ind_{\overline{H}\to H}\overline{W}^*$ be the induced H-module described before Prop. 4.6, with $m = \ell$. Recall that T denotes the integral closure of V in L, so $T = \bigcap_{i=0}^{\ell-1} \sigma^i(W)$ [E, p. 95, Th. 3.3.(b)]. Let $\gamma\colon T^* \to Ind_{\overline{H}\to H}\overline{W}^*$ be the map given by $\gamma(t) = \sum_{i=0}^{\ell-1} \sigma^i \otimes \overline{\sigma^{-i}(t)}$ (the bar denotes image in $\overline{W}^*$). The surjectivity of γ is equivalent to the assertion that for every $r_0, \ldots, r_{\ell-1} \in \overline{W}^*$ there is $t \in T^*$ with $\overline{\sigma^{-i}(t)} = r_i$ in $\overline{W}$ for each i, i.e., $\overline{t} = \overline{\sigma^i}(r_i)$ in $\overline{\sigma^i(W)}$. This holds by the Approximation Theorem [E, p. 79, Th. (11.14)] or [ZS, p. 30, Lemma 2]. (For this the valuation rings $\sigma^0(W), \ldots, \sigma^{\ell-1}(W)$ need not be independent, just incomparable. This result uses only the Chinese Remainder Theorem applied to T.) Also, since $\sigma^\ell \cdot \overline{\sigma^{-(\ell-1)}(t)} = \overline{\sigma^\ell(\sigma^{-(\ell-1)}(t))} = \overline{\sigma(t)}$, we have $\sigma \cdot \gamma(t) = \gamma(\sigma(t))$, so γ is an H-module epimorphism. Therefore, the corresponding map $T^*/T^{*p} \to Ind_{\overline{H}\to H}(\overline{W}^*/\overline{W}^{*p})$ is an H-module epimorphism. So, $(T^*/T^{*p})^{(\alpha)}$ maps onto $\left(Ind_{\overline{H}\to H}(\overline{W}^*/\overline{W}^{*p})\right)^{(\alpha)}$, which by Prop. 4.6 projects onto $(\overline{W}^*/\overline{W}^{*p})^{(\overline{\alpha})}$. That is, for any $a \in \overline{W}^* - \overline{W}^{*p}$ such that $[a] \in (\overline{W}^*/\overline{W}^{*p})^{(\overline{\alpha})}$ there is $t \in T^*$ with $[\overline{t}] = [a]$ in $\overline{W}^*/\overline{W}^{*p}$. If we choose $c = t$, then for the resulting $K = L(\sqrt[p]{c})$ we are in Case II above, with $\overline{R} = \overline{W}(\sqrt[p]{\overline{t}}) = \overline{W}(\sqrt[p]{a})$, and $\overline{U}$ is the degree p Galois extension of $\overline{V}$ within $\overline{R}$. Since we can do this for any $[a] \in (\overline{W}^*/\overline{W}^{*p})^{(\overline{\alpha})}$, Prop. 1.7 shows that every Galois extension of $\overline{V}$ of degree p is realizable as some $\overline{U}$, and so lies in $\overline{Y}$.

Now, $F(p)$ is the direct limit of finite towers of Galois extensions of degree p starting with F (see Prop. 1.1). If S' is the top field in such a tower, then $\overline{Y \cap S'}$ is obtained from $\overline{V}$ by a succession of Galois extensions of degree 1 or p. Hence $\overline{Y \cap S'} \subseteq \overline{V}(p)$ for each S', and therefore $\overline{Y} \subseteq \overline{V}(p)$. But, iteration of the argument in the preceding paragraph shows that any finite degree extension of $\overline{V}$ within $\overline{V}(p)$ is obtainable as $\overline{Y \cap S'}$ for a suitably built S'. Hence, $\overline{Y} = \overline{V}(p)$, as desired.

We now determine Δ_Y.

For the trivial $\overline{H}$-module Δ_W, we have the induced H-module $Ind_{\overline{H}\to H}\Delta_W$. Let $\beta\colon L^* \to Ind_{\overline{H}\to H}\Delta_W$ be the map given by $d \mapsto \sum_{i=0}^{\ell-1} \sigma^i \otimes w(\sigma^{-i}(d))$. Since $\sigma^\ell \cdot w(\sigma^{-(\ell-1)}(d)) = w(\sigma(d))$, as $w \circ \sigma^\ell = w$ and σ^ℓ acts trivially on Δ_W, this β is an H-module homomorphism. By reducing mod p we obtain an H-module homomorphism $\overline{\beta}\colon L^*/L^{*p} \to Ind_{\overline{H}\to H}(\Delta_W/p\Delta_W)$. So, for our $c \in L^*$ used to define K, since $[c] \in (L^*/L^{*p})^{(\alpha)}$, we have $\overline{\beta}[c] \in (Ind_{\overline{H}\to H}\Delta_W/p\Delta_W)^{(\alpha)}$, so Prop. 4.6 shows that $w(c) + p\Delta_W \in (\Delta_W/p\Delta_W)^{(\alpha|_{\overline{H}})}$.

Suppose first that $\mu_p \not\subseteq \overline{V}$. Then, $\ell < s = [L : F]$, by Prop. 4.3. so $\overline{H}$, of order s/ℓ, is nontrivial. Since the cyclotomic character α has order s, its restriction $\alpha|_{\overline{H}}$ has order $|\overline{H}|$, so is nontrivial. Since $\overline{H}$ acts trivially on Δ_W, it follows that $(\Delta_W/p\Delta_W)^{(\alpha|_{\overline{H}})} = (0)$. Now, the only way we could have Δ_U larger than Δ_V is if our c is in Case I above. But then we would have $w(c) \notin p\Delta_W$, yielding a nontrivial element in the trivial group $(\Delta_W/p\Delta_W)^{(\alpha|_{\overline{H}})}$. Since this cannot occur, we see that Case I never arises when $\mu_p \not\subseteq \overline{V}$. Therefore, $\Delta_U = \Delta_V$ for every degree p Galois extension S of F. It follows by iteration and passage to the direct limit that $\Delta_Y = \Delta_V$, as asserted.

Now suppose instead that $\mu_p \subseteq \overline{V}$. Prop. 4.3 shows that $\ell = s$, i.e., there are s different extensions $W_1, \ldots, W_s$ of V to L. Consider first the extreme case where $\mu_p \subseteq V/\mathfrak{p}$ for each nonzero prime ideal $\mathfrak{p}$ of V. For any such $\mathfrak{p}$, the extensions of the localizations $V_\mathfrak{p}$ to L are the localizations $W_{1\mathfrak{p}}, \ldots, W_{s\mathfrak{p}}$. (Each $W_{i\mathfrak{p}}$ coincides with the localization of W_i at its prime ideal lying over $\mathfrak{p}$.) Since $\mu_p \subseteq \overline{V_\mathfrak{p}}$, which is the quotient field of $V/\mathfrak{p}$, Prop. 4.3 applied to $V_\mathfrak{p}$ shows that $V_\mathfrak{p}$ has s different extensions to L. (The Prop. applies, as $char(\overline{V_\mathfrak{p}}) \neq p$.) So, $W_{i\mathfrak{p}} \neq W_{j\mathfrak{p}}$ for $i \neq j$. Now, for each i, the rings between W_i and L are the $W_{i\mathfrak{p}}$ as $\mathfrak{p}$ ranges over the nonzero prime ideals of V. Since $W_{i\mathfrak{p}} \neq W_{j\mathfrak{p}}$ for $i \neq j$, it follows that the valuation rings $W_1, \ldots, W_s$ are pairwise independent, i.e., there is no valuation ring of L (smaller than L itself) containing both W_i and W_j for any $i \neq j$. Because of this independence, the Approximation Theorem (see [E, p. 80, (11.16)]) applies, and shows that our map $\beta\colon L^* \to Ind_{\overline{H}\to H}\Delta_W$ is surjective; so $\overline{\beta}\colon L^*/L^{*p} \to Ind_{\overline{H}\to H}(\Delta_W/p\Delta_W)$ is also surjective, so it is also surjective when restricted to the α-eigencomponents. By Prop. 4.6 $(Ind_{\overline{H}\to H}(\Delta_W/p\Delta_W))^{(\alpha)}$ projects onto $(\Delta_W/p\Delta_W)^{(\alpha|_{\overline{H}})}$, which here is all of $\Delta_W/p\Delta_W$ since $|\overline{H}| = 1$ as $\ell = s$. This means that for any $\varepsilon \in \Delta_W - p\Delta_W$ there is $c \in L^*$ such that $[c] \in (L^*/L^{*p})^{(\alpha)}$ and $w(c) \equiv \varepsilon \ (mod\ p\Delta_W)$. If we let $K = L(\sqrt[p]{c})$ for this choice of c, then we are in Case I above, which shows that $\Delta_U = \Delta_R = \langle \frac{1}{p}\varepsilon \rangle + \Delta_W$. Since this is true for any $\varepsilon \in \Delta_W - p\Delta_W$, it follows by iteration and passage to the direct limit that $\Delta_Y = \varinjlim \frac{1}{p^n}\Delta_V = \mathbb{Z}[1/p] \otimes_\mathbb{Z} \Delta_V$. This is what is asserted in the theorem, since in the extreme case we are now considering $P = (0)$, so $\widetilde{V} = V$ and $\widetilde{Y} = Y$.

We handle the general situation by combining the cases previously considered. Suppose $\mu_p \subseteq \overline{V}$. For the prime ideal P defined in the theorem, we have $\mu_p \not\subseteq \overline{V_P}$, which is the quotient field of V/P. Now, Y_Q is an extension of V_P to $F(p)$. Since $\mu_p \not\subseteq \overline{V_P}$ and $char(\overline{V_\mathfrak{p}}) \neq p$, by applying to $V_\mathfrak{p}$ the argument given previously for V we obtain $\Delta_{Y_Q} = \Delta_{V_P}$, as desired. Furthermore, $\overline{Y_Q} \cong \overline{V_P}(p)$. Thus, $\widetilde{Y} = Y/Q$ can be viewed as an extension of $\widetilde{V} = V/P$ from $\overline{V_P}$ to $\overline{V_P}(p)$. By the choice of P, the extreme case considered in the previous paragraph applies to $\widetilde{V}$. Hence, $\Delta_{\widetilde{Y}} = \mathbb{Z}[1/p] \otimes_\mathbb{Z} \Delta_{\widetilde{V}}$. $\square$

Example 4.7 Let $F_0 = \mathbb{Q}(x,y)$, the rational function field in two variables over $\mathbb{Q}$. Let $V_0 = \mathbb{Q}[x]_{(x)} + y\mathbb{Q}(x)[y]_{(y)}$. Here, we are localizing first with respect to the prime ideal (x) of $\mathbb{Q}[x]$, and second with respect to the prime ideal (y) of $\mathbb{Q}(x)[y]$. Then, V_0 is a valuation ring of F_0 with $\overline{V_0} \cong \mathbb{Q}$ and $\Delta_{V_0} = \mathbb{Z} \times \mathbb{Z}$. If $v_0\colon F_0^* \to \Delta_{V_0}$ is the associated valuation, then $v_0(x) = (1,0)$ and $v_0(y) = (0,1)$. Note that V_0 is the intersection with F_0 of the standard Henselian valuation ring on $\mathbb{Q}((x))((y))$ described in Ex. 4.2 above. For any odd prime p, let $F = F_0(\sqrt[p]{1+x})$. To see how V_0 extends to F, let T be the integral closure of V_0 in F, and let $S = V_0[\sqrt[p]{1+x}] \subseteq T$. Since $S \cong V_0[t]/\big(t^p - (1+x)\big)$, we have

$$S/M_{V_0}S \cong \overline{V_0}[t]/\big(t^p - (1+\overline{x})\big) \cong \mathbb{Q}[t]/(t^p-1) \cong \mathbb{Q}[t]/(t-1) \oplus \mathbb{Q}[t]/(t^{p-1}+\ldots+1) \cong \mathbb{Q} \oplus \mathbb{Q}(\mu_p)\,.$$

So, T, being integral over S, has at least two maximal ideals N_1 and N_2, with $\mathbb{Q} \subseteq T/N_1$ and $\mathbb{Q}(\mu_p) \subseteq N_2$. The Fundamental Inequality shows that for the extensions $V_i = T_{N_i}$ of V_0 to F, we have $\overline{V_1} \cong \mathbb{Q}$, $\overline{V_2} \cong \mathbb{Q}(\mu_p)$, and $\Delta_{V_1} = \Delta_{V_2} = \Delta_{V_0} = \mathbb{Z} \times \mathbb{Z}$. Furthermore, V_1 and V_2 are the only extensions of V_0 to F. If Y_i is any extension of V_i to $F(p)$, then Th. 4.5 shows that $\overline{Y_1} \cong \mathbb{Q}(p)$ and $\Delta_{Y_1} = \mathbb{Z} \times \mathbb{Z}$. Let $\mathfrak{p}$ be the prime ideal yV_2. Then, $V_2/\mathfrak{p} \cong \mathbb{Q}(x)(\sqrt[p]{1+x})$, which does not contain μ_p. So, $\mathfrak{p}$ is the prime ideal P of Th. 4.5 for V_2. Since $\Delta_{V_2/\mathfrak{p}} = \mathbb{Z} \times 0$, Th. 4.5 shows that $\Delta_{Y_2} = \mathbb{Z}[1/p] \times \mathbb{Z}$ while $\overline{Y_2} \cong \mathbb{Q}(\mu_p)(p)$.

Remark 4.8 We had hoped to use valuation theory to construct an example of a nonsplit algebra of degree p in ${}_pBr(J)^H$. However, we will now show why Th. 4.5 does not help in this. Let V be a valuation ring of F with $char(\overline{V}) \neq p$, let W be an extension of V to L with associated valuation $w\colon L^* \to \Delta_W$, and let Z be an extension of W to J. There are three types of symbol algebras $A = (a,b;L)_\omega$ (with $a,b \in L^*$ and $\omega \in \mu_p^*$) for which it is known that w extends to a valuation on A, and hence A is a division algebra: (1) $w(a)$ and $w(b)$ map to $\mathbb{Z}/p\mathbb{Z}$-independent elements of $\Delta_W/p\Delta_W$. Then, cf. [JW, Cor. 2.6], the valuation ring of A is tame and totally ramified over W, with residue division algebra $\overline{V}$ and value group $\langle \frac{1}{p}w(a), \frac{1}{p}w(b)\rangle + \Delta_W$. (2) $w(a) \notin p\Delta_W$ and $w(b) = 0$, and for the image $\overline{b}$ of b in $\overline{W}$ we have $\overline{b} \notin \overline{W}^{*p}$. Then, cf. [JW, Cor. 2.9], the valuation ring of A is semiramified over W, with residue division algebra $\overline{W}(\sqrt[p]{\overline{b}})$ and value group $\langle \frac{1}{p}w(a)\rangle + \Delta_W$. (3) $w(a) = w(b) = 0$ and $(\overline{a},\overline{b};\overline{W})_{\overline{\omega}}$ is a division ring. Then, the valuation ring on A is unramified over V, with residue algebra $(\overline{a},\overline{b};\overline{W})_{\overline{\omega}}$ and value group Δ_W. For, if i and j are standard generators of $A = (a,b;L)_\omega$, then it is easy to check that the map $u\colon A - \{0\} \to \Delta_W$ given by $u\big(\sum_{r=0}^{p-1}\sum_{s=0}^{p-1} c_{rs}\, i^r j^s\big) = min\{w(c_{rs}) \,|\, c_{rs} \neq 0\}$ $(c_{rs} \in L)$ is a valuation on A with the specified

residue algebra and value group. (The proof is similar to but easier than the proof of [JW, Th. 2.5].) Since type (3) reduces the problem of obtaining a division algebra to the same problem over the residue field, it is not helpful for constructing examples, and we will not consider this type further.

Suppose we choose $a, b \in L^*$ so that for some character χ: $H \to \mathbb{Z}/p\mathbb{Z}^*$, we have $[a] \in (L^*/L^{*p})^{(\chi)}$ and $[b] \in (L^*/L^{*p})^{(\alpha\chi^{-1})}$. Then, $[A] \in {}_pBr(L)^H$ by Lemma 3.3, so $[A \otimes_L J] \in {}_pBr(J)^H$. but, we will see that the valuation conditions that assure A is a division algebra break down over J. Suppose first that $\mu_p \notin \overline{V}$; so, in the notation of Th. 4.5 and its proof, $\ell < [L : F]$ and $\overline{H}$ is nontrivial. Suppose $w(a) \notin p\Delta_W$; then as in the proof of Th. 4.5, Prop. 4.6 implies that the image of $w(a)$ is nontrivial in $\Delta_W/p\Delta_W{}^{(\chi|_{\overline{H}})}$; this forces $\chi|_{\overline{H}}$ to be trivial, as $\overline{H}$ acts trivially on Δ_W. Hence, $\alpha\chi^{-1}|_{\overline{H}} = \alpha|_{\overline{H}}$, which is nontrivial and is identified with the cyclotomic character $\overline{\alpha}$ for $\mathcal{G}(\overline{W}/\overline{V})$. The nontriviality of $\alpha\chi^{-1}|_{\overline{H}}$ forces $w(b) \in p\Delta_W$, so we may assume $w(b) = 0$. If $b \notin \overline{W}^{*p}$, then A is a division algebra of type (2). But, Prop. 4.6 implies that $\overline{b}$ maps to $(\overline{W}^*/\overline{W}^{*p})^{(\alpha\chi^{-1}|_{\overline{H}})} = (\overline{W}^*/\overline{W}^{*p})^{(\overline{\alpha})}$. Hence, on passing to J we find that $\overline{b} \in (\overline{Z}^*/\overline{Z}^{*p})^{(\overline{\alpha})}$, which is trivial as $\overline{Z} \cong \overline{V}(p)(\mu_p)$—see Remark 4.1. This means that $\overline{b} \in \overline{Z}^{*p}$, and we have lost the conditions for type (2) for $A \otimes_L J$. Likewise, if $w(b) \notin p\Delta_W$, then we are forced to have $w(a) \in p\Delta_W$, and when we adjust a so that $w(a) = 0$, the same argument as just given shows that $\overline{a} \in \overline{Z}^{*p}$. Thus, we have not been able to obtain a type (1) or a type (2) valued division algebra in ${}_pBr(J)^H$ when $\mu_p \notin \overline{V}$.

Suppose instead that $\mu_p \subseteq \overline{V}$. Since $\overline{Z} = \overline{V}(p)(\mu_p) = \overline{V}(p)$ and $\mu_p \subseteq \overline{V}$, $\overline{Z}^*/\overline{Z}^{*p}$ is trivial. Therefore, we will not obtain any valued division algebras of degree p of type (2) or type (3) over J. We are left to search for type (1) division algebras. Thus, we may assume that $w(a)$ and $w(b)$ are $\mathbb{Z}/p\mathbb{Z}$-independent in $\Delta_W/p\Delta_W$. Here $\overline{H}$ is trivial, but choose the prime ideal P of V as in Th. 4.5, and let $\mathfrak{P}$ be the prime ideal of W with $\mathfrak{P} \cap V = P$, and $\widetilde{H}$ the (nontrivial) decomposition group of $W_{\mathfrak{P}}$ over V_P; let $w_{\mathfrak{P}}$ be the valuation of $W_{\mathfrak{P}}$. We have an H-module homomorphism $\widetilde{\gamma}$: $L^*/L^{*p} \to ind_{\widetilde{H}\to H}(\Delta_{W_{\mathfrak{P}}}/p\Delta_{W_{\mathfrak{P}}})$ so since $[a] \in (L^*/L^{*p})^{(\chi)}$ we find that $\widetilde{\gamma}[a] \in \big(ind_{\widetilde{H}\to H}(\Delta_{W_{\mathfrak{P}}}/p\Delta_{W_{\mathfrak{P}}})\big)^{(\chi)}$. By Prop. 4.6 it follows that $w_{\mathfrak{P}}(a) \in \big(\Delta_{W_{\mathfrak{P}}}/p\Delta_{W_{\mathfrak{P}}}\big)^{(\chi|_{\widetilde{H}})}$. Since $\widetilde{H}$ acts trivially on $\Delta_{W_{\mathfrak{P}}}$, this implies that $w_{\mathfrak{P}}(a) \in p\Delta_{W_{\mathfrak{P}}}$ or $\chi|_{\widetilde{H}}$ is trivial. If $w_{\mathfrak{P}}(a) \in p\Delta_{W_{\mathfrak{P}}}$, we can modify a by a p-th power in L^* to assume that $w_{\mathfrak{P}}(a) = 0$; but then, for $\widetilde{W} = W/\mathfrak{P}$ the exact sequence like (4.2) for Δ_W shows that $w(a) \in \Delta_{\widetilde{W}}$. But then, Th. 4.5 shows that $w(a) \in p\Delta_Z$, so that $(a, b; J)_\omega$ is not a type (1) valued division algebra over J. On the other hand, if $\chi|_{\widetilde{H}}$ is trivial, then $\alpha\chi^{-1}|_{\widetilde{H}} = \alpha|_{\widetilde{H}}$, which is nontrivial. Hence, the argument just given for a now shows that $w(b) \in p\Delta_Z$, so again we do not obtain a type (1) valued division algebra over J.

References

[A_1] A. A. Albert, On normal Kummer fields over a non-modular field, *Trans. Amer. Math. Soc.*, **36** (1934), 885–892; =[A_5, 427–434].

[A_2] A. A. Albert, *Modern Higher Algebra*, University of Chicago Press, Chicago, 1937.

[A_3] A. A. Albert, Noncyclic algebras with pure maximal subfields, *Bull. Amer. Math. Soc.*, **44** (1938), 576–579; =[A_5, 581–584].

[A_4] A. A. Albert, *Structure of Algebras*, rev. printing, Amer. Math. Soc., Providence, 1961.

[A_5] A. A. Albert, *Collected Papers*, Part 1, eds. R. E. Block, et. al., Amer. Math. Soc., Providence, R. I., 1993.

[B] N. Bourbaki, *Elements of Mathematics, Commutative Algebra*, Addison-Wesley, Reading, Mass., 1972 (English trans. of *Éléments de Mathématique, Algèbre Commutative*).

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

[D] P. K. Draxl, *Skew Fields*, Cambridge Univ. Press, Cambridge, England, 1983.

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

[JW] B. Jacob and A. Wadsworth, A new construction of noncrossed product algebras, *Trans. Amer. Math. Soc.*, **293** (1986), 693–721.

[M] A. S. Merkurjev, Brauer groups of fields, *Comm. Algebra*, **11** (1983), 2611–2624.

[MS] A. S. Merkurjev and A. A. Suslin, K-cohomology of Severi-Brauer varieties and the norm residue homomorphism, *Izv. Akad. Nauk SSSR*, **46** (1982), 1011–1046; English Trans. *Math. USSR Izv.*, **21** (1983), 307–340.

[MW_1] J. Mináč and R. Ware, Demushkin groups of rank $\aleph_0$ as absolute Galois groups, *Manuscripta Mathematica*, **73** (1991), 411–421.

[MW_2] J. Mináč and R. Ware, Pro-2-Demushkin groups of rank $\aleph_0$ as Galois groups of maximal 2-extensions of fields, *Math. Ann.*, **292** (1992), 337–357.

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

[R] J. J. Rotman, *An Introduction to Homological Algebra*, Academic Press, New York, 1979.

[Sa] D. J. Saltman, Generic Galois extensions and problems in field theory, *Advances in Math.*, **43** (1982), 250–283.

[S_1] J.-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979 (English trans. of *Corps Locaux*).

[S_2] J.-P. Serre, *Galois Cohomology*, Springer-Verlag, Berlin, 1997 (English trans. of *Cohomologie Galoisienne*).

[Sr] V. Srinivas, *Algebraic K-Theory*, 2nd ed., Birkhäuser, Boston, 1996.

[V] U. Vishne, Galois cohomology of fields without roots of unity, preprint, 2002; available at: `http://www.mathematik.uni-bielefeld.de/LAG/`

[ZS] O. Zariski and P. Samuel, *Commutative Algebra*, vol. II, Springer-Verlag, New York, 1975.

Department of Mathematics
Middlesex College
University of Western Ontario
London, Ontario N6A 5B7
Canada
e-mail: minac@uwo.ca

Department of Mathematics, 0112
University of California, San Diego
9500 Gilman Drive
La Jolla, CA 92093-0112
USA
e-mail: arwadsworth@ucsd.edu