UNIVERSITY OF CALIFORNIA, SAN DIEGO

Division Algebras Over Generalized Local Fields

A dissertation submitted in partial satisfaction of the requirements for the degree Doctor of Philosophy

in

Mathematics

by

Frank H. Chang

Committee in charge:

Professor Adrian Wadsworth, Chair
Professor Joseph Goguen
Professor Ronald Graham
Professor Lance Small
Professor Audrey Terras

2004

The dissertation of Frank H. Chang is approved, and it is acceptable in quality and form for publication on microfilm:

____

____

____

____

____

Chair

University of California, San Diego

2004

To Catherine and Byron.

Learning without thought is labor lost;
thought without learning is perilous.
- Confucius, Analects (bk. II, ch. XV)

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I give many, many thanks to Professor Adrian Wadsworth for his tireless patience in proofreading, correcting, teaching, and nurturing.

I must also give thanks to all the professors and teachers who helped me get to graduate school (among whom are Professor Jim Agler, Professor Sam Buss, Professor James R. Cheatham, Professor Don Smith, Professor Ruth Williams, Professor Hans Wenzl).

I would also like to thank my former classmates (Aubin, Cameron, Eric, Glick, Graham, JLee, Rino) for sticking together and for sticking around. Finally, I would like to thank Nick Loehr, Jason Bell, and Jeff Ovall for sharing many enjoyable conversations about mathematics and teaching.

The author acknowledges that, without the support of his wife and family, he would never have finished.

VITA

September 5, 1974	Born, Pittsburgh, Pennsylvania
1997	B. A., Mathematics, University of California, San Diego
1997	B. A., Music Composition, University of California, San Diego
1997–2003	Teaching assistant, Department of Mathematics, University of California, San Diego
2001	C. Phil., Mathematics, University of California, San Diego
2004	Ph. D., Mathematics, University of California, San Diego

ABSTRACT OF THE DISSERTATION

Division Algebras Over Generalized Local Fields

by

Frank H. Chang
Doctor of Philosophy in Mathematics

University of California San Diego, 2004

Professor Adrian Wadsworth, Chair

We call F a generalized local field (abbreviated GLF) if F is Henselian and $\overline{F}$, the residue field of F, is finite. In this thesis, we prove several results on finite-dimensional division algebras over GLF's. The aim of the first half of the thesis is to give formulas for understanding the underlying division algebra and subfields of a given algebra. We first show that every division algebra over a GLF is isomorphic to a tensor product of cyclic algebras. Also, we give formulas for computing the degree, value group, residue field, and underlying division algebra of any algebra of the form $N \otimes_F T$, where N is nicely semi-ramified over F and T is tame and totally ramified over F. In addition. we show how to compute the index of $D \otimes_F K$, where K is a finite-degree extension of F.

The second half of this thesis is devoted to the corestriction map, a generalization of the norm map to higher cohomology groups. We focus on corestriction of characters and algebras for any finite-degree extension of fields L/F, with the goal of handling corestriction in the context of GLF's. We prove several projection-type formulas in the case where F contains fewer roots of unity than L. The formulas combine to give a formula for handling corestriction of symbol algebras over radical extensions. The final section applies these results to corestriction of algebras over generalized local fields.

Introduction

Let F be a field and let D be an algebra over F. We let $[D : F]$ denote the dimension of D over F as a vector space and $Z(D)$ denote the center of D. In this work, we will only consider algebras which are finite-dimensional over their center. We say D is a central simple F-algebra if $Z(D) = F$, $[D : F] < \infty$, and D has no non-trivial two-sided ideals. We say D is an F-division algebra if $Z(D) = F$, $[D : F] < \infty$, and every non-zero element of D is invertible. We will let $\mathcal{D}(F)$ stand for the set of all F-division algebras.

In 1843, Hamilton constructed the quaternions, $\mathbb{H}$, which provided the first example of a noncommutative division ring. The question of existence was answered, however, one may ask, what types of division algebras exist over a given field? For example, up to isomorphism, $\mathbb{H}$ is the only (finite-dimensional) non-commutative $\mathbb{R}$-division algebra. By the Wedderburn structure theorem, every central simple F-algebra, A, is isomorphic to some size matrices over some $D \in \mathcal{D}(F)$. This D is unique up to isomorphism and is called the underlying division algebra of A. We say that two algebras are similar if they represent the same class in $Br(F)$ (written $A \sim B$). Similarity gives an equivalence relation on central simple F-algebras. The resulting set of equivalence classes form the Brauer group $Br(F)$ under tensor product (taken over F). For any central simple F-algebra, A, the dimension of A over F is always a perfect square. Thus, we may define the degree, $deg(A) = \sqrt{[A : F]}$, and the Schur index, $ind(A) = deg(D)$, where D is the underlying division algebra of A. (Note that $ind(A) = deg(A)$ if and only if $A \in \mathcal{D}(F)$.)

We now introduce a very important type of central simple algebra. Let $F \subseteq K$ be a finite-dimensional Galois extension of fields, and let G be the Galois group $Gal(K/F)$. Suppose that $f : G \times G \to K^*$ is a 2-*cocycle*, i.e., for all $\sigma, \tau, \rho \in G$, $f(\sigma,\tau)f(\sigma\rho,\tau)^{-1}f(\rho,\sigma\tau) = \tau(f(\rho,\sigma))$. We will write $(K/F, G, f)$ for the *crossed product* algebra defined by the conditions:

1. $(K/F, G, f)$ is a right K-vector space with base $\{u_\sigma \mid \sigma \in G\}$.

2. For all $c \in K, \sigma \in G$, $cu_\sigma = u_\sigma \sigma(c)$.

3. For every $\sigma, \tau \in G$, $u_\sigma \cdot u_\tau = u_{\sigma\tau} f(\sigma, \tau)$.

The crossed product $(K/F, G, f)$ is a central simple F-algebra of degree $|G|$ with maximal subfield K. By Köthe's Theorem (cf. [Rei75, Th. 7.15(ii)]), every $D \in \mathcal{D}(F)$ has a maximal subfield separable over F. Thus, every central simple F-algebra is similar to a crossed product (cf. Section 1.2.1). We define the relative Brauer group, $Br(K/F)$, to be the subgroup of $Br(F)$ consisting of all algebras for which $A \otimes_F K \sim K$. If K is a maximal subfield of A, then $[A] \in Br(K/F)$. The correspondence defined by $[A] \leftrightarrow [f]$ is an isomorphism between $Br(K/F)$ and $H^2(G, K^*)$. Also, $Br(F_{sep}/F) = Br(F)$, whence $Br(F) \cong H^2(G_F, F^*_{sep})$, where $G_F = Gal(F_{sep}/F)$.

If K is cyclic Galois over F, then the structure of $(K/F, G, f)$ simplifies. Let σ be a generator for $Gal(K/F)$. Then, there exists an $b \in F^*$ such that the 2-cocycle f' defined by

$$f'(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } 0 \le i, j, i+j < n; \\ b & \text{if } 0 \le i, j, < n \le i+j \end{cases}$$

differs from f by a 2-coboundary. Define x by $cx = x\sigma(c)$ for all $c \in K$ and $x^n = b$. Then, $\{1, x, \ldots, x^{n-1}\}$ is a K-base of A. In this case, $A = (K/F, G, f)$ is a called a *cyclic* algebra and we will adopt the usual convention of writing $A = (K/F, \sigma, b)_n$.

Let us write μ_n for the group of n-th roots of unity and μ_n^* for the set of generators of μ_n. Assume that $\mu_n \in F^*$ (so $char(F) \nmid n$) and take $\omega \in \mu_n^*(F)$. Fix $a \in F^*$ such that aF^{*n} has order n in F^*/F^{*n}. Let $K = F(\sqrt[n]{a})$ and suppose $\sigma \in Gal(K/F)$

satisfies $\sigma(\sqrt[n]{a}) = \omega\sqrt[n]{a}$. Then for any $b \in F^*$, the cyclic algebra $A = (K/F, \sigma, b)_n$ has generators i, j over F such that $i^n = a, j^n = b$, and $ij = \omega ji$, i.e. $\{i^k j^l : 0 \leq k < n,\ 0 \leq l < n\}$ is an F-base for A.

In general, if $a, b \in F^*$ and $\mu_n \subseteq F$, then the F-algebra, A, generated over F by i, j satisfying relations $i^n = a, j^n = b$, and $ij = \omega ji$ is a central simple F-algebra (cf. [Mil71, Theorem 15.1] or [Dra83, p. 78, Th. 1]). We call A a symbol algebra and will denote A by any of the following expressions

$$A_\omega(a, b; F)_n, \quad (a, b; F, \omega)_n, \quad (a, b; F)_n, \quad (a, b; \omega)_n, \quad (a, b)_n.$$

Note $deg(A) = n$, and A is a cyclic algebra if $[F(\sqrt[n]{a}) : F] = n$. In particular, this holds if A is a division algebra.

In the early 1930's, Brauer, Hasse, and Noether showed that if F is a number field, then every F-division algebra is a cyclic algebra (cf. [BHN32]). However, in 1932, Albert gave an example of a non-cyclic division algebra. Naturally, one would ask if there were any non-crossed product division algebras. This remained a major open question for several decades. Thus, it was a major breakthrough, when, in 1972, Amitsur gave the first example of a non-crossed product division algebra. (A detailed account of Amitsur's approach can be found in [Row80, Ch. 3], [Jac75], or [Ami72].) We will briefly summarize his approach and show how valuation theory helps in constructing a non-crossed product. Amitsur constructs a universal division ring, $UD(F; n)$, as the ring of quotients of an algebra generated by generic matrices. The key theorem he proves in showing that certain $UD(F; n)$ are not crossed products is the following:

Theorem. *Let G be a finite group of order n. If $UD(F; n)$ is a crossed product with Galois group G, then for any division algebra D of degree n over a field $M \supseteq F$, D is also a crossed product with Galois group isomorphic to G.*

Thus, $UD(F; n)$ is a non-crossed product if we can construct division algebras D_1, D_2 of dimension n^2 over fields $M_1, M_2 \supseteq F$ such that D_1, D_2 are crossed products but for every pair of maximal subfields $N_i \subseteq D_i$, $Gal(N_1/M_2) \ncong Gal(N_2/M_2)$. Such a construction is difficult because there are two questions which are often hard to answer.

1. Given a central simple algebra, can we determine the underlying division algebra, D, of A?

2. Can we classify or determine all the subfields (up to isomorphism) of a given division algebra?

If a valuation is present, these questions are often easier to answer. Also, more recently, there have been other constructions of non-crossed product algebras using valuation theory, cf. [JW86] and [Bru95].

Let F be a field with valuation v. For any field $K \supseteq F$, it is well known that v has at least one, but often many different extensions to valuations on K (cf. [End72, p. 62, Cor. 9.7]). However, the situation is very different for division algebras. It was shown by Ershov, and, independently by Wadsworth, that if $D \in \mathcal{D}(F)$, then v extends to D if and only if v has a unique extension to each subfield $L \subseteq D$ containing F (cf. [Ers82, p. 53-55] and [Wad86]). Thus, unlike the commutative setting, if a valuation v on F extends to $D \in \mathcal{D}(F)$, then the extension is unique.

We say that F is *Henselian* with respect to v if Hensel's Lemma holds for v. We know that F is Henselian with respect to v if and only if v has a unique extension to every field algebraic over F (cf. [Rib85, Th. 3] and [End72, Cor. 16.6]). Thus, if F is Henselian, then v has a unique extension to each $D \in \mathcal{D}(F)$. For $D \in \mathcal{D}(F)$ with valuation v, we define the valuation ring $V_D = \{d \in D^* \mid v(d) \geq 0\} \cup \{0\}$, the unique maximal ideal M_D of V_D, $M_D = \{d \in D^* \mid v(d) > 0\} \cup \{0\}$, the residue division algebra $\overline{D} = V_D/M_D$, and the value group $\Gamma_D = v(D^*)$. (All of the definitions and notation pertaining to valuation theory can be found in Section 1.3.)

Tignol and Wadsworth answered question 2 above for tame and totally ramified (TTR) algebras over Henselian fields in [TW87] (i.e. $D \in \mathcal{D}(F)$ such that $[D : F] = |\Gamma_D : \Gamma_F|$ and $char(\overline{F}) \nmid [D : F]$). In the same paper, they answered question 1, but for tensor products of symbol algebras over strictly Henselian fields; i.e. Henselian fields which have separably closed residue field. In [TW87, Th. 3.8], Tignol and Wadsworth showed that, if D is a tame and totally ramified (TTR) division algebra over F, then there is a 1-1 correspondence between isomorphism classes of F-subalgebras of D and subgroups of Γ_D/Γ_F. In order to obtain this classification, Tignol and Wadsworth introduce the idea of an armature; for a central simple algebra, A, an armature, $\mathcal{A}$ is an abelian subgroup of A^*/F^* such that $F[\mathcal{A}] = A$ and $|\mathcal{A}| = [A : F]$ (cf. Section 1.4.1). Another important tool used in the paper is the following non-degenerate bilinear symplectic pairing when D is TTR

$$C_D : (\Gamma_D/\Gamma_F) \times (\Gamma_D/\Gamma_F) \to \overline{F}^*$$

given by $(v(a)+\Gamma_F, v(b)+\Gamma_F) \mapsto \overline{aba^{-1}b^{-1}}$ (cf. Section 1.4). We call C_D the *canonical pairing* of v on D. If A is a central simple algebra with an armature, $\mathcal{A}$, then the valuation v induces a map $\overline{w} : \mathcal{A} \to (\mathbb{Q} \otimes_{\mathbb{Z}} \Gamma_F)/\Gamma_F$ (cf. Section 1.4). If $\mathcal{A}$ has exponent s, then $\overline{w}$ is given by $\overline{w}(a) = \frac{1}{s}v(a^s) + \Gamma_F$ for $aF^* \in \mathcal{A}$. In the classification of subalgebras of D, a subalgebra A is a subfield if and only if $\overline{w}(A) = \Gamma_A/\Gamma_F$ is a totally isotropic subgroup of Γ_D/Γ_F (with respect to C_D).

This classification of the subfields of a given TTR division algebra allows us to construct quite easily division algebras D_1 and D_2 with the properties described in the paragraph preceding questions 1 and 2. This construction is given in detail in [Wad02, Examples 5.2].

In the case that F is strictly Henselian, i.e. F is Henselian and $\overline{F}$ is separably closed, Tignol and Wadsworth provide an algorithm (cf. [TW87, Th. 4.3]) for explicitly computing the underlying division algebra, D, of a given algebra, A, when A is presented as a tensor product of symbol algebras. The resulting D is always TTR, whence, by Draxl's Theorem (Th. 1.4.5), a tensor product of symbol algebras. More recently, in [Bru01] Eric Brussel gives another algorithm using alternating matrices.

In this thesis, we will study division algebras over generalized local fields (GLF), i.e. fields F such that F is Henselian and $\overline{F}$ is finite. These fields are the next step up in complexity from strictly Henselian fields in the following ways. First, if F is strictly Henselian, then all division algebras over F are TTR. Although this is not the case when F is a GLF, every $D \in \mathcal{D}(F)$ has the form $D \sim N \otimes_F T$ where N is nicely semi-ramified (abbreviated NSR, cf. Section 1.3) and T is TTR over F. So it is not necessarily the case that D is the tensor product of symbol algebras. However, we will show that D is necessarily a tensor product of cyclic algebras and in the process, show how to compute D from a given $N \otimes_F T$ decomposition. Second, although $Br(\overline{F})$ is trivial because $\overline{F}$ is finite, $\overline{F}$ is no longer separably closed, so F has non-trivial unramified field extensions, i.e. fields K over F such that $[K : F] = [\overline{K} : \overline{F}]$ and $\overline{K}$ is separable over $\overline{F}$. Thus, the subfields of a given division algebra no longer necessarily TTR as in the strictly Henselian case.

As the name suggests, generalized local fields are a generalization of the local fields studied in number theory. It is well-known that non-Archmedian local fields have finite residue and satisfy Hensel's Lemma. The difference is that local fields are discrete (i.e. $\Gamma_F \cong \mathbb{Z}$), whereas GLF's are allowed to have as value group any totally ordered abelian group. For example, for any finite field, K, the Laurent series field $K((x)) = \left\{ \sum_{i=k}^{\infty} a_i x^i |\ k \in \mathbb{Z}, a_i \in k \right\}$ is a GLF with respect to the valuation $v\left(\sum_{i=k}^{\infty} a_i x^i \right) = \min\{i|\ a_i \neq 0\}$. More generally, we form the n-fold iterated Laurent series, $F = K((x_1))((x_2)) \ldots ((x_n))$ (cf. Section 2.1). Then F has is a generalized local field with $\Gamma_F = \mathbb{Z}^n$, $\overline{F} = K$. The added flexibility in value group allows for greater complexity in the division algebras over F. For example, it is not necessarily true that every division algebra over a GLF is cyclic as was the case over a local field.

We will first generalize the results from [TW87] and provide an answer to both questions above for F, a GLF, and for $D \in \mathcal{D}(F)$ presented as a tensor product $N \otimes_F T$. In Chapter 2, we prove a few basic results concerning question 1 above for division algebras over F a GLF. We show in Proposition 2.1.4 that the decomposition

$D \sim N \otimes_F T$ gives us a nice formula for computing $deg(D)$, Γ_D and $\overline{D}$, namely

$$deg(D) = \frac{deg(N) \cdot deg(T)}{|(\Gamma_N \cap \Gamma_T) : F|},$$
$$\Gamma_D = \Gamma_N + \Gamma_T,$$
$$[\overline{D} : \overline{F}] = \frac{deg(N)}{|(\Gamma_N \cap \Gamma_T) : F|}.$$

Note that, since $\overline{F}$ is finite, $\overline{D}$ is a field and is determined by its degree over $\overline{F}$. We show in Theorem 2.2.1 that the algorithm in [TW87, Th. 4.3] holds more generally, as follows.

Theorem. *Suppose (F, v) is a valued field, and A is a central simple F-algebra with armature $\mathcal{A}$. Assume that $\text{char}(\overline{F}) \nmid [A : F]$. Let $s = \exp(\mathcal{A})$, so F contains a primitive s-th root of unity. Suppose that for any $a \in A^*$ with $aF^* \in \mathcal{K} = \ker(\overline{v_A})$ we have $a^s \in F^{*s}$. If D is the underlying division algebra of A, then $[D : F] = |\mathcal{K}^\perp : (\mathcal{K} \cap \mathcal{K}^\perp)|$, $\Gamma_D/\Gamma_F = \overline{v_A}(\mathcal{K}^\perp) \subseteq \Delta/\Gamma_F$, and the canonical pairing on Γ_D/Γ_F is isometric (via $\overline{v_A}$) to the pairing on $\mathcal{K}^\perp/(\mathcal{K} \cap \mathcal{K}^\perp)$ induced by $B_{\mathcal{A}}$. In particular,*

1. *A is a division algebra if and only if $\overline{v_A}$ is injective.*

2. *If $\mathcal{K}^\perp \subseteq \mathcal{K}$, then A is split.*

This helps us prove (cf. Theorem 2.4.1)

Theorem. *Every division algebra over a GLF is isomorphic to a tensor product of cyclic algebras.*

Eric Brussel at Emory University has proven this result using a different method, although we have just recently received his proof. In proving this result, we also obtain a way of computing the underlying division algebra, D, the value group, Γ_D, and the residue, $\overline{D}$ of a given tensor product $N \otimes_F T$ with N NSR and T TTR. We show also that, although $D \sim N \otimes_F T$ for some N,T which are NSR and TTR over F, this D need not be isomorphic to the tensor product of an NSR algebra with a

TTR algebra. However, D always can be written as $D \cong C \otimes_F T$, where C is a cyclic algebra and T is TTR. This answers question 1 above for F a GLF and any A written as $N \otimes_F T$.

In Chapter 3, we address question 2 concerning subfields of algebras. Suppose that $K \supseteq F$ is a finite degree extension of GLF's. We would like to get information about D_K, the underlying division algebra of $D \otimes_F K$, i.e. what happens to D under the restriction map $res_{F/K} : Br(F) \to Br(K)$. Note that K is isomorphic to a subfield of D if and only if $ind(D_K) = ind(D)/[K : F]$ (cf. Prop. 1.2.2), so computing D_K gives us information about the subfield structure of D. By primary decomposition (cf. Prop. 1.2.1), it is enough to consider the case where D is p-primary; i.e. $deg(D)$ is a power of a prime p. For unramified field extensions of F, we have the following result (cf. Prop. 3.3.1).

Proposition. *Suppose K is the unramified field extension of F with $[K : F] = p^k$. Say $D \sim N \otimes_F T$ with N NSR and T TTR over F. Let $\deg(N) = p^n$ and let $|(\Gamma_N \cap \Gamma_T) : \Gamma_F| = p^m$. Then $deg(D) = p^{\ell_0} \cdot deg(D_K)$, where $\ell_0 = \min\{n - m,\ k\}$. Also, $\Gamma_{D_K} = [K : F]\Gamma_N + \Gamma_T$ and $[\overline{D_K} : \overline{K}] = p^{n-m-\ell_0}$.*

The result shows that the amount of reduction in the index of D depends on the size of the field extension $[I : F]$ as well as degree of N and the overlap in value group, $\Gamma_N \cap \Gamma_T$. The totally ramified field extension case is much more complicated. Since F is Henselian, if K is tame and totally ramified over F, then K is totally ramified of radical type (TRRT) [Sch50, p. 64, Theorem 3]. Thus, K can obtained from F by a series of cyclic totally ramified radical extensions. Even in the cyclic case, the result is quite complex. Suppose $D \sim N \otimes_F T$ is p-primary. Then, we have (cf. Theorem 3.3.3)

Theorem. *Suppose K is a cyclic TTR field extension of F with $\Gamma_K \subseteq \Gamma_D$. Let $p^k = [K : F]$, $p^n = deg(N)$, $p^m = |(\Gamma_N \cap \Gamma_T) : \Gamma_F|$. Let σ, σ_ω, γ, θ, and ρ be as defined preceding Theorem 3.3.3 and let $\langle -, - \rangle$ denote the armature pairing on $\mathcal{T}$.*

Then,

$$ind\ D_K = \frac{\ell}{p^k} \cdot ind\ D,$$

where

$$\ell = ord_{\mathbb{Q}/\mathbb{Z}}\Big(\langle\widetilde{\theta}, \widetilde{\rho}\rangle + \lambda p^{n-m+\gamma-k}\Big), \tag{0.1}$$

and $\lambda \in \overline{comp}(\sigma_\omega, \sigma)$ *is prime to* p.

The constants in the formula show that the index of D_K depends on $p^n = deg(N), p^m = |(\Gamma_N \cap \Gamma_T) : \Gamma_F|, p^k = [K : F]$, as well as γ (which measures the relative size of $K \cap T$ to $|(\Gamma_K/\Gamma_F) \cap (\Gamma_T/\Gamma_F)|$), λ (a compatibility factor), and $\widetilde{\theta}, \widetilde{\rho}$ (which depends on how Γ_K lies in $\Gamma_D = \Gamma_N + \Gamma_T$). With these formulas, we are able, in principle to answer question 2 by computing D_K for various extensions K of F. In particular, K is isomorphic to a subfield of D if and only if $\ell = 1$. Note also that ℓ is the order of a sum of terms, so ℓ could be smaller than the order of $\langle\widetilde{\theta}, \widetilde{\rho}\rangle$ or $\lambda p^{n-m+\gamma-k}$; i.e. it is possible for K to be a subfield of D for a non-obvious reason.

Finally, in Chapter 4, we provide some methods for how to compute corestriction. Let L/F be a finite degree separable field extension. The corestriction map is dual to the restriction map in that $cor_{L/F} : Br(L) \to Br(F)$ and the composition $cor_{L/F} \circ res_{L/F}$ is multiplication by $[L : F]$. Also, the corestriction map is a generalization of the norm map to higher cohomological dimension (cf. 1.6.1). In general, the corestriction map is very difficult to compute. Rosset and Tate give a complicated recursive formula for corestriction in [RT83]. In a few cases, the formula simplifies; Merkurjev gives a few basic corestriction formulas in [Mer85]. In the case where F is Henselian, Hwang gave extensive calculations concerning corestriction (cf. [Hwa95a], [Hwa95b]).

The majority of the material in the thesis on corestriction is handled outside the context of valuation theory, but is motivated by GLF's. These results rely on either decomposing cyclic and symbol algebras into cup products (cf. Section 1.5) or finding an algebra that restricts to the algebra in question. The corestriction map $cor_{L/F}$ is less difficult if F has enough roots of unity, e.g. if F and L have the same roots of unity. For example, we have the classical projection formula at our disposal for symbol algebras with a slot in F (cf. Theorem 4.2.3). However, if F has fewer roots of unity than L, then the map is more complicated. For example, by using characters and a projection formula for cup products, we prove the following projection-type formula for symbol algebras (cf. Theorem 4.2.4)

Theorem. *Let F be a field with $\mathrm{char}(F) \nmid n$ and let $L = F(\mu_n)$, where μ_n is the set of n-th roots of unity. Then for $a, b \in F^*$ and $\zeta \in \mu_n^*$, we have*

$$\mathrm{cor}_{L/F}\,(a, b; L, \zeta)_n = \left(a, b; F, \eta^{n/d}\right)_d,$$

where d is the order of $\mathrm{N}_{L/F}(\zeta)$ and $\eta \in \mu_n^*$ satisfies $\mathrm{N}_{L/F}(\eta) = \zeta^{n/d}$.

The situation becomes more complicated if the symbol algebra over L has one slot which does not lie in F. The next proposition appears as Prop. 4.2.15.

Proposition. *Let F be a field and p be a prime. If $p = 2$, assume $\mu_4 \subseteq F$. Take $\zeta \in \mu_{p^k}^*$ for some $k \geq 1$ and let $L = F(\zeta)$. Let $\omega \in L$ be p^N root of unity for some $N \in \mathbb{N}$. Let θ be any p^k-th root of ω. Suppose $\mu_{p^k} \cap F = \mu_{p^r}$ and let $p^\ell = [L(\theta) : L]$. Then for any $b \in F^*$,*

$$\mathrm{cor}_{L/F}\,(\omega, b; L, \zeta)_{p^k} = \left(E/F,\ \sigma|_E,\ b\right),$$

where E is determined by $F \subseteq E \subseteq L(\theta)$ and $[E : F] = p^\ell$, and σ is a generator of $Gal(L(\theta)/F)$ which satisfies $\sigma^{[L:F]}(\theta) = \zeta^{p^{k-\ell}}\theta$.

By using group extensions and the cup product, we can handle corestriction over cyclotomic extensions (cf. Section 4.5.1 and 4.5.2). This allows us to remove the assumption $\mu_4 \subseteq F$ in the proposition above. These results together with some basic results about radical extensions (cf. [GV81] or [Alb03]) allow us to compute $\mathrm{cor}_{L/F}\,(a, b; L, \zeta)_n$, where $a, b \in L$ are radical over F (i.e. some power of a and of b lies in F).

Theorem. *Suppose $F \subseteq N$ is a finite degree field extension. Suppose $\mu_n \subseteq N$ for some n. Let $s_1, s_2 \in N$ be elements such that s_1, s_2 each have finite order in N^*/F^*. Then we can compute $\mathrm{cor}_{N/F}\,(s_1, s_2; N)_n$ via Theorem 4.7.1 and Theorem 4.7.2.*

The formula in Theorem 4.7.2 is very complicated, however, it allows us to recover some of Hwang's results in greater generality (F has a valuation, but is not necessarily Henselian). For example, in the p-primary case, we have (cf. Theorem 4.8.4)

Theorem. *Let F be a valued field. Suppose that $K = F(t_1, t_2)$ is a totally ramified extension of F with respect to v such that $o(t_iF^*) = p^{m_i}$ for $m_i \in \mathbb{N}$. Suppose $T = (t_1, t_2; K)_{p^k}$ is a TTR symbol algebra over K. Let $T' = \mathrm{cor}_{K/F}T$. Then*

$$T' = \left((-1)^{\epsilon_1} t_1^{p^{l_1}} t_2^d, (-1)^{\epsilon_2} t_2^{p^{m_2}}; F\right)_{p^k},$$

with ϵ_1, ϵ_2, and d as defined in Theorem 4.7.2. Also, T' is TTR over F and

$$\Gamma_{T'} = \frac{1}{p^k}\left(\langle v(t_1), v(t_2)\rangle \cap \Gamma_F\right) + \Gamma_F \subseteq \Gamma_T.$$

Finally, we show in Section 4.9 that, when L/F is an extension of GLF's and $D \in \mathcal{D}(L)$, we can compute $D' = cor_{L/F}(D)$ as well as obtain the value group, $\Gamma_{D'}$ and residue $\overline{D'}$.

Chapter 1

Background

In this chapter, we introduce notation and conventions which will be used throughout this paper. We give a review of basic results in the study of central simple algebras and noncommutative valuation theory in the first three sections. In Section 1.4, we recall a few results from [TW87] on TTR algebras and armatures. Then, in Section 1.5, we cover some known results about characters, cup products, and cyclic algebras, some of which can be found in [Ser79]. We define the corestriction and restriction maps in Section 1.6. Finally, we conclude the chapter by introducing the notation of compatibility in Section 1.7.

1.1 Notation and Convention

We let $\mathbb{N}$ stand for the natural numbers, $\{1, 2, \dots\}$. We let $\mathbb{Q}$ stand for the field of rational numbers. Let G be a group. If $a \in G$, we use $o(a)$ to denote the order of a, i.e. $o(a) \in \mathbb{N}$ is minimal such that $a^{o(a)} = 1 \in G$. We may sometimes write $o_G(a)$ if G is not clear from context. If G is finite, we write $exp(G) = lcm\{o(a) : a \in G\}$ for the exponent of G.

For $n \in \mathbb{N}$ and F a field, we write $\mu_n \subseteq F$ to mean that F contains the set of n-th roots of unity. We will also write $\mu(F), \mu_n(F), \mu_n^*(F)$ for, respectively, the set of all roots of unity in F, all n-th roots of unity in F, and all primitive n-th roots of unity in F. If p is a prime, then we use μ_{p^∞} to denote the group of all p-power roots of unity. Let F_{alg} be a given algebraic closure of F. We write F_{sep} for the separable closure of F within F_{alg}.

For a given field extension $F \subseteq K$, we write $Gal(K/F)$ for the Galois group of K over F, i.e. the group of F-automorphisms of K. We write G_F for the Galois group of F_{sep} over F. If $H \subseteq Gal(K/F)$, then we write $\mathcal{F}(H)$ for the fixed field of H.

1.2 Central Simple Algebras

The material in this section can be found in [Pie82, Ch. 12 to Ch. 14] and [Rei75, Ch. 7].

If R is a ring, then the *center* of R is $Z(R) = \{r \in R| \text{ for all } s \in R, rs = sr\}$. For F, a field, an F-*algebra*, A, is a ring (with 1) which contains F in its center, namely $F \subseteq Z(A)$. A *central simple* F-algebra is a finite-dimensional F-algebra, A, with no non-trivial ideals satisfying $Z(A) = F$. We will frequenty omit "F-" when F is understood from context. We define $A^* = \{a \in A \mid \exists\, b \in A \text{ with } ab = ba = 1\}$, the group of units of A. A *division algebra* is an algebra where every non-zero element is a unit, i.e. $A^* = A \backslash \{0\}$. We let $\mathcal{D}(F)$ represent the set of all finite-dimensional division algebras over F. We write $[A : F]$ for the dimension of A over F.

If A is a central simple F-algebra, then Wedderburn's Theorem tells us that $A \cong M_n(D)$, where D is a division algebra over F. Also, D is uniquely determined up to isomorphism and is called *the underlying division algebra* of A. Define a relation on central simple F-algebras by setting $A \sim B$ if A and B have isomorphic underlying division algebras. These classes form a group, $Br(F)$, under the tensor product, $\otimes_F$; we call $Br(F)$ the Brauer group of F. We will denote by $[A]$ the class of A in $Br(F)$. We say that A is split if $[A] = [F]$.

Now, $[A : F]$ is a always a square in $\mathbb{N}$. We write $deg(A) = \sqrt{[A : F]}$ for the degree of A. For any subfield K of A containing F, K is a *maximal subfield* if

$[K : F] = deg(A)$. If D is the underlying division algebra of F, then we write $ind(A) = \sqrt{[D : F]}$ for the (Schur) index of A.

We have the following primary decomposition for division algebras

Proposition 1.2.1. *For $D \in \mathcal{D}(F)$ with $deg(D) = p_1^{e_1} \cdots p_r^{e_r}$ where $p_1, \ldots, p_r$ are distinct primes, there is a unique (up to isomorphism) decomposition $D = D_1 \otimes_F \ldots \otimes_F D_r$ where $D_i \in \mathcal{D}(F)$ and $deg(D_i) = p_i^{e_i}$ for all i.*

Proof. See [Pie82, Th. 14.4]. □

Now suppose that $K \supseteq F$ is any extension of fields. Then $A \otimes_F K$ is a central simple K-algebra, and we write A_K for the underlying division algebra of $A \otimes_F K$. We define the relative Brauer group, $Br(K/F)$, to be the subgroup of $Br(F)$ consisting of all algebras for which $A_K = K$. If K is a maximal subfield of A, i.e. a field K with $[K : F] = deg(A)$, then $[A] \in Br(K/F)$. We may detect subfields of a division algebra D by computing the reduction in index (cf. 1.2.2).

Proposition 1.2.2. *If $D \in \mathcal{D}(F)$ and $K \supseteq F$ is a finite-degree field extension, then*

$$deg(D_K) \geq \frac{deg(D)}{[K : F]}.$$

Equality holds if and only if K is isomorphic to a subfield of D.

Proof. See [Pie82, §14.4] □

Now let $F \subseteq K$ be a finite-dimensional Galois extension of fields, and let G be the Galois group $Gal(K/F)$. Suppose that $f : G \times G \to K^*$ is a 2-*cocycle*, i.e., for all $\sigma, \tau, \rho \in G$, $f(\sigma, \tau) f(\sigma\rho, \tau)^{-1} f(\rho, \sigma\tau) = \tau(f(\rho, \sigma))$. We will write $(K/F, G, f)$ for the *crossed product* algebra defined by the conditions:

1. $(K/F, G, f)$ is a right K-vector space with base $\{u_\sigma \mid \sigma \in G\}$.

2. For all $c \in K, \sigma \in G$, $cu_\sigma = u_\sigma \sigma(c)$.

3. For every $\sigma, \tau \in G$, $u_\sigma \cdot u_\tau = u_{\sigma\tau} f(\sigma, \tau)$.

The crossed product $(K/F, G, f)$ is a central simple F-algebra of degree $|G|$ with maximal subfield K. The correspondence defined by $[A] \leftrightarrow [f]$ is an isomorphism between $Br(K/F)$ and $H^2(G, K^*)$. Moreover, every central simple F-algebra with maximal subfield K is a K/F crossed product. By Köthe's Theorem, every $D \in \mathcal{D}(F)$ has a maximal subfield separable over F. If L is such a maximal subfield of D and K is the Galois closure of L over F, then K is a maximal subfield of $M_n(D)$, where $n = [K : L]$. Thus, every central simple F-algebra is similar to a crossed product and $Br(F_{sep}/F) = Br(F)$.

1.2.1 Cyclic and Symbol Algebras

We now describe two important examples of crossed products. Basic results on cyclic and symbol algebras can be found in [Pie82, Ch. 15], [Rei75, Ch. 7], or [Mil71, §15].

If K is a field cyclic Galois over F with $[K : F] = n$, then the structure of $(K/F, G, f)$ simplifies. Let σ be a generator for $Gal(K/F)$. Then, there exists an $b \in F^*$ such that the 2-cocycle f' defined by, for $0 \le i, j, \le n$,

$$f'(\sigma^i, \sigma^j) = \begin{cases} 1 & \text{if } i + j < n; \\ b & \text{if } i + j \ge n \end{cases}$$

differs from f by a 2-coboundary. There is an $x \in A$ such that $cx = x\sigma(c)$ for all $c \in K$ and $x^n = b$. Then, $\{1, x, \dots, x^{n-1}\}$ is a K-base of A. In this case, $A = (K/F, G, f)$ is a called a *cyclic* algebra and we will adopt the usual convention of writing $A = (K/F, \sigma, b)_n$.

Now assume that $\mu_n \in F^*$ (so $char(F) \nmid n$) and take $\omega \in \mu_n^*(F)$. Fix $a \in F^*$ such that aF^{*n} has order n in F^*/F^{*n}. Let $K = F(\sqrt[n]{a})$ and suppose $\sigma \in Gal(K/F)$ satisfies $\sigma(\sqrt[n]{a}) = \omega\sqrt[n]{a}$. Then for any $b \in F^*$, the cyclic algebra $A = (K/F, \sigma, b)_n$ has generators i, j over F such that $i^n = a, j^n = b$, and $ij = \omega ji$, i.e. $\{i^k j^l : 0 \le k < n,\ 0 \le l < n\}$ is an F-base for A.

In general, if $a, b \in F^*$ and $\mu_n \subseteq F$, then the F-algebra A, generated over F by i, j satisfying relations $i^n = a, j^n = b$, and $ij = \omega ji$ is a central simple F-algebra (cf. [Mil71, Theorem 15.1] or [Dra83, p. 78, Th. 1]). We call A a symbol algebra and will denote A by any of the following expressions

$$A_\omega(a, b; F)_n, \quad (a, b; F, \omega)_n, \quad (a, b; F)_n, \quad (a, b; \omega)_n, \quad (a, b)_n.$$

Note that $deg(A) = n$, and this A is a cyclic algebra if $[F(\sqrt[n]{a}) : F] = n$. In particular, this holds if A is a division algebra.

We now list many important properties of cyclic and symbol algebras.

Proposition 1.2.3. *Let L/F be a cyclic Galois field extension with $[L : F] = n$ and let σ be a generator for Gal(L/F). Take $a, b \in F^*$ and $k \in \mathbb{N}$ with k be prime to n. Suppose $F \subseteq E \subseteq L$ with $[E : F] = m$. Then, we have*

1. $(L/F, \sigma, a)_n \otimes_F (L/F, \sigma, b)_n \sim (L/F, \sigma, ab)_n$.
2. $(L/F, \sigma^k, a^k)_n \cong (L/F, \sigma, a)_n$.
3. $(L/F, \sigma, a^{n/m})_n \sim (E/F, \sigma|_E, a)_m$.

Proof. See [Pie82, Corollary 15.1a and 15.1b]. □

Proposition 1.2.4. *Take $a, b, c \in F^*$ and $n \in \mathbb{N}$ with* char$(F) \nmid n$. *Suppose $\mu_n \subseteq F$ and $\omega \in \mu^*(F)$. Then, the following properties hold.*

1. $(ac, b)_n \sim (a, b)_n \otimes (c, b)_n$ *and* $(a, bc)_n \sim (a, b)_n \otimes (a, c)_n$.
2. $(a, b)_n \sim (b, a^{-1})_n$.
3. *If i is prime to n, then* $(a, b^i; \omega^i)_n \cong (a, b; \omega)_n$.
4. *If $m \mid n$, then* $(a, b^m; \omega)_n \sim (a, b; \omega^m)_{n/m}$.
5. *$(a, b)_n$ is split if and only if b lies in the image of the norm map* $N : F(\sqrt[n]{a})^* \to F^*$.

6. $(a,-a)_n$ *is split.*

7. $(a,1-a)_n$ *is split.*

8. $(a,a)_n \sim (a,-1)_n$*. If* $n = p^r$*, where* p *is prime, then* $(a,a)_n \sim (a,(-1)^{p-1})_n$*.*

Proof. The first seven properties can be found in [Mil71, §15] or [Ser79, Ch. XIV, Prop. 4].

To prove property 1.2.4.8, note that $(a,a)_n \sim (a,a^{-1})_n$ by property 1.2.4.2. So $(a,a)_n \sim (a,a^{-1})_n \otimes (a,-a)_n \sim (a,-1)_n$, using that $(a,-a)_n$ is split. Suppose $n = p^r$. If $p = 2$, then $(a,(-1)^{p-1})_n \cong (a,-1)_n$. If p is odd, then $(a,-1)_n$ has order dividing both 2 and p, whence $(a,-1)_n$ is split and $(a,-1)_n \sim (a,1)_n \cong (a,(-1)^{p-1})_n$. □

We conclude this section by recalling a couple of calculations involving cyclic algebras from [Rei75]. In Prop. 1.2.5, $res_{E/F} : Br(F) \to Br(E)$ is the scalar extension map defined by $[A] \mapsto [A \otimes_F E]$ (see Section 1.6).

Proposition 1.2.5. *Let* L/F *be a finite-degree cyclic Galois extension with generator* $\sigma \in Gal(L/F)$*. Take* $b \in F^*$*. Let* E/F *be any field extension and let* EL *be the composite of* E *and* L *in some larger field containing both* E *and* L*. Let* k *be the smallest integer such that* σ^k *fixes* $L \cap E$*, so* $\langle \sigma^k \rangle = Gal(L/L \cap E) \cong Gal(EL/L)$*. Then,*

$$\mathrm{res}_{E/F}(L/F,\sigma,b) = E \otimes_F (L/F,\sigma,b) \sim (EL/E,\sigma^k,b).$$

Proof. See [Rei75, Thm. 30.8]. □

Proposition 1.2.6. *Suppose* $F \subseteq L \subseteq E$ *are fields where* E *is cyclic Galois over* F*. Let* $G = Gal(E/F)$ *with generator* $\sigma \in Gal(E/F)$ *and let* $H = Gal(E/F)$*. So* $G/H = Gal(L/K)$ *is generated by* $\overline{\sigma} = \sigma H$*. Then for any* $b \in F^*$*,*

$$(L/F,\overline{\sigma},b) \sim (E/F,\sigma,b^{[E:L]}).$$

Proof. See [Rei75, Thm. 30.10]. □

1.3 Valuation Theory

In this section, we will review some basic valuation theory and prove a few results about generalized local fields. The material on noncommutative valuation theory can be found in [Sch50] and [End72]. All of the material here concerning Henselian valuations appears in [JW90]. Also, there is now a survey paper on valuation theory over finite-dimensional division algebras, [Wad02].

Let F be a field and let D be a finite-dimensional F-division algebra. Let Γ be a totally ordered additive abelian group. A *valuation* v on D is a function $v : D^* \to \Gamma$ satisfying, for all $a, b \in D^*$

1. $v(ab) = v(a) + v(b)$.

2. $v(a+b) \geq \min(v(a), v(b))$ for $a + b \neq 0$.

Associated to v we have

the valuation ring	$V_D = \{d \in D^* \mid v(d) \geq 0\} \cup \{0\}$;
the unique maximal (left and right) ideal V_D	$M_D = \{d \in D^* \mid v(d) > 0\} \cup \{0\}$;
the group of valuation units	$U_D = \{d \in D^* \mid v(d) = 0)\}$;
the residue division algebra	$\overline{D} = V_D/M_D$;
the value group	$\Gamma_D = v(D^*)$.

We will write Λ_D for the relative value group Γ_D/Γ_F. We will denote the divisible hull of Γ_D by $\Delta_D = \Gamma_D \otimes_{\mathbb{Z}} \mathbb{Q}$. For E a sub-division ring of D, the restriction $v|_E$ is a valuation on E. In this case, Γ_E is a subgroup of Γ_D. Also, $\overline{E}$ is canonically isomorphic to a sub-division ring of $\overline{D}$. We call $|\Gamma_D : \Gamma_E|$ the *ramification index* of D over E and $[\overline{D} : \overline{E}]$ the *residue degree* of D over E. There is a fundamental inequality, [Sch50, p. 21]

$$[\overline{D} : \overline{E}] \cdot |\Gamma_D : \Gamma_E| \leq [D : E].$$

If $v|_E$ is Henselian (see next paragraph) and $E = Z(D)$, Draxl has sharpened the fundamental inequality to an Ostrowski-type defect theorem, see [Dra84, Th. 2]

$$[D : E] = q^k [\overline{D} : \overline{E}] \cdot |\Gamma_D : \Gamma_E|,$$

where $q = 1$ if $char(\overline{D}) = 0$ and $q = char(\overline{D})$ if $char(\overline{D}) \neq 0$, and $k \geq 0$ is an integer. Morandi has proven that this equation is true without the Henselian assumption (see [?]). We say that D is *defectless* over E if $q^k = 1$.

For $d \in D$, the conjugation map $c_d : D \to D$ given by $c_d(a) = dad^{-1}$ induces an $\overline{F}$-automorphism of $\overline{D}$ which restricts to an $\overline{F}$-automorphism of $Z(\overline{D})$. Thus, we have a surjective map, $\theta_D : \Lambda_D \to Gal(Z(\overline{D})/\overline{F})$ given by $\theta_D(v(d) + \Gamma_F) = c_d \mid_{Z(\overline{D})}$ (cf. [JW90, Prop. 1.7]).

1.3.1 Henselian fields

Let F be a field with valuation v. We say that F is *Henselian* with respect to v if Hensel's Lemma holds for v. For any field $K \supseteq F$, it is well known that v has at least one, but often many different extensions to valuations on K (cf. [End72, p. 62, Cor. 9.7]). However, the situation is very different for division algebras. It was shown by Ershov, and, independently by Wadsworth, that if $D \in \mathcal{D}(F)$, then v extends to D if and only if v has a unique extension to each subfield $L \subseteq D$ containing F (cf. [Ers82, p. 53-55] or [Wad86]). Thus, unlike the commutative setting, if a valuation v on F extends to $D \in \mathcal{D}(F)$, then the extension is unique.

We know that F is Henselian with respect to v if and only if v has a unique extension to every field algebraic over F (cf. [Rib85, Th. 3] or [End72, Cor. 16.6]). Thus, if F is Henselian, then v has a unique extension to each $D \in \mathcal{D}(F)$.

Let F be a Henselian field and let L be a finite degree field extension of F. We say L is *unramified* (or *inertial*) over F if $[\overline{L} : \overline{F}] = [L : F]$ and $\overline{L}$ is separable over $\overline{F}$. If L/F is algebraic of infinite degree, then L is unramified over F if every finite degree subfield of L is unramified over F. We say L is *tamely ramified* over F if $char(\overline{F}) = 0$ or $char(\overline{F}) = p \neq 0$ and $\overline{L}$ is separable over $\overline{F}$, $p \nmid |\Gamma_L : \Gamma_F|$, and $[L : F] = [\overline{L} : \overline{F}]|\Gamma_L : \Gamma_F|$. We say L is *tame and totally ramified* (TTR) over F if L is tamely ramified over F and $[L : F] = |\Gamma_L : \Gamma_F|$. By [Sch50, p.64, Th. 3], if L/F is TTR, then L/F is *totally ramified of radical type* (TRRT), i.e. there exist $n_1, \ldots, n_m$

with $n_1 \dots n_m = n = [L : F]$ and $t_1, \dots t_m \in F$ such that $L = F(\sqrt[n_1]{t_1}, \dots, \sqrt[n_m]{t_m})$ and $nv(t_i)/n_i + n\Gamma_F$ are independent of order n_i in $\Gamma_F/n\Gamma_F$.

Fix an algebraic closure, F_{alg}, of F. There is a unique maximal unramified extension, F_{nr} of F; i.e. for every field L with $F \subseteq L \subseteq F_{alg}$, L is unramified over F if and only if $L \subseteq F_{nr}$. By [End72, §19] or [JW90, p.135], there is a one-to-one correspondence between fields L such that $F \subseteq L \subseteq F_{nr}$ and fields $\overline{L}$ such that $\overline{F} \subseteq \overline{L} \subseteq \overline{F}_{sep}$. In this correspondence, L is Galois over F if and only if $\overline{L}$ is Galois over $\overline{F}$, in which case $Gal(L/F) \cong Gal(\overline{L}/\overline{F})$.

1.3.2 Division Algebras Over Henselian fields

Let F be a Henselian field. We now describe a few types of division algebras over F. Take $D \in \mathcal{D}(F)$. We say that D is an *inertial division algebra* over F if $[\overline{D} : \overline{F}] = [D : F]$ and $Z(\overline{D}) = \overline{F}$. We say that D is *inertially split* if $[D] \in Br(F_{nr}/F)$. We say that D is *tame* if either $char(\overline{F}) = 0$, or $char(\overline{F}) = p$ and the p-primary component of D is inertially split. Equivalently, D is tame if D is defectless over F, $Z(\overline{D})$ is separable over $\overline{F}$ and $char(\overline{F}) \nmid |ker(\theta_D)|$, where θ_D is the map defined in Section 1.3 (cf. [JW90, Lemma 6.1]). We say D is *totally ramified* over F if $[D : F] = |\Gamma_D : \Gamma_F|$. Finally, D is said to be *tame and totally ramified* (TTR) over F if D is totally ramified over F and $char(\overline{F}) \nmid [D : F]$. We let $IBr(F), SBr(F)$, and $TBr(F)$ denote the subgroups of $Br(F)$ consisting of inertial, inertially split, and tame division algebras respectively.

Remark 1.3.1. If $F \subseteq K$ are Henselian fields and $D \in TBr(F)$, then D_K is also tame, since $F_{nr} \subseteq K_{nr}$ and ${}_pBr(F) \to {}_pBr(K)$, where ${}_pBr(F)$ and ${}_pBr(K)$ denote the p-primary component of $Br(F)$ and $Br(K)$ respectively.

We now construct an important type of inertially split algebra. Let F be a Henselian field and suppose $L_1, \dots, L_k$ are cyclic Galois unramified extensions of F such that $L_1 \otimes_F \dots \otimes_F L_k$ is a field. Let σ_i be a generator for $Gal(L_i/F)$ and let $n_i = [L_i : F]$. Let $n = lcm(n_1, \dots, n_k)$ and suppose $a_1, \dots, a_k \in F^*$ are such that $\frac{n}{n_1}v(a_1), \dots, \frac{n}{n_k}v(a_k)$ generate a subgroup of $\Gamma_F/n\Gamma_F$ of order $n_1 \cdots n_k$. Let $N = \otimes_{i=1}^k (L_i/F, \sigma_i, a_i)_{n_i}$. Then N is split by $L_1 \cdots L_k = L_1 \otimes_F \dots \otimes_F L_k$, so $N \in SBr(F)$. Note that N has a maximal subfield, $L_1 \cdots L_k$, which is unramified over F and also a maximal subfield, $F(\sqrt[n_1]{a_1}, \dots, \sqrt[n_k]{a_k})$, which is TRRT over F. Also, $\overline{N} = \overline{L_1 \cdots L_k}$ and $\Gamma_N = \langle \frac{1}{n_1}v(a_1), \dots, \frac{1}{n_k}v(a_k)\rangle + \Gamma_F$. Thus, $deg(N) = [\overline{N} : \overline{F}] = |\Gamma_N : \Gamma_F| = n_1 \cdots n_k$. We say that such an N is *nicely semiramified* (NSR) over F. For more on NSR algebras, see [JW90, §4].

We conclude this section by recalling a condition for determining if a tensor product of valued division algebras is still a division algebra. Morandi originally proved the following result (in greater generality) in [Mor89, Th. 1]; the result can also be found in [JW90, §1].

Theorem 1.3.2. *Let F be a field and let $D_1 \in \mathcal{D}(F)$ and let D_2 be a division ring with $Z(D_2) \supseteq F$. Suppose there are valuations w_1 on D_1 and w_2 on D_2 such that w_1 is defectless and $w_1|_F = w_2|_F$. If $\overline{D_1} \otimes_{\overline{F}} \overline{D_2}$ is a division ring and $\Gamma_{D_1} \cap \Gamma_{D_2} = \Gamma_F$, then $D_1 \otimes_F D_2$ is a division ring with center $Z(D_2)$. Furthermore, there is a unique valuation v on $D_1 \otimes_F D_2$ such that $v|_{D_i} = w_i$ for $i = 1, 2$. Also, $\overline{D_1 \otimes_F D_2} \cong \overline{D_1} \otimes_{\overline{F}} \overline{D_2}$ and $\Gamma_{D_1 \otimes_F D_2} = \Gamma_{D_1} + \Gamma_{D_2}$ (in the divisible hull of Γ_{D_2}).*

1.4 TTR Algebras and Armatures

In this section, we will review several results from [TW87] and define some terminology and conventions that we will use later when dealing with TTR algebras. These will be used in Chapter 2 and Chapter 3.

In the commutative setting, we have the following classical result, see [TW87, Prop. 1.4] or [End72, (20.11)].

Proposition 1.4.1. *Let $F \subseteq K$ be a TTR extension of valued fields. Let $\ell = exp(\Gamma_K/\Gamma_F)$.*

1. *If K is Galois over F, then there is a perfect pairing $\gamma : Gal(K/F) \times (\Gamma_K/\Gamma_F) \to \mu_\ell(\overline{F})$ given by $(\sigma, v(a) + \Gamma_F) \mapsto \overline{\sigma(a)a^{-1}}$.*

2. *If F is Henselian, then K is Galois over F if and only if $\mu_\ell \subseteq F$ if and only if $\mu_\ell \subseteq \overline{F}$.*

Thus, if K is Galois over F, then $Gal(K/F) \cong \Gamma_K/\Gamma_F$, so $Gal(K/F)$ is necessarily abelian.

In the noncommutative setting, Tignol and Wadsworth showed that a similar pairing exists (cf. [TW87, Prop. 3.1]):

Proposition 1.4.2. *Let F be a valued field and let $D \in \mathcal{D}(F)$ be TTR over F. There exists a well-defined bilinear symplectic pairing*

$$C_D : (\Gamma_D/\Gamma_F) \times (\Gamma_D/\Gamma_F) \to \overline{F}^*$$

given by $(v(a) + \Gamma_F, v(b) + \Gamma_F) \mapsto \overline{aba^{-1}b^{-1}}$. Furthermore, C_D is non-degenerate and consequently, $\mu_\ell \subseteq \overline{F}$, where $\ell = exp(\Gamma_D/\Gamma_F)$, and $\Gamma_D/\Gamma_F \cong H \times H$ for some finite abelian group H.

We call C_D the *canonical pairing* of v on D.

1.4.1 Armatures

We now describe the notion of an armature. This idea was first introduced in [TW87] and is a useful tool for dealing with TTR algebras and tensor products of symbol algberas. Let F be a field and let A be an algebra over F. For $t \in A$, we will use $\widetilde{t}$ to denote $tF^* \in A^*/F^*$.

Definition 1.4.3. Let A be a finite-dimensional F-algebra. A subgroup $\mathcal{A}$ of A^*/F^* is an *armature* of A if $\mathcal{A}$ is abelian, $|\mathcal{A}| = [A : F]$ and $F[\mathcal{A}] = A$.

For example, if $A = (a, b; F, \omega)_n$ is a symbol algebra with standard generators i, j (i.e. $i^n = a, j^n = b$, and $ij = \omega ji$), then $\mathcal{A} = \{\widetilde{i}^k\widetilde{j}^l \mid 0 \leq k < n, 0 \leq l < n\}$ is an armature for A.

Suppose A_1 and A_2 are F-algebras with respective armatures $\mathcal{A}_1$ and $\mathcal{A}_2$. Then $\mathcal{A} = \{\widetilde{a \otimes b} : \widetilde{a} \in \mathcal{A}_1, \widetilde{b} \in \mathcal{A}_2\}$ is an armature for $A_1 \otimes_F A_2$. So $\mathcal{A} \cong \mathcal{A}_1 \times \mathcal{A}_2$. In particular, if A is a tensor product of symbol algebras over F, then A has an armature. Conversely, if $Z(A) = F$ and $[A : F] < \infty$, then whenever A has an armature, A is a tensor product of symbol algebras over F (cf. [TW87, Prop. 2.7]).

There is a well-defined non-degenerate symplectic bilinear pairing associated to $\mathcal{A}$, namely $B_{\mathcal{A}} : (\alpha F^*, \beta F^*) \mapsto \alpha\beta\alpha^{-1}\beta^{-1}$. $B_{\mathcal{A}}$ takes values in $\mu(F)$. Let $s = exp(\mathcal{A})$. Define the relative value homomorphism, $\overline{v_A} : \mathcal{A} \to \Delta_F/\Gamma_F$ by $\alpha F^* \mapsto \frac{1}{s} v(\alpha^s) + \Gamma_F$, where $s = exp(\mathcal{A})$. We have the following result (cf. [TW87, Prop. 3.3].

Proposition 1.4.4. *Suppose $A \in \mathcal{D}(F)$ is TTR over F and suppose A has an armature $\mathcal{A}$. Then $\overline{v_A}$ gives an isomorphism $\mathcal{A} \cong \Gamma_A/\Gamma_F$ and $B_{\mathcal{A}}$ is isometric to C_A via $\overline{v_A}$, i.e.*

$$\begin{array}{ccc} \mathcal{A} \times \mathcal{A} & \xrightarrow{B_{\mathcal{A}}} & \mu(F) \\ {\scriptstyle (\overline{v_A}, \overline{v_A})} \downarrow & & \downarrow {\scriptstyle \rho} \\ \Gamma_A/\Gamma_F \times \Gamma_A/\Gamma_F & \xrightarrow{C_A} & \mu(\overline{F}) \end{array}$$

is commutative where $\rho : V_F \to \overline{F}$ is the natural projection which canonically identifies $\mu_n(F)$ with $\mu_n(\overline{F})$ when $\mathrm{char}(\overline{F}) \nmid n$. Consequently $A \cong A_1 \otimes_F \ldots \otimes_F A_k$, where the A_i are symbol algebras with $[A_i : F] = n_i^2 > 1$ and $n_k \mid n_{k-1} \mid \cdots \mid n_1$ are uniquely determined as the invariant factors of Γ_A/Γ_F.

Together with [TW87, Prop. 3.5], we see that A is TTR over F if and only if $\overline{v_A}$ is an isomorphism.

1.4.2 Conventions for TTR Algebras

We have the following theorem proved by Draxl (cf. [Dra84, Th. 1]).

Theorem 1.4.5. *Suppose $D \in \mathcal{D}(F)$ is TTR over F. If F is Henselian, then D is isomorphic to a tensor product of symbol algebras.*

It follows, as noted in the previous section, that any such D has an armature. So Prop. 1.4.4 applies to D. Let p be a prime. Suppose T is a p-primary TTR division algebra over F. So, by Theorem 1.4.5, $T \cong (a_1, b_1)_{p^{r_1}} \otimes_F \ldots \otimes_F (a_d, b_d)_{p^{r_d}}$, where $a_1, b_1, \ldots, a_d, b_d \in F^*$. We will show later in Proposition 1.4.6 that $a_1, b_1, \ldots, a_d, b_d$ map to $\mathbb{Z}/p\mathbb{Z}$-independent elements in $\Gamma_F/p\Gamma_F$, i.e. for $m_i, n_i \in \mathbb{Z}$

$$\sum_{i=1}^{d} m_i v(a_i) + n_i v(b_i) \in p\Gamma_F \text{ if and only if } m_i, n_i \in p\mathbb{Z} \text{ for all } i.$$

Let $p^r = lcm\{p^{r_1}, \ldots, p^{r_k}\}$ and let ω be a primitive p^r root of unity. For $1 \leq \ell \leq k$, we let i_ℓ, j_ℓ be standard generators of $(a_\ell, b_\ell)_{p^{r_\ell}}$, i.e.

$$i_\ell^{p^{r_\ell}} = a_\ell,\ j_\ell^{p^{r_\ell}} = b_\ell,\ i_\ell j_\ell = \omega^{p^{r-r_\ell}} j_\ell i_\ell.$$

Also, let $\mathcal{T}$ denote the armature of T generated by $i_1F^*, j_1F^*, \ldots, i_dF^*, j_dF^*$.

Now, if $\tau \in T$ is the pre-image of an element $\tau F^* \in \mathcal{T}$, then we will call τ an *armature element* of T. Suppose τ is an armature element of T. We may write $\widetilde{\tau} = \widetilde{i_1}^{s_1}\widetilde{j_1}^{t_1} \ldots \widetilde{i_d}^{s_d}\widetilde{j_d}^{t_d}$, with each s_k and t_k uniquely determined up to p^{r_k}. So, for some $f \in F^*$, we have

$$\tau = f i_1^{s_1} j_1^{t_1} \ldots i_d^{s_d} j_d^{t_d} \tag{1.1}$$

We call $i_k^{s_k}$ and $j_k^{t_k}$ *factors* of τ; if we want to be more specific, then we will say "*the* i_k *factor*" or "*the* j_k *factor*".

Now suppose that $\widetilde{\tau}$ has order p^e. Note that $\mathcal{T}$ is a direct sum of finite groups, with $\widetilde{i_1}$, $\widetilde{j_1}$, $\ldots$, $\widetilde{i_d}$, $\widetilde{j_d}$ each generating a different direct summand. Thus, each factor has order dividing p^e (i.e. $i_k^{s_k p^e} F^* = j_k^{t_k p^e} F^* = F^*$). Furthermore, some factor of τ must have order p^e in T^*/F^*; we will call any such factor a *leading term* or a *leading factor* of τ.

Proposition 1.4.6. *Suppose T is a p-primary TTR division algeba over F. Then $T \cong (a_1, b_1)_{p^{r_1}} \otimes_F \ldots \otimes_F (a_d, b_d)_{p^{r_d}}$, where $a_1, b_1, \ldots, a_d, b_d \in F^*$ map to $\mathbb{Z}/p\mathbb{Z}$-independent elements in $\Gamma_F/p\Gamma_F$.*

Proof. Suppose there exist $m_i, n_i \in \mathbb{Z}$ such that

$$\sum_{k=1}^{d} m_i v(a_i) + n_i v(b_i) \in p\Gamma_F.$$

Let $i_1, j_1, \ldots, i_d, j_d$ be standard generators for T and let $\mathcal{T}$ be the armature generated by $i_1F^*, j_1F^*, \ldots, i_dF^*, j_dF^*$. Then, $\widetilde{i_1}^{m_1p^{r_1-1}}, \widetilde{j_1}^{n_1p^{r_1-1}}, \cdots, \widetilde{i_d}^{m_dp^{r_d-1}}, \widetilde{j_d}^{n_dp^{r_d-1}}$ are $\mathbb{Z}/p\mathbb{Z}$-independent in $\mathcal{T}$. Since $v : \mathcal{T} \to \Gamma_T/\Gamma_F$ is an isomorphism (Theorem 1.4.4), the elements $\frac{1}{p}v(a_1), \frac{1}{p}v(b_1), \ldots, \frac{1}{p}v(a_d), \frac{1}{p}v(b_d)$ have $\mathbb{Z}/p\mathbb{Z}$ independent images in $(1/p\Gamma_F \cap \Gamma_T)/\Gamma_F$. Thus, $v(a_1), v(b_1), \ldots, v(i_d), v(j_d)$ have $\mathbb{Z}/p\mathbb{Z}$-independent images in $\Gamma_F/p\Gamma_F$. □

1.5 Cohomology and Cyclic and Symbol Algebras

In this section, we will use Galois cohomology to describe cyclic and symbol algebras via cup products. The material concerning cyclic algebras and characters is not new, however, the author cannot find a good reference in the literature. Material on group and Galois cohomology can be found in [Ser79, Ch. VII], [NSW00], and [CF67].

1.5.1 Characters and Semi-symbols

Let $F \subseteq K$ be an algebraic Galois extension (possibly of infinite degree). Set $G = \mathit{Gal}(K/F)$, a profinite group. We will denote by $\mathit{Hom}_c(G, \mathbb{Q}/\mathbb{Z})$, the group of continuous homomorphisms from G to $\mathbb{Q}/\mathbb{Z}$, i.e. homomorphisms with open kernel where G has the Krull topology and $\mathbb{Q}/\mathbb{Z}$ has the discrete topology. This group is called the *character group* of G, and its elements are characters of G. Also, we write F_{sep} for the separable closure of F and G_F for the absolute Galois group of F, $\mathit{Gal}(F_{sep}/F)$. We will write $X(F)$ to denote $\mathit{Hom}_c(G_F, \mathbb{Q}/\mathbb{Z})$ and $X(K/F)$ to denote $\mathit{Hom}_c(\mathit{Gal}(K/F), \mathbb{Q}/\mathbb{Z})$.

Now let A be a discrete $\mathbb{Z}[G]$-module (i.e., A is given the discrete topology and G acts continuously on A). We will sometimes refer to $\mathbb{Z}[G]$-modules as G-modules, cf. [Ser79, Ch. VII]. We let $Z^n(G,A)$ denote the set of continuous n-cocycles, $B^n(G,A)$ the set of continuous n-coboundaries, and $H^n(G,A) = Z^n(G,A)/B^n(G/A)$ the group of continuous n-cohomology classes. When G is understood from context, we may abbreviate $Z^n(G,A)$, $B^n(G,A)$, and $H^n(G,A)$ to $Z^n(A)$, $B^n(A)$, and $H^n(Z)$ respectively.

In this sections, we construct semi-symbols, which are elements of $H^2(G_F, F^*_{sep})$ corresponding to cyclic algebras in $Br(F)$. This construction is described briefly in [Ser79, Chapter XIV, §1].

Fix a field F. The exact sequence of discrete G_F-modules (with trivial G_F-action)

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0,$$

begets a long exact sequence in cohomology

$$\dots \longrightarrow H^1(G_F,\mathbb{Q}) \longrightarrow H^1(G_F,\mathbb{Q}/\mathbb{Z}) \xrightarrow{\delta} H^2(G_F,\mathbb{Z}) \longrightarrow H^2(G_F,\mathbb{Q}) \longrightarrow \dots$$

From the triviality of the G_F-action, we have that $H^1(G_F,\mathbb{Q}/\mathbb{Z}) = Z^1(G_F,\mathbb{Q}/\mathbb{Z}) = Hom_c(G_F,\mathbb{Q}/\mathbb{Z})$. Also, because $\mathbb{Q}$ is uniquely divisible, both $H^1(G_F,\mathbb{Q})$ and $H^2(G_F,\mathbb{Q})$ are trivial; thus $H^1(G_F,\mathbb{Q}/\mathbb{Z}) \cong H^2(G_F,\mathbb{Z})$ via the connecting homomorphism δ. Thus, if we take $\chi \in Hom_c(G_F,\mathbb{Q}/\mathbb{Z})$, then $\delta\chi \in H^2(G_F,\mathbb{Z})$. Now take an element $b \in F^* = H^0(G_F, F^*_{sep})$. The cup product $\delta\chi \cup b$ is an element of $H^2(G_F, \mathbb{Z} \otimes_{\mathbb{Z}} F^*_{sep}) = H^2(G_F, F^*_{sep}) = Br(F)$. A *semi-symbol* is an element of the form $\delta\chi \cup b$. As in [Ser79, Chapter XIV, §1], we will write (χ, b) for the semi-symbol $\delta\chi \cup b$.

Now δ is a group homomorphism and the cup product is bilinear, so for $\chi_1, \chi_2 \in Hom_c(G_F,\mathbb{Q}/\mathbb{Z})$ and $a, b \in F^*$ we have

$$(\chi_1, b) + (\chi_2, b) = (\chi_1 + \chi_2, b) \qquad \text{and} \qquad (\chi_1, b) + (\chi_1, c) = (\chi_1, bc).$$

1.5.2 Relationship to cyclic algebras

We wish to show explicitly that the central simple algebra of degree $n = o(\chi)$ represented by (χ, b) is a cyclic algebra. Let $F(\chi)$ denote the fixed field of $ker(\chi)$. Since $ker(\chi)$ is open (so of finite index) and normal in G_F, $F(\chi)$ is a finite degree Galois extension of F, with Galois group isomorphic to $G_F/ker(\chi)$. But $G_F/ker(\chi)$ is isomorphic to the finite subgroup $im(\chi)$ of $\mathbb{Q}/\mathbb{Z}$, so $Gal(F(\chi)/F)$ is cyclic. Say $G_F/ker(\chi) \cong (\frac{1}{n}\mathbb{Z})/\mathbb{Z}$. Let $\sigma_\chi = \chi^{-1}(1/n)$, then $\sigma_\chi|_{F(\chi)}$ is a distinguished generator of $Gal(F(\chi)/F)$.

Set $L = F(\chi)$, $\sigma = \sigma_\chi$, and $G = Gal(L/F)$. Note that χ is the inflation to G_F of a uniquely determined character of G. For simplicity, consider χ as an element of $Hom_c(G, \mathbb{Q}/\mathbb{Z})$ and (χ, b) as an element of $H^2(G, L^*) = Br(L/F)$. Note that $b \in F^* = H^0(G, L^*) = H^0(G_F, F^*_{sep})$.

Let us chase down the 2-cocycle $\delta\chi : G \times G \to \mathbb{Z}$, which is the image of χ under the connecting homomorphism

$$\begin{array}{ccc} & Z^1(G,\mathbb{Q}) \to Z^1(G,\mathbb{Q}/\mathbb{Z}) \\ & \downarrow \partial & . \\ Z^2(G,\mathbb{Z}) \to Z^2(G,\mathbb{Q}) & & \end{array}$$

Recall that $\chi(\sigma) = 1/n \ mod\ \mathbb{Z}$. For $0 \le i < n$, define $\chi'(\sigma^i) = i/n$. Then χ' maps to χ under the map of cocycles $Z^1(G, \mathbb{Q}) \to Z^1(G, \mathbb{Q}/\mathbb{Z})$. So $\delta(\chi) = \partial(\chi')$ is defined by $\partial(\chi')(\sigma^i, \sigma^j) = \chi'(\sigma^i) + \chi'(\sigma^j) - \chi'(\sigma^{i+j})$. After simplification, we see that, for $0 \le i, j < n$,

$$\delta(\chi)(\sigma^i, \sigma^j) = \begin{cases} 0, & \text{if} \quad i + j < n \\ 1, & \text{if} \quad i + j \ge n \end{cases}$$

From an easy cup product computation (cf. [Ser79, p.176]), we see that

$$(\delta\chi \cup b)(g_1, g_2) = \delta\chi(g_1, g_2) \otimes_{\mathbb{Z}} b = b^{\delta\chi(g_1,g_2)},$$

where $g_1, g_2 \in G$, and the last equality identifies $\mathbb{Z} \otimes_{\mathbb{Z}} L^*$ with L^*. Thus, the 2-cocycle,

(χ, b) is defined by, for $0 \leq i, j < n$,

$$(\chi, b)(\sigma^i, \sigma^j) = \begin{cases} 1, & \text{if} \quad i + j < n \\ b, & \text{if} \quad i + j \geq n \end{cases}$$

Therefore, (χ, b) corresponds to the cyclic algebra $(L/F, \sigma, b)_n$, where $n = o(\chi)$.

1.6 Restriction and Corestriction

We now describe two homological maps with Brauer group interpretations. Most of the facts from this section can be found in [Ser79, Ch. VIII], [Pie82, Ch. 14], [Rei75, Ch. 7], or [NSW00].

Let $H \subseteq G$ be groups with $|G : H| < \infty$. Let A be a G-module. For $k \geq 0$, we define the homological *restriction* map $res_k : H^k(G, A) \to H^k(H, A)$ by $[f] \mapsto [f|_{\underbrace{H \times \cdots \times H}_{k \text{ times}}}]$. Now suppose K/F is a finite-degree separable field extension. Let $G = G_F$ and $H = G_K$. Since $Br(F) \cong H^2(G, F^*_{sep})$ and $Br(K) \cong H^2(H, F^*_{sep})$, we have a corresponding map $res_{K/F} : Br(F) \to Br(K)$ given by scalar extension, $[A] \mapsto [A \otimes_F K]$ (cf. [Pie82, Ch. 14.7]).

There is a corresponding map going in the other direction $cor_k : H^k(H, A) \to H^k(G, A)$.

Definition 1.6.1. Suppose $H \subseteq G$ are groups with $|G : H| < \infty$. Let $g_1, \ldots, g_m$ a fixed set of coset representatives of H in G. Let A be a G-module and for $a \in A^H = H^0(H, A)$, define

$$cor_0(a) = N_{G/H}(a) = (\sum_{i=1}^{m} g_m)a.$$

The map cor_0 extends to maps at each level $cor_k : H^k(H, A) \to H^k(G, A)$ for $k \geq 0$ (cf. [Ser79, Ch. VII]). For each k, we have $cor_k \circ res_k(f) = mf$ (cf. [Ser79, Ch. VII, Prop. 6]). If K/F is a finite-degree separable field extension, then we have a corresponding map $cor_{K/F} : Br(K) \to Br(F)$, however, this map is difficult to describe (cf. [Jac96, §3.13, p.149]). An explicit formula for how to compute $cor_{K/F}$ cohomologically is given in the appendix of [Hwa95a].

Both *res* and *cor* have some important functorial properties.

Proposition 1.6.2. *Let $H \subseteq G$ be groups with $|G : H| = m < \infty$. Let A be a G-module. Fix $k \geq 0$ and let ∂_k denote the boundary map $\partial_k : H^k(\cdot, A) \to H^{k+1}(\cdot, A)$. Then the following diagram commutes.*

$$\begin{array}{ccccc} H^k(G,A) & \xrightarrow{res} & H^k(H,A) & \xrightarrow{cor} & H^k(G,A) \\ \downarrow{\scriptstyle \partial_k} & & \downarrow{\scriptstyle \partial_k} & & \downarrow{\scriptstyle \partial_k} \\ H^{k+1}(G,A) & \xrightarrow{res} & H^{k+1}(H,A) & \xrightarrow{cor} & H^{k+1}(G,A). \end{array}$$

Proof. See [Bro94, Ch.III, §9], [NSW00, Prop 1.5.2], or [Ser79, Ch. VII, §7]. □

Proposition 1.6.3. *Let $F \subseteq L$ be a finite degree field extension. Then the following diagram commutes*

$$\begin{array}{ccc} Br(L) & \xrightarrow{res_{L(x)/L}} & Br(L(x)) \\ \downarrow{\scriptstyle cor_{L/F}} & & \downarrow{\scriptstyle cor_{L(x)/F(x)}} \\ Br(F) & \xrightarrow{res_{F(x)/F}} & Br(F(x)) \end{array}$$

i.e. $res_{F(x)/F}cor_{L/F} = cor_{L(x)/F(x)}res_{L(x)/L}$. *Furthermore, if $A \in Br(L)$ and $B \in Br(F)$ satisfy*

$$cor_{L(x)/F(x)}res_{L(x)/L}(A) = res_{F(x)/F}(B),$$

then $cor_{L/F}(A) = B$.

Proof. Let K be a field and let $K[x]$ and $K(x)$ denote the polynomial ring and function field in one variable over K respectively. Fix $D \in \mathcal{D}(K)$. Since D has no zero-divisors, $D \otimes_K K[x] \cong D[x]$ has no zero divisiors. Then, by transitivity of scalar extension, $D \otimes_K K(x) \cong D[x] \otimes_{K[x]} K(x)$. Because $D[x] \otimes_{K[x]} K(x)$ is a central localization of $D[x]$, $D \otimes_K K(x)$ is a division algebra over $K(x)$ of dimension $[D : K]$. Since $D \in \mathcal{D}(K)$ was arbitrary, this shows that $res_{K(x)/K}$ is injective.

We may identify $Br(F)$ and $Br(L)$ with their images respectively in $Br(F(x))$ and $Br(L(x))$ (via the injective maps $res_{F(x)/F}$ and $res_{L(x)/L}$). Since $Gal(L(x)/F(x)) \cong Gal(L/F)$, and $cor_{L/F}$ is a sum over $Gal(L/F)$, the maps $cor_{L/F}$ and $cor_{L(x)/F(x)}$ agree on the image of $Br(L)$ in $Br(L(x))$. Thus, $res_{F(x)/F} cor_{L/F} = cor_{L(x)/F(x)} res_{L(x)/L}$.

Applying this to the assumption on A and B, we get $res_{F(x)/F} cor_{L/F}(A) = res_{F(x)/F}(B)$. The injectivity of $res_{F(x)/F}$ finishes the argument. □

Proposition 1.6.4. *Suppose L/F is a finite Galois extension. Let $G = G_F$, $H = G_L$ and suppose $\sigma_1, \ldots, \sigma_m$ form a complete set of coset representatives of H in G. If $\chi \in X(L)$, then $cor_{L/F}(\chi)(g) = \sum_{i=1}^{m} \chi(\sigma_i g \sigma_{i'}^{-1})$, where $i' \in \{1, \ldots, m\}$ is determined by the condition $\sigma_i g \sigma_{i'}^{-1} \in H$.*

Proof. See [Mer85, 1.3]. □

1.7 Compatibility Factors

There are two types of compatibility factors which will arise often in our restriction and corestriction formulae. We will describe them both here. Let G be a group.

Suppose G_1, G_2 are cyclic subgroups of G with distinguished generators g_1, g_2 respectively. There are, for $i = 1, 2$, surjective homomorphisms $\mu_i : G_i \to G_1 \cap G_2$ given by $\mu_i(g) = g^{|G_i : G_1 \cap G_2|}$. We define $comp(g_1, g_2) = \{c \in \mathbb{Z} : \mu_1(g_1)^c = \mu_2(g_2)\}$. For any c_1 satisfying $\mu_1(g_1)^{c_1} = \mu_2(g_2)$, we have $comp(g_1, g_2) = \{c \in \mathbb{Z} : c \equiv c_1 \ mod \ |G_1 \cap G_2|\}$. If $c_1 \in comp(g_1, g_2)$ and $c_2 \in comp(g_2, g_1)$, then necessarily, $c_1 c_2 \equiv 1 \ mod \ |G_1 \cap G_2|$. We say that g_1 and g_2 are *compatible* if $1 \in comp(g_1, g_2)$.

Suppose instead that G_1, G_2 are normal subgroups of G where G/G_i are both cyclic. Let σ_i be distinguished generators of G/G_i. There are surjective homomorphisms $\pi_i : G/G_i \to G/G_1G_2$ given by $\pi_i(\sigma) = \sigma G_1 G_2$. We may similarly define $\overline{comp}(\sigma_1, \sigma_2) = \{c \in \mathbb{Z} : \pi_1(\sigma_1)^c = \pi_2(\sigma_2)\}$. Again, for any c_1 satisfying $\pi_1(\sigma_1)^{c_1} = \pi_2(\sigma_2)$, we have $\overline{comp}(\sigma_1, \sigma_2) = \{c \in \mathbb{Z} : c \equiv c_1 \; mod \; |G : G_1G_2|\}$. Finally, if $c_1 \in \overline{comp}(\sigma_1, \sigma_2)$ and $c_2 \in \overline{comp}(\sigma_2, \sigma_1)$, then necessarily, $c_1c_2 \equiv 1 \; mod \; |G : G_1G_2|$ and we say that σ_1 and σ_2 are *compatible* if $1 \in \overline{comp}(\sigma_1, \sigma_2)$.

Remark 1.7.1. In the previous paragraph σ_1 and σ_2 are compatible if and only if there is a $\sigma \in G$ for which $\sigma G_i = \sigma_i$ for $i = 1, 2$. For, if there exists a $\sigma \in G$ with $\sigma G_i = \sigma_i$, then $\pi_1(\sigma_1) = \sigma G_1G_2 = \pi_2(\sigma_2)$, so σ_1 and σ_2 are compatible. For the converse, suppose σ_1 and σ_2 are compatible. Let $\tau_i \in G$ satisfy $\tau_i G_i = \sigma_i$ for $i = 1, 2$. Then $\tau_1 G_1 G_2 = \pi_1(\sigma_1) = \pi_2(\sigma_2) = \tau_2 G_1 G_2$, whence there exist $g_i \in G_i$ such that $\tau_1 g_1 = \tau_2 g_2$. Set $\sigma = \tau_1 g_1 = \tau_2 g_2$, so $\sigma G_1 = \tau_1 G_1 = \sigma_1$ and $\sigma G_2 = \tau_2 G_2 = \sigma_2$.

Remark 1.7.2. In both cases the set of compatibility factors are cosets of cyclic subgroups of $\mathbb{Z}$. If G_1 and G_2 are cyclic with generators g_1 and g_2 respectively, then $|G_1 \cap G_2| = 1$ if and only if $comp(g_1, g_2) = \mathbb{Z}$. In general, $comp(g_1, g_2)$ is a coset of $|G_1 \cap G_2|\mathbb{Z}$ in $\mathbb{Z}$. Similarly, if G/G_1 and G/G_2 are cyclic with generators σ_1, σ_2, then $|G/G_1G_2| = 1$ if and only if $\overline{comp}(\sigma_1, \sigma_2) = \mathbb{Z}$. In general, $\overline{comp}(\sigma_1, \sigma_2)$ is a coset of $|G : G_1G_2|\mathbb{Z}$ in $\mathbb{Z}$. Note, however, that $comp(g_1, g_2)$ and $\overline{comp}(\sigma_1, \sigma_2)$ will always contain a integer prime to $|G_1 \cap G_2|$ and $|G/G_1G_2|$ respectively.

Chapter 2

Algebras Over Generalized Local Fields

Recall that we call F a generalized local field (abbrev. GLF) if F is Henselian and $\overline{F}$ is a finite field. The study of algebras over GLF's is motivated by what can be said in the strictly Henselian case (i.e. the case where F is Henselian and $\overline{F}$ is separably closed). Strictly Henselian fields have abelian profinite absolute Galois groups, whereas the absolute Galois group of a GLF is abelian by procyclic. Correspondingly, the structure of division algebras over GLF's is more complicated. For example, every division algebra over a strictly Henselian field is isomorphic to a tensor product of symbol algebras. (For, division algebras are always TTR over their center.) However, one cannot hope to say the same over a GLF; there exist cyclic NSR division algebras which cannot be symbol algebras because F doesn't contain enough roots of unity. We show in Theorem 2.4.1 that every division algebra over a GLF is isomorphic to a tensor product of cyclic algebras. Eric Brussel at Emory University has proven Theorem 2.4.1 using a different method, however, we have just recently received his proof (cf. [Bru04]).

Also, for tensor products of symbol algebras over a strictly Henselian field, Tignol and Wadsworth gave an algorithm for computing the underlying division algebra in

[TW87, Th. 4.3]. We may ask, do we have a similar algorithm for over a GLF? To this end, we first show, in Theorem 2.2.1, that the algorithm given in [TW87, Th. 4.3] holds more generally; given a valued field F, and A, a tensor product of symbol algebras (over F) with an appropriate property, the algorithm in [TW87, Th. 4.3] will still compute the underlying division algebra. We apply this algorithm in Theorem 2.4.1 to produce the underlying division algebra over an algebra presented as $N \otimes_F T$, where N is an NSR division algebra and T is a TTR division algebra.

The chapter is organized as follows. In Section 2.1, we prove several basic facts about algebras over a GLF. In Section 2.2, we show in Theorem 2.2.1 that [TW87, Th. 4.3] holds in greater generality. We give applications for Theorem 2.2.1 in Section 2.3. Finally, in Section 2.4 we prove Theorem 2.4.1 from Theorem 2.2.1 by using an index formula, Prop. 2.1.4.

2.1 Background

In this section, we give a few examples of generalized local fields and prove a few important facts about division algebras over GLF's.

As mentioned in the introduction, generalized local fields are a generalization of the local fields studied in number theory. The non-Archimedian local fields of number theory are fields with complete discrete (rank 1) valuations with finite residue field. These were the fields for which Hensel proved Hensel's Lemma. The difference between local fields and GLF's is that GLF's are allowed to have as value group any totally ordered abelian group. For example, for any finite field, K, the Laurent series field $K((x))$ is a local field, whence a generalized local field. In general, we may iterate the Laurent series construction; define $K((x_1))((x_2))\ldots((x_i)) = \big(K((x_1))((x_2))\ldots((x_{i-1}))\big)((x_i))$. We have a more explicit description of such a field. Give $\mathbb{Z}^n = \prod_{i=1}^{n} \mathbb{Z}$ the right-to-left lexicographical ordering (i.e. $(a_1, \ldots, a_n) < (b_1, \ldots, b_n)$ if there is a k such that $a_k < b_k$ and $a_i = b_i$ for all $i > k$). Then, we define the n-fold iterated Laurent series over K,

$$F = K((x_1))((x_2))\dots((x_n)) = \left\{ \sum_{(a_1,\dots,a_n)\in\mathbb{Z}^n} c_{a_1,\dots,a_n} x_1^{a_1}\cdots x_n^{a_n} \,\middle|\, \begin{array}{c}\{(a_1,\dots,a_n)|\ c_{a_1,\dots,a_n}\neq 0\}\\ \text{is well-ordered}\end{array} \right\}.$$

Then F is a GLF with respect to the standard valuation

$$v\left(\sum_{(a_1,\dots,a_n)\in\mathbb{Z}^n} c_{a_1,\dots,a_n} x_1^{a_1}\cdots x_n^{a_n} \right) = \min\{(a_1,\dots,a_n)|\ c_{a_1,\dots,a_n}\neq 0\}.$$

In this case, $\Gamma_F = \mathbb{Z}^n$ and $\overline{F} = K$.

We may view the valuation over n-fold iterated Laurent series as the composition of n discrete valuations. In general, if w is a valuation on K and y is a valuation on $\overline{K}$, then we may form the the composite valuation, v, on K as follows. Let W be the valuation ring associated to w and let $Y \subseteq \overline{K}$ be the valuation ring associated to y. Let $V = \pi^{-1}(Y) \subseteq K$ where $\pi : W \to \overline{K}$ is the canonical epimorphism. Then V is a valuation ring with quotient field K. The valuation v associated to V is the composite valuation of w and y. The residue field of K with respect to V is $\overline{Y}$ and there is a canonical short exact sequence

$$0 \longrightarrow \Gamma_y \longrightarrow \Gamma_v \longrightarrow \Gamma_w \longrightarrow 0,$$

where $\Gamma_y, \Gamma_v, \Gamma_w$ are the value groups with respect to y, v, and w respectively. In this construction v is Henselian if and only if y and w are each Henselian (see [Rib85, p. 211, Prop. 10]). This allows us to see that, for K a finite field, $F = K((x_1))((x_2))\dots((x_n))$ is Henselian with respect to the standard valuation.

Using composite valuations, we may construct other examples of generalized local fields. For any local field K, the field $F = K((x_1))((x_2))\dots((x_n))$ is a GLF with value group $\Gamma_K + \mathbb{Z}^n \cong \mathbb{Z}^{n+1}$ and residue $\overline{K}$. Recently, there has been extensive work done on higher local fields; these are generalized local fields with valuation constructed as the composite of n complete discrete valuations. A compilation of recent results (given in a 1999 conference) in given in [FK00]. In particular, we find a full classification of higher local fields as well as a development of the Milnor K-group and generalized class field theory for higher local fields.

We now prove some properties about division algebras over a GLF.

Proposition 2.1.1. *Suppose F is a GLF. If $I \in \mathcal{D}(F)$ is inertial over F, then I is split, i.e. $IBr(F)$ is trivial.*

Proof. Because F is Henselian, [JW90, Th. 2.8] tells us that $IBr(F) \cong Br(\overline{F})$. By a famous result of Wedderburn, since $\overline{F}$ is finite, every finite-dimensional $\overline{F}$-central division algebra is a field. In other words, $\mathcal{D}(\overline{F}) = \{\overline{F}\}$, so $IBr(F) \cong Br(\overline{F}) = \{[\overline{F}]\}$ is trivial. □

Corollary 2.1.2. *If D is tame, then $D \sim N \otimes_F T$ where $N, T \in \mathcal{D}(F)$, with N NSR and T TTR.*

Proof. Since F is Henselian and D is tame, [JW90, Lemma 6.2] tells us that $D \sim S \otimes_F T$, where $[S] \in SBr(F)$ and T is tame and totally ramified. By [JW90, Lemma 5.14], $S \sim I \otimes_F N$, where $I \in IBr(F)$ and N is NSR. But $IBr(F)$ is trivial, so $D \sim S \otimes_F T \sim N \otimes_F T$. □

Proposition 2.1.3. *Suppose F is a GLF. Then every finite-degree unramified field extension of F is cyclic Galois over F. Furthermore, unramified fields over F are classified by degree. In particular, if N is inertially split over F, then the underlying division algebra of N is cyclic.*

Proof. Since $\overline{F}$ is finite, field extensions of $\overline{F}$ are cyclic Galois over $\overline{F}$ and are classified by their degree. By the correspondence between unramified extensions of F and fields separable over $\overline{F}$ (cf. Section 1.3.1), the same is true of unramified field extensions of F. If N is an inertially split division algebra, then the underlying division algebra, D, of N is NSR and split by a unramified, whence, cyclic extension. Thus, D is isomorphic to a cyclic algebra. □

For $D \in \mathcal{D}(F)$, we write Λ_D for Γ_D/Γ_F.

Proposition 2.1.4. *Let (F, v) be a Henselian valued field. Take $N, T \in \mathcal{D}(F)$, with N nicely semiramified over F and T tame and totally ramified over F. Let D be the underlying division algebra of $N \otimes_F T$. Then*

$$\frac{deg\ D}{deg\ \overline{D}} = \frac{deg\ N \cdot deg\ T}{\left|\Lambda_N \cap \Lambda_T\right|}.$$

Proof. We will use residue and value group information to recover $[D : F]$.

We have a surjective map, $\theta_N : \Lambda_N \to Gal(Z(\overline{N})/\overline{F})$ given by $\theta_N(v(d) + \Gamma_F) = c_d\big|_{Z(\overline{N})}$ where $c_d : \overline{N} \to \overline{N}$ is induced by conjugation by d (cf. Section 1.3 or [JW90, Prop. 1.7]). Since N is nicely semiramified over F, we have that $\overline{N}$ is a field and $|\Lambda_N| = [\overline{N} : \overline{F}]$; thus θ_N is an isomorphism. Nicely semiramified division algebras are, by definition, inertially split, so we use [JW90, Theorem 6.3] to obtain $Z(\overline{D}) \cong \mathcal{F}\big(\theta_N(\Lambda_N \cap \Lambda_T)\big)$.

$$\begin{aligned}
[Z(\overline{D}) : \overline{F}] &= \big[\mathcal{F}\big(\theta_N(\Lambda_N \cap \Lambda_T)\big) : \overline{F}\big] && \text{(Theorem 6.3)} \\
&= \big[Gal(Z(\overline{N})/\overline{F}) : \theta_N(\Lambda_N \cap \Lambda_T)\big] && \text{(Galois correspondence)} \\
&= |\Lambda_N : (\Lambda_N \cap \Lambda_T)| && (\theta_N \text{ is an isomorphism}) \\
&= |\Lambda_N| / |\Lambda_N \cap \Lambda_T|.
\end{aligned}$$

Also, [JW90, Theorem 6.3] tells us that $\Gamma_D = \Gamma_N + \Gamma_T$. Thus, $\Lambda_D = \Lambda_N + \Lambda_T$, so $|\Lambda_D| = |\Lambda_N||\Lambda_T|/|\Lambda_N \cap \Lambda_T|$. Thus, as D is defectless, we have, by Draxl's Ostrowski-type inequality (cf. Section 1.3),

$$\begin{aligned}
(deg\ D/deg\ \overline{D})^2 &= [D : F]/[\overline{D} : Z(\overline{D})] \\
&= [\overline{D} : \overline{F}] \cdot |\Lambda_D| / [\overline{D} : Z(\overline{D})] \\
&= [Z(\overline{D}) : \overline{F}] \cdot |\Lambda_N||\Lambda_T| / |\Lambda_N \cap \Lambda_T| \\
&= |\Lambda_N|^2 |\Lambda_T| / |\Lambda_N \cap \Lambda_T|^2 \\
&= [N : F] \cdot [T : F] / |\Lambda_N \cap \Lambda_T|^2.
\end{aligned}$$

This shows that $deg\ D/deg\ \overline{D} = deg\ N \cdot deg\ T / \big|\Lambda_N \cap \Lambda_T\big|$. □

The formula in Prop. 2.1.4 simplifies if $\overline{D}$ is a field. Note that $\overline{D}$ is always a field if F is a GLF.

Corollary 2.1.5. *If $\overline{D}$ is a field, then* $deg(D) = deg(N)deg(T)/|\Lambda_N \cap \Lambda_T|, \Gamma_D = \Gamma_N + \Gamma_T$, *and* $[\overline{D} : \overline{F}] = deg(N)/|\Lambda_N \cap \Lambda_T|$.

Proof. If $\overline{D}$ is a field, then $deg(\overline{D}) = 1$, so Prop. 2.1.4 yields the following formula for $deg(D)$,

$$deg(D) = \frac{deg(N)deg(T)}{|\Lambda_N \cap \Lambda_T|}.$$

From [JW90, Theorem 6.3],

$$\Gamma_D = \Gamma_N + \Gamma_T.$$

Also, $|\Lambda_D| = |\Lambda_N + \Lambda_T| = |\Lambda_N| \cdot |\Lambda_T|/|\Lambda_N \cap \Lambda_T| = deg\ N \cdot (deg\ T)^2/|\Lambda_N \cap \Lambda_T| = deg\ D \cdot deg\ T$. Thus,

$$[\overline{D} : \overline{F}] = \frac{[D : F]}{[\Gamma_D : \Gamma_F]} = \frac{(deg\ D)^2}{|\Lambda_D|} = \frac{deg\ D}{deg\ T} = \frac{deg\ N}{|\Lambda_N \cap \Lambda_T|}.$$

This gives us the size of the residue. □

Remark 2.1.6. If $\overline{D}$ is a field and we also have $\Gamma_N \subseteq \Gamma_T$, then $\Lambda_N \cap \Lambda_T = \Lambda_N$, so $\overline{D} = \overline{F}$ by Corollary 2.1.5. In this case, D is tame and totally ramified with the same value group as T. If we pass to the separable closure, we see also that the canonical pairings, C_D and C_T are the same.

2.2 Symbol Algebra Algorithm

Our goal in this section is to prove that every division algebra over a GLF is isomorphic to a tensor product of cyclic algebras. In the process, we will show how to compute the underlying division algebra of an algebra presented in the form $N \otimes_F T$ where N is NSR and T is TTR. We will need the following generalization of [TW87, Theorem 4.3] which was given only for non-strictly Henselian fields.

Suppose (F, v) is a valued field, and A is a central simple F-algebra with armature $\mathcal{A}$. Let $s = exp(\mathcal{A})$ and let $\overline{v_A} : \mathcal{A} \to \frac{1}{s}\Gamma_F/\Gamma_F$ be defined by $\overline{v_A}(aF^*) = \frac{1}{s}v(a^s) + \Gamma_F$. We write $\mathcal{K}$ for the kernel of $\overline{v_A}$. We let $B_{\mathcal{A}}$ denote the armature pairing $B_{\mathcal{A}} : \mathcal{A}\times\mathcal{A} \to$

$\mu(F)$. Let $\mathcal{K}^\perp$ be the subgroup of $\mathcal{A}$ orthogonal to $\mathcal{K}$ with respect to $B_\mathcal{A}$. If $a \in A^*$ is an armature element, then we write $\widetilde{a}$ for aF^*.

Theorem 2.2.1. *Let $F, v, A, \mathcal{A}$, and $\mathcal{K}$ be as described above. Assume that $\text{char}(\overline{F}) \nmid [A:F]$. Let $s = \exp(\mathcal{A})$, so F contains a primitive s-th root of unity. Suppose that for any $a \in A^*$ with $aF^* \in \mathcal{K}$ we have $a^s \in F^{*s}$. If D is the underlying division algebra of A, then D is TTR over F, $[D:F] = |\mathcal{K}^\perp : (\mathcal{K} \cap \mathcal{K}^\perp)|$, $\Gamma_D/\Gamma_F = \overline{v_A}(\mathcal{K}^\perp) \subseteq \Delta/\Gamma_F$, and the canonical pairing on Γ_D/Γ_F is isometric (via $\overline{v_A}$) to the pairing on $\mathcal{K}^\perp/(\mathcal{K} \cap \mathcal{K}^\perp)$ induced by $B_\mathcal{A}$. In particular,*

1. *A is a division algebra if and only if $\overline{v_A}$ is injective.*

2. *If $\mathcal{K}^\perp \subseteq \mathcal{K}$, then A is split.*

Remark 2.2.2. The first part of the proof is similar to the one found in [TW87, Theorem 4.3].

Remark 2.2.3. Let $\phi_s : \mathcal{A} \to F^*/F^{*s}$ be the map defined by sending $aF^* \mapsto a^s F^{*s}$. The condition on $\mathcal{K}$ translates to the triviality of $\phi_s(\mathcal{K})$. Later, in Theorem 2.3.2, we will prove that, for ϕ_s to be trivial on $\mathcal{K}$, it is enough to check that $\phi_s(\mathcal{K}) \subseteq T$ where $T \subseteq F^*/F^{*s}$ is generated by a set of independent uniformizers.

Remark 2.2.4. The condition on $\mathcal{K}$ actually gives us more specific information which we will frequently use below. Let $a \in A$ be an element with $a^s \in F^{*s}$. Set $k = o(aF^*)$ in $\mathcal{A}$. We will show that, in fact, $a^k \in F^{*k}$. Let $a^k = x \in F^*$. By hypothesis, $a^s = y^s$ for some $y \in F^*$. Since $s = exp(\mathcal{A})$, we have $k \mid s$ and F contains an s/k-th root of unity. Since $y^s = a^s = (a^k)^{s/k} = x^{s/k}$, we get $y^k = \omega x$, where ω is some suitably chosen s/k-th root of unity. Thus, $a^k = x = (\zeta y)^k$, where $\zeta \in F^*$ is any s-th root of unity satisfying $\zeta^k = \omega^{-1}$. So $a^k \in F^{*k}$.

Proof. Let $n^2 = dim_F A = |\mathcal{A}|$. Consider first the case where $\mathcal{K}^\perp \subseteq \mathcal{K}$. Then $\mathcal{K}^\perp$ is totally isotropic and there is a maximal totally isotropic subgroup, $\mathcal{L}$, of $\mathcal{A}$ containing $\mathcal{K}^\perp$. We have $|\mathcal{L}| = n$ and $\mathcal{L} = \mathcal{L}^\perp \subseteq \mathcal{K}^{\perp\perp} = \mathcal{K}$. Set $L = F[\mathcal{L}]$, which is commutative, as $\mathcal{L}$ is totally isotropic. Since $\mathcal{L}$ is finite abelian, $\mathcal{L} = \oplus\mathcal{L}_i$, where each $\mathcal{L}_i$ is cyclic. Then $F[\mathcal{L}] = \oplus F[\mathcal{L}_i]$. Suppose l_iF^* is a generator of $\mathcal{L}_i$, and $|\mathcal{L}_i| = k_i$. Then $L = \oplus F[\mathcal{L}_i] \cong \oplus F[x_i]/(x_i^{k_i} - l_i^{k_i})$. However, $l_i \in L$, means $l_iF^* \in \mathcal{L} \subseteq \mathcal{K}$. Thus, by Remark 2.2.4, $l_i^{k_i} = f_i^{k_i}$ for some $f_i \in F^*$. Thus, $L \cong F \oplus \cdots \oplus F$ (n times). So A contains a family of n orthogonal idempotents, whence A is split. This completes the case where $\mathcal{K}^\perp \subseteq \mathcal{K}$.

Now we return to the general case. Since $\mathcal{K}^\perp \cap \mathcal{K}$ is the radical of $\mathcal{K}^\perp$, $B_\mathcal{A}$ induces a non-degenerate symplectic pairing on $\mathcal{K}^\perp/(\mathcal{K} \cap \mathcal{K}^\perp)$. Choose pre-images $s_1, t_1, \ldots, s_\ell, t_\ell \in A$ such that their images, $\overline{\widetilde{s}}_i, \overline{\widetilde{t}}_i$, in $\mathcal{K}^\perp/(\mathcal{K} \cap \mathcal{K}^\perp)$ form a symplectic base.

Let $n_i = o(\overline{\widetilde{s}}_i) = o(\overline{\widetilde{t}}_i)$ in $\mathcal{K}^\perp/(\mathcal{K} \cap \mathcal{K}^\perp)$. Then $\widetilde{s}_i^{\,n_i} \in (\mathcal{K} \cap \mathcal{K}^\perp) \subseteq \mathcal{K}$. Let $m_i = o(\widetilde{s}_i^{\,n_i})$ in $\mathcal{K}$. Again, by Remark 2.2.4, we see that $(s_i^{n_i})^{m_i} = c_i^{m_i}$ for some $c_i \in F^*$. In the same manner, let $h_i = o(\widetilde{t}_i^{\,n_i})$, whence $(t_i^{n_i})^{h_i} = d_i^{h_i}$ for some $d_i \in F^*$.

Let $E = (c_1, d_1; \omega_1)_{n_1} \otimes \cdots \otimes (c_\ell, d_\ell; \omega_\ell)_{n_\ell}$, where $\omega_i = B_\mathcal{A}(\widetilde{s}_i, \widetilde{t}_i)$. Then E has an armature, $\mathcal{E}$, generated by images mod F^* of the standard generators, i_k, j_k, of each symbol algebra. Let $B_\mathcal{E}$ denote the pairing associated to $\mathcal{E}$. We have the following commutative diagram,

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\overline{v_E}} & \Delta/\Gamma_F \\ \downarrow & & \| \\ \dfrac{\mathcal{K}^\perp}{(\mathcal{K} \cap \mathcal{K}^\perp)} & \xrightarrow{\overline{v_A}} & \Delta/\Gamma_F, \end{array}$$

where the vertical map is the isometry $\widetilde{i_k} \mapsto \overline{\widetilde{s}}_k$, $\widetilde{j_k} \mapsto \overline{\widetilde{t}}_k$. The bottom map is injective, whence, by [TW87, Prop. 3.5], E is a tame and totally ramified division algebra and v extends to a valuation on E. Also, $\Gamma_E/\Gamma_F = \overline{v_A}(\mathcal{K}^\perp)$, $[E : F] = |\mathcal{E}| = |\mathcal{K}^\perp : (\mathcal{K} \cap \mathcal{K}^\perp)|$.

We claim that E is the underlying division algebra of A. To this end, we would like to show that $A \otimes_F E^{op}$ is split. Let $\mathcal{E}'$ denote the armature of E^{op}. Then $\mathcal{A} \perp \mathcal{E}' = \{(a \otimes e)F^* \mid aF^* \in \mathcal{A},\ eF^* \in \mathcal{E}\}$ is an armature for $A \otimes_F E^{op}$. For convenience, we will denote by $(\widetilde{a}, \widetilde{e})$ the element $(a \otimes e)F^*$. Also, let $\overline{y} : \mathcal{A} \perp \mathcal{E} \to \Delta/\Gamma_F$ be the associated valuation homomorphism sending $(\widetilde{a}, \widetilde{e}) \mapsto \overline{v_A}(\widetilde{a}) + \overline{v_E}(\widetilde{e})$. Let $\mathcal{M}$ be the kernel of $\overline{y}$. By the case handled above, it suffices to show that $\mathcal{M}^\perp \subseteq \mathcal{M}$ and for any $a \otimes e \in A \otimes_F E^{op}$ with $(\widetilde{a}, \widetilde{e})F^* \in \mathcal{M}$, we have $(\widetilde{a}, \widetilde{e})^s \in F^{*s}$.

Denote by $g : \mathcal{K}^\perp \to \mathcal{E}$ the composition of surjective maps

$$\mathcal{K}^\perp \to \mathcal{K}^\perp/(\mathcal{K}^\perp \cap \mathcal{K}) \to \mathcal{E}$$

where the last map the isometry from the previous commutative diagram. So,

$$B_{\mathcal{E}}(g(\widetilde{a}), g(\widetilde{b})) = B_{\mathcal{A}}(\widetilde{a}, \widetilde{b}) \tag{2.1}$$

for any $\widetilde{a}, \widetilde{b} \in \mathcal{K}^\perp$. In addition, $\overline{v_E}(g(\widetilde{s_k})) = \overline{v_E}(\widetilde{i_k}) = \frac{1}{n_k}v(c_k) + \Gamma_F = \overline{v_A}(\widetilde{s_k})$. Similarly, $\overline{v_E}(g(\widetilde{t_k})) = \overline{v_A}(\widetilde{t_k})$. Since $g(\widetilde{s_1}), g(\widetilde{t_1}), \ldots, g(\widetilde{s_\ell}), g(\widetilde{t_\ell})$ generate $im(g)$, we have $\overline{v_E}(g(\widetilde{a})) = \overline{v_A}(\widetilde{a})$ for all $\widetilde{a} \in \mathcal{K}^\perp$.

Take any $(\widetilde{a}, \widetilde{e}) \in \mathcal{M}^\perp$. There is a $\widetilde{p} \in \mathcal{K}^\perp$ such that $g(\widetilde{p}) = \widetilde{e}$. Fix $\widetilde{r} \in \mathcal{K}^\perp$. Then $\overline{y}(\widetilde{r}, g(\widetilde{r})^{-1}) = \overline{v_A}(\widetilde{r}) + \overline{v_E}(g(\widetilde{r})^{-1}) = 0$. So $(\widetilde{r}, g(\widetilde{r})^{-1}) \in \mathcal{M}$, thus,

$$\begin{aligned} 1 &= B_{\mathcal{A}\perp\mathcal{E}'}((\widetilde{a}, \widetilde{e}), (\widetilde{r}, g(\widetilde{r})^{-1})) \\ &= B_{\mathcal{A}}(\widetilde{a}, \widetilde{r}) \cdot B_{\mathcal{E}'}(\widetilde{e}, g(\widetilde{r})^{-1}) \\ &= B_{\mathcal{A}}(\widetilde{a}, \widetilde{r}) \cdot B_{\mathcal{E}}(g(\widetilde{p}), g(\widetilde{r})) \\ &= B_{\mathcal{A}}(\widetilde{a}, \widetilde{r}) \cdot B_{\mathcal{A}}(\widetilde{p}, \widetilde{r}) \\ &= B_{\mathcal{A}}(\widetilde{ap}, \widetilde{r}). \end{aligned}$$

Since $\widetilde{r} \in \mathcal{K}^\perp$ was arbitrary, $\widetilde{ap} \in \mathcal{K}^{\perp\perp} = \mathcal{K}$. Thus,

$$0 = \overline{v_A}(\widetilde{ap}) = \overline{v_A}(\widetilde{a}) + \overline{v_A}(\widetilde{p}) = \overline{v_A}(\widetilde{a}) + \overline{v_E}(\widetilde{e}) = \overline{y}(\widetilde{a}, \widetilde{e}).$$

So $(\widetilde{a}, \widetilde{e}) \in \mathcal{M}$, whence $\mathcal{M}^\perp \subseteq \mathcal{M}$.

It remains to show that, for any $a \otimes e \in A \otimes_F E^{op}$ with $(\widetilde{a}, \widetilde{e}) \in \mathcal{M}$, we have $(a \otimes e)^s \in F^{*s}$. Note that $n_i \mid s$ for all i (see Remark 2.2.5 below), so $exp(\mathcal{E}) = exp(\mathcal{E}') \mid s$, whence $exp(\mathcal{A} \perp \mathcal{E}') = s$. Also, by Remark 2.2.5 below, $m_i \mid s/n_i$, so by the construction of the s_k, we have

$$i_k^s = (i_k^{n_k m_k})^{s/n_k m_k} = (c_k^{m_k})^{s/n_k m_k} = (s_k^{n_i m_i})^{s/n_k m_k} = s_k^s.$$

Similarly, $j_k^s = t_k^s$. Write $e = f i_1^{p_1} j_1^{q_1} \dots i_\ell^{p_\ell} j_\ell^{q_\ell}$, where $f \in F^*$ and $p_k, q_k \geq 0$. Since the map $\mathcal{K}^\perp/(\mathcal{K} \cap \mathcal{K}^\perp) \to \mathcal{E}$ given by $\overline{\widetilde{s_k}} \mapsto \widetilde{i_k}$, $\overline{\widetilde{t_k}} \mapsto \widetilde{j_k}$ is an isometry (see equation (2.1), we have, for some ω determined solely by the armature pairing $(B_\mathcal{A}, B_\mathcal{E})$

$$\begin{aligned} e^s &= f^s (i_1^{p_1} j_1^{q_1} \dots i_\ell^{p_\ell} j_\ell^{q_\ell})^s \\ &= f^s i_1^{sp_1} j_1^{sq_1} \dots i_\ell^{sp_\ell} j_\ell^{sq_\ell} \omega \\ &= f^s s_1^{sp_1} t_1^{sq_1} \dots s_\ell^{sp_\ell} t_\ell^{sq_\ell} \omega \\ &= f^s (s_1^{p_1} t_1^{q_1} \dots s_\ell^{p_\ell} t_\ell^{q_\ell})^s. \end{aligned}$$

Thus, $e^s = f^s b^s$, where $b = s_1^{p_1} t_1^{q_1} \dots s_\ell^{p_\ell} t_\ell^{q_\ell} \in A$ is an armature element with $\widetilde{b} \in \mathcal{K}^\perp$ (as $\widetilde{s_k}, \widetilde{t_k} \in \mathcal{K}^\perp$). So, $(a \otimes e)^s = a^s \cdot f^s b^s$. Also, $(\widetilde{a}, \widetilde{e}) \in \mathcal{M}$ implies that $\overline{y}((\widetilde{a}, \widetilde{e})) \in \Gamma_F$, whence $\overline{v_A}(\widetilde{ab}) = \frac{1}{s} v((ab)^s) + \Gamma_F = \frac{1}{s} v((fab)^s) + \Gamma_F = \frac{1}{s} v((ae)^s) + \Gamma_F = y((\widetilde{a}, \widetilde{e})) + \Gamma_F = \Gamma_F$. So $\widetilde{ab} \in \mathcal{K}$. By the condition on $\mathcal{K}$, $(ab)^s \in F^{*s}$. Note that

$$B_\mathcal{A}(\widetilde{b}, \widetilde{a}) = B_\mathcal{A}(\widetilde{b}, \widetilde{ab}) = 1,$$

since $\widetilde{b} \in \mathcal{K}^\perp$ and $\widetilde{ab} \in \mathcal{K}$. So a and b commute in A^*, whence $(a \otimes e)^s = a^s f^s b^s = f^s (ab)^s \in F^{*s}$. □

Remark 2.2.5. Note that E is independent of the choices of c_i and d_i. If $z_i = o(\widetilde{s_i})$ in $\mathcal{K}^\perp \subseteq \mathcal{A}$ and $n_i = o(\overline{\widetilde{s_i}})$ in $\mathcal{K}^\perp/(\mathcal{K} \cap \mathcal{K}^\perp)$, then $n_i \mid z_i \mid s$. However, $s_i^{n_i(z_i/n_i)} F^* = F^*$, so $m_i = o(\widetilde{s_i^{n_i}}) \mid z_i/n_i \mid s/n_i$. (Note that, in fact, $m_i n_i = z_i$.) Thus, $m_i n_i \mid s$, so F^* contains an $m_i n_i$-th root of unity; i.e. any m_i-th root of unity is an n_i-th power in F^*. Since the c_i are determined up to a m_i-th root of unity, the symbol algebra, $(c_i, d_i)_{n_i}$, is independent of the choice of c_i. A similar argument for d_i provides the uniqueness of E up to isomorphism.

2.3 Applying Earlier Results

Let F be a valued field. We wish to apply Theorem 2.2.1 in a special case to help compute the underlying division algebra of certain tensor products of TTR symbol algebras.

Let p be a prime and let s be any power of p. Let $t_1, \dots, t_n \in F$ be elements whose images in $\Gamma_F/p\Gamma_F$ are linearly independent. Let T be the subgroup of F^*/F^{*s} generated by $t_1, \dots, t_n$. Then,

Proposition 2.3.1. *The map $w : T \to \Gamma_F/s\Gamma_F$ induced by v is injective.*

Proof. Let w be the map induced by v sending $F^*/F^{*s} \to \Gamma_F/s\Gamma_F$. Then w is a well-defined group homomorphism. Since, $v(t_1), \dots, v(t_n)$ are linearly independent in $\Gamma_F/p\Gamma_F$, they must be linearly independent in $\Gamma_F/s\Gamma_F$. Thus, w is one-to-one. $\square$

Theorem 2.3.2. *Suppose p is odd. Let $T \subseteq F^*/F^{*s}$ be as defined preceding Prop. 2.3.1. Let $A = (a_1, b_1)_{p^{r_1}} \otimes_F \cdots \otimes_F (a_k, b_k)_{p^{r_k}}$, where $a_iF^{*s}, b_iF^{*s} \in T$ for all i and for $s = \max\{p^{r_i}\}$. Then the underlying division algebra of A is a TTR division algebra over F and can be computed via Theorem 2.2.1.*

Proof. Let B be the group of armature elements of A^* and let $K \leq B$ be the subgroup defined by $K/F^* \cong \mathcal{K}$. In order to use Theorem 2.2.1, we need to verify that for any $z \in K$ we have $z^s \in F^{*s}$. Let ϕ_s be the s-th power map. Then ϕ_s maps $B/F^* \to F^*/F^{*s}$. We claim that, because p is odd, $im(\phi_s) \subseteq T$.

Note, for any $x, y \in B$, we have $xyx^{-1}y^{-1} = \zeta \in \mu_s$. Then,

$$(xy)^s = \zeta^{1+2+\cdots+(s-1)} y^s x^s. \tag{2.2}$$

But p is odd, so s is odd and

$$1 + 2 + \cdots + (s-1) = \frac{s(s-1)}{2} \in s\mathbb{Z}. \tag{2.3}$$

Hence, $(xy)^s = x^s y^s$, i.e. ϕ_s is a group homomorphism.

Let $i_1, j_1, \dots, i_k, j_k$ be a set of standard generators for B. We assumed $a_iF^{*s}, b_iF^{*s} \in T$ for all i, so $\phi_s(i_l), \phi_s(j_l) \in T$. Since ϕ_s is a group homomorphism, this shows that $im(\phi_s) \subseteq T$.

Suppose now that $z \in K$, i.e. $v(zF^*) = \Gamma_F$. Then $v(z^sF^{*s}) = s\Gamma_F$. We have the following composition of maps

$$B/F^* \xrightarrow{\phi_s} T \xrightarrow{w} \Gamma_F/s\Gamma_F,$$

where the last map is injective by Proposition 2.3.1. By assumption $w(\phi_s(zF^*)) = v(z^sF^{*s}) \in s\Gamma_F$, so $zF^* \in ker(\phi_s)$; in other words, $z^s \in F^{*s}$, which was to be shown. □

Remark 2.3.3. Theorem 2.3.2 holds in greater generality. The key to the proof lies in showing that $\phi_s(\mathcal{K}) \subseteq T$. If $p = 2$ and for all $x, y \in K$ we have xyF^* has order less than s (in $\mathcal{K}$), or, if $p = 2$ and $\mu_{2s} \subseteq F$, then $\phi_s|_{\mathcal{K}}$ is a group homomorphism, whence $\phi_s(\mathcal{K}) \subseteq T$ and the result still holds.

Remark 2.3.4. Let $C = \langle t_1, \dots, t_k \rangle \subseteq F^*$. We want to show that, whenever Theorem 2.2.1 applies, the underlying division algebra of A is isomorphic to a tensor product of symbol algebras whose slots are in C. The slots of A can be altered by s-th powers in F^*, whence, $A = (a_1, b_1)_{p^{r_1}} \otimes_F \cdots \otimes_F (a_k, b_k)_{p^{r_k}}$ where $a_i, b_i \in C$. Since $v(t_1), \dots, v(t_k)$ are independent in $\Gamma_F/p\Gamma_F$, we have that C/p^mC maps injectively into F^*/F^{*p^m} for any $m \in \mathbb{N}$. Consequently, $C \cap F^{*p^m} = p^mC$.

Let $i_1, j_1, \dots, i_k, j_k$ be a set of standard generators for A and let

$$B = \langle i_1, j_1, \dots, i_k, j_k \rangle.$$

Then, $B \cap F^* \subseteq C$. Suppose D is the underlying division algebra of A produced by Theorem 2.2.1. Let $s_1, t_1, \dots, s_\ell, t_\ell \in B$ map to a symplectic base of $\mathcal{K}^\perp/(\mathcal{K} \cap \mathcal{K}^\perp)$. Let $p^{n_i} = o(s_iF^*) = o(t_iF^*)$ modulo $\mathcal{K} \cap \mathcal{K}^\perp$ and let $p^{m_i} = o(s_i^{p^{n_i}}F^*) = o(t_i^{p^{n_i}}F^*)$. In the proof of Theorem 2.2.1, we saw that $s_i^{p^{n_i+m_i}}, t_i^{p^{n_i+m_i}} \in F^{*p^{m_i}}$. Since $s_i, t_i \in B$ and $B \cap F^* \cap F^{*p^{m_i}} \subseteq C \cap F^{*p^{m_i}} = p^{m_i}C$, we have $s_i^{p^{n_i+m_i}}, t_i^{p^{n_i+m_i}} \in p^{m_i}C$. Thus, there exist $c_i, d_i \in C$, such that $s_i^{p^{n_i+m_i}} = c_i^{p^{m_i}}$ and $t_i^{p^{n_i+m_i}} = d_i^{p^{m_i}}$, whence $D \cong \bigotimes_{i=1}^{\ell} (c_i, d_i; F)_{p^{n_i}}$ as desired.

Remark 2.3.5. Here is an example showing that Theorem 2.3.2 does not always hold if $p = 2$. Let $A = (t_1, t_1)_2$ with $v(t_1) \notin 2\Gamma_F$ and suppose $\mu_4 \not\subseteq \overline{F}$, so $\mu_4 \not\subseteq F$. Then $A = (-1, t_1)_2$ is an NSR division algebra which is not split, hence A is not TTR. Note here that A has standard generators i, j such that $i^2 = j^2 = t_1$ and $ij = -ji$. We have that $jiF^* \in \mathcal{K}$ since $v(ji) = v(t_1) \in \Gamma_F$, however, $(ji)^2 = jiji = -j^2i^2 = -t_i^2 \notin \langle t_1F^{*2} \rangle$ as $-1 \notin F^{*2}$.

2.4 Structure of Division Algebras Over a GLF

In this section, we show that every division algebra over a GLF, F, is isomorphic to a tensor product of cyclic algebras (cf. Theorem 2.4.1). The proof allows us to compute the underlying division algebra of an algebra presented as $N \otimes_F T$ where N is NSR over F and T is TTR over F. Finally, we show that, even though every algebra is similar to $N \otimes_F T$ (cf. Cor. 2.1.2), there exist division algebras which are not isomorphic to $N \otimes_F T$ for any choice of N NSR and T TTR over F.

Theorem 2.4.1. *If F is a generalized local field, then every tame $D \in \mathcal{D}(F)$ is isomorphic to a tensor product of cyclic algebras.*

Proof. Since D is the tensor product of its primary components (cf. Prop. 1.2.1), it suffices to prove the theorem for each primary component of D.

Assume that D is p-primary. Since D is tame, $p \neq char(\overline{F})$ or D is inertially split. If D is inertially split, then $D \cong N$, where N is a cyclic NSR algebra over F (cf. 2.1.3). Thus, D is cyclic. Thus, we assume henceforward that D is not inertially split and $p \neq char(\overline{F})$.

Let $D \sim N \otimes_F T$ where N and T are NSR and TTR division algebras over F respectively. Then N, T are p-primary as well. Now we will aim to show that the underlying division algebra of $N \otimes_F T$ is isomorphic to a tensor product of cyclic algebras.

By Prop. 2.1.3, $N \cong (L/F,\ \sigma,\ c)_{p^n}$ where L/F is an unramified extension of degree p^n with $\langle\sigma\rangle = Gal(L/F)$ and $c \in F^*$ satisfies $v(c) \notin p\Gamma_F$. Since, by Prop. 2.1.1, all inertial algebras over F are split, for any valuation unit $x \in F^*$, we have $(L/F,\ \sigma,\ c)_{p^n} \sim (L/F,\ \sigma,\ c)_{p^n} \otimes_F (L/F,\ \sigma,\ x)_{p^n} \sim (L/F,\ \sigma,\ cx)_{p^n}$. By comparison of dimensions,

$$N \cong (L/F,\ \sigma,\ c)_{p^n} \cong (L/F,\ \sigma,\ cx)_{p^n}.$$

Since T is tame and totally ramified, Draxl's Theorem (Theorem 1.4.5) tells us that $T \cong \bigotimes_{k=1}^{d} (a_k, b_k)_{p^{r_k}}$, where $a_1, b_1, \ldots, a_d, b_d$ map to a $\mathbb{Z}/p\mathbb{Z}$-independent set in

$\Gamma_F/p\Gamma_F$. Thus, we can write

$$N \otimes_F T \cong (L/F,\ \sigma,\ xc)_{p^n} \otimes_F (a_1, b_1)_{p^{r_1}} \otimes_F \cdots \otimes_F (a_d, b_d)_{p^{r_d}},$$

where $x \in F^*$ is a valuation unit to be specified later. Also, for $1 \leq k \leq d$, we will let i_k and j_k denote the standard generators of the symbol algebra $(a_k, b_k)_{p^{r_k}}$. Finally, we will let $\mathcal{T}$ be the armature of T generated by $\{i_k F^*, j_k F^* \mid 1 \leq k \leq d\}$.

If Λ_N and Λ_T are disjoint, then $N \otimes_F T$ is already a division algebra via the Morandi criterion (Theorem 1.3.2) or Prop. 2.1.4, whence D is isomorphic to a tensor product of cyclic algebras. Thus, assume that $\Lambda_N \cap \Lambda_T$ is non-trivial. Since Λ_N is generated by $\frac{1}{p^n}v(c) + \Gamma_F$, we have that $\Lambda_N \cap \Lambda_T$ is generated by $\frac{1}{p^m}v(c) + \Gamma_F$, for some $m \in \mathbb{N},\ 0 < m \leq n$.

Simplifications:

Let $\tau \in T$ be an armature element with $v(\tau) = \frac{1}{p^m}v(c)$. There exist $f \in F^*$ and non-negative integers s_k, t_k such that

$$\tau = f i_1^{s_1} j_1^{t_1} \dots i_d^{s_d} j_d^{t_d}. \tag{2.4}$$

By [TW87, Prop. 3.3] (cf. Prop. 1.4.4), $\mathcal{T} \cong \Gamma_T/\Gamma_F$ via the relative valuation map, so $o(\tau F^*) = o(v(\tau) + \Gamma_F)$. Thus, τF^* has order p^m. Assume that j_1 is a leading term of τ and let $t_1 = qp^\alpha$ (cf. Section 1.4.2). Let z be any multiplicative inverse of q modulo p^{r_1}. By Prop. 1.2.3, $(L/F, \sigma, c)_{p^n} \cong (L/F, \sigma^z, c^z)_{p^n}$, so we may replace σ, c, τ with σ^z, c^z, τ^z and assume $q = 1$. Since $o(\widetilde{j_1^{t_1}}) = o(\widetilde{\tau}) = p^m$, we have

$$m \leq \alpha + m = r_1. \tag{2.5}$$

Now $\tau^{p^m} = \omega f^{p^m} i_1^{s_1 p^m} j_1^{t_1 p^m} \dots i_d^{s_d p^m} j_d^{t_d p^m}$, where $\omega \in \mu(F)$ is determined by the armature pairing on $\mathcal{T}$. For $1 \leq k \leq d$, the elements $i_k F^*, j_k F^*$ are all independent in $\mathcal{T}$; in fact, they generate separate cyclic subgroups of $\mathcal{T}$. Thus, for all k, $i_k^{s_k p^m}$ and $j_k^{t_k p^m}$ are in F^*. So,

$$\begin{aligned} \tau^{p^m} &= \omega f^{p^m} i_1^{s_1 p^m} j_1^{t_1 p^m} \dots i_d^{s_d p^m} j_d^{t_d p^m} \\ &= \omega f^{p^m} a_1^{s_1 p^{m-r_1}} b_1^{t_1 p^{m-r_1}} \dots a_d^{s_d p^{m-r_d}} b_d^{t_d p^{m-r_d}}, \end{aligned}$$

where $s_k p^{m-r_k}, t_k p^{m-r_k}$ are non-negative integers for $1 \leq k \leq d$. Since $v(\omega) = 0$,

$$v(c) = v(\tau^{p^m}) = v(f^{p^m} a_1^{s_1 p^{m-r_1}} b_1^{t_1 p^{m-r_1}} \dots a_d^{s_d p^{m-r_d}} b_d^{t_d p^{m-r_d}}),$$

whence, for some valuation unit $u \in F^*$, we obtain the equality

$$uc = f^{p^m} a_1^{s_1 p^{m-r_1}} b_1^{t_1 p^{m-r_1}} \dots a_d^{s_d p^{m-r_d}} b_d^{t_d p^{m-r_d}}. \tag{2.6}$$

We showed above that $N \cong (L/F, \sigma, uc)_{p^n}$. Thus, we may replace c by cu; since $v(c) = v(cu)$, we still have $v(\tau) = \frac{1}{p^m} v(c)$. We noted above in (2.5) that $\alpha = r_1 - m$, so $t_1 = p^\alpha = p^{r_1 - m}$. This gives us the following equations

$$c = f^{p^m} a_1^{s_1 p^{m-r_1}} b_1 a_2^{s_2 p^{m-r_2}} b_2^{t_2 p^{m-r_2}} \dots a_d^{s_d p^{m-r_d}} b_d^{t_d p^{m-r_d}}, \tag{2.7}$$

$$v(\tau) = \frac{1}{p^m} v(c) = v(f i_1^{s_1} j_1^{p^{r_1 - m}} i_2^{s_2} j_2^{t_2} \dots i_d^{s_d} j_d^{t_d}). \tag{2.8}$$

Case $r_1 \geq n$:

For this case, we may let $x = 1$, i.e., $(L/F,\ \sigma,\ xc)_{p^n} = (L/F,\ \sigma,\ c)_{p^n}$. We will argue by induction on d.

We can write

$$(L/F,\ \sigma,\ c)_{p^n} \sim (L/F,\ \sigma,\ a_1^{s_1 p^{m-r_1}} b_1)_{p^n} \otimes_F (L/F,\ \sigma,\ a_1^{-s_1 p^{m-r_1}} b_1^{-1} c)_{p^n}.$$

Then,

$$\begin{aligned} N \otimes_F T \sim\ & (L/F,\ \sigma,\ a_1^{s_1 p^{m-r_1}} b_1)_{p^n} \otimes_F (a_1, b_1)_{p^{r_1}} \\ & \otimes_F (L/F,\ \sigma,\ a_1^{-s_1 p^{m-r_1}} b_1^{-1} c)_{p^n} \otimes_F (a_2, b_2)_{p^{r_2}} \otimes_F \dots \otimes_F (a_d, b_d)_{p^{r_d}} \\ \sim\ & T_1 \otimes_F N_1 \otimes_F T_2, \end{aligned}$$

where T_1 is the underlying algebra of $(L/F,\ \sigma,\ a_1^{s_1 p^{m-r_1}} b_1)_{p^n} \otimes_F (a_1, b_1)_{p^{r_1}}$, N_1 is the underlying NSR algebra of $(L/F,\ \sigma,\ a_1^{-s_1 p^{m-r_1}} b_1^{-1} c)_{p^n}$, and $T_2 = (a_2, b_2)_{p^{r_2}} \otimes_F \dots \otimes_F (a_d, b_d)_{p^{r_d}}$. Since $r_1 \geq n$, the value group of $(L/F,\ \sigma,\ a_1^{s_1 p^{m-r_1}} b_1)_{p^n}$ is contained in value group of $(a_1, b_1)_{p^{r_1}}$. Thus, Remark 2.1.6 tells us that T_1 is a TTR division algebra, with value group generated over Γ_F by $\frac{1}{p^{r_1}} v(a_1)$ and $\frac{1}{p^{r_1}} v(b_1)$. So T_1 is in fact cyclic. Let D_1 be the underlying division algebra of $N_1 \otimes_F T_2$. From equation (2.7), $a_1^{-s_1 p^{m-r_1}} b_1^{-1} c = f^{p^m} a_2^{s_2 p^{m-r_2}} b_2^{t_2 p^{m-r_2}} \dots a_d^{s_d p^{m-r_d}} b_d^{t_d p^{m-r_d}}$, so Γ_{T_1} and $\Gamma_{D_1} = \Gamma_{N_1} + \Gamma_{T_2}$ are disjoint mod Γ_F. Thus, $D \cong T_1 \otimes_F D_1$ by Theorem 1.3.2, and it remains to show that D_1 is isomorphic to a tensor product of cyclic algebras.

If $d = 1$, then the above calculation shows that $D = T_1$, which is a cyclic algebra. For $d > 1$, note that we have reduced the problem to looking at $N_1 \otimes_F T_2$, where T_2 is a product of $d-1$ TTR symbol algebras, whence we are done by induction.

Case $r_1 < n$:

Let us tensor $N \otimes_F T$ with the split algebra $(a_1, xc)_{p^{r_1}} \otimes_F (a_1, (xc)^{-1})_{p^{r_1}}$. Thus,

$$\begin{aligned} N \otimes_F T &\sim (L/F,\ \sigma,\ xc)_{p^n} \otimes_F (a_1, xc)_{p^{r_1}} \\ &\qquad \otimes_F (a_1, (xc)^{-1})_{p^{r_1}} \otimes_F (a_1, b_1)_{p^{r_1}} \otimes_F \dots \otimes_F (a_d, b_d)_{p^{r_d}} \\ &\sim (L/F,\ \sigma,\ xc)_{p^n} \otimes_F (a_1, xc)_{p^{r_1}} \\ &\qquad \otimes_F (a_1, (xc)^{-1} b_1)_{p^{r_1}} \otimes_F (a_2, b_2)_{p^{r_2}} \dots \otimes_F (a_d, b_d)_{p^{r_d}}. \end{aligned} \tag{2.9}$$

Let C be the underlying division algebra of $(L/F,\ \sigma,\ xc)_{p^n} \otimes_F (a_1, xc)_{p^{r_1}}$. For $i = 1, 2$, define $\chi_i : G_F \to \mathbb{Q}/\mathbb{Z}$ by $\chi_1(\sigma) = 1/p^n$ and $\chi_2(\gamma) = 1/p^{r_1}$, where $\gamma(\sqrt[p^{r_1}]{a_1}) = \zeta \sqrt[p^{r_1}]{a_1}$ for $\zeta = i_1 j_1 i_1^{-1} j_1^{-1}$. Thus, $(L/F,\ \sigma,\ xc)_{p^n}$ and $(a_1, xc)_{p^{r_1}}$ correspond to the semi-symbols to (χ_1, xc) and (χ_2, xc) (cf. Section 1.5). By the bilinearity of semi-symbols, $(L/F,\ \sigma,\ xc)_{p^n} \otimes_F (a_1, xc)_{p^{r_1}}$ corresponds to the semi-symbol $(\chi_1 + \chi_2, xc)$, i.e. C is similar to a cyclic algebra of degree at most p^n.

Now let

$$B = (a_1, (xc)^{-1} b_1)_{p^{r_1}} \otimes_F (a_2, b_2)_{p^{r_2}} \dots \otimes_F (a_d, b_d)_{p^{r_d}}.$$

Then, by (2.9),

$$N \otimes_F T \sim C \otimes_F B. \tag{2.10}$$

We will use i_0, j_0 to denote the generators of the symbol algebra $(a_1, (xc)^{-1} b_1)_{p^{r_1}}$. Let $\mathcal{B}$ be the armature of B generated by $i_0 F^*, j_0 F^*, i_2 F^*, j_2 F^*, \dots, i_d F^*, j_d F^*$. Set $\mathcal{K} = \{bF^* \in \mathcal{B} |\ v(b) \in \Gamma_F\} = \ker(\overline{v_B})$, where $\overline{v_B} : \mathcal{B} \to \Gamma_B/\Gamma_F$ is the relative valuation homomorphism. Let us determine $\mathcal{K}$ and show that the hypotheses of Theorem 2.2.1 are met.

Determining $\mathcal{K}$:

Note that $v(i_0) = \frac{1}{p^{r_1}}v(a_1) = v(i_1) \in \Gamma_T$. Also, for $k \geq 2$, we already have $v(i_k), v(j_k) \in \Gamma_T$. T is TTR, so the relative valuation map on the armature of T is injective. Let $\mathcal{H}$ be the subgroup of $\mathcal{B}$ generated by $i_0F^*, i_2F^*, j_2F^*, \ldots, i_dF^*, j_dF^*$; $\overline{v_B}$ is injective on $\mathcal{H}$.

A typical element in $\mathcal{B}$ will have the form $j_0^t hF^*$, where $hF^* \in \mathcal{H}$. From the injectivity on $\mathcal{H}$, we have $\overline{v_B}(j_0^t hF^*) = 0$ if and only if $\overline{v_B}(j_0^t F^*) = -\overline{v_B}(hF^*)$. Thus, it suffices to compute $\langle \overline{v_B}(j_0F^*)\rangle \cap \overline{v_B}(\mathcal{H})$.

Recall from (2.5) that $m \leq r_1$. Also, $v(j_0) = \frac{1}{p^{r_1}}v((xc)^{-1}b_1) = \frac{1}{p^{r_1}}v(c^{-1}b_1)$ and $v(i_0) = v(i_1)$. Using equation (2.8), we obtain

$$\begin{aligned} v(j_0^{p^{r_1-m}} i_0^{s_1} i_2^{s_2} j_2^{t_2} \ldots i_d^{s_d} j_d^{t_d}) &= \frac{1}{p^m}v(b_1c^{-1}) + v(i_1^{s_1} i_2^{s_2} j_2^{t_2} \ldots i_d^{s_d} j_d^{t_d}) \\ &= v(i_1^{s_1} j_1^{p^{r_1-m}} i_2^{s_2} j_2^{t_2} \ldots i_d^{s_d} j_d^{t_d}) - \frac{1}{p^m}v(c) \qquad (2.11) \\ &= -v(f) \quad \in \quad \Gamma_F. \end{aligned}$$

Thus, $\overline{v_B}(j_0^{p^{r_1-m}}F^*) \in \overline{v_B}(\mathcal{H})$. Let $\ell \geq 0$ be the smallest non-negative integer such that $\overline{v_B}(j_0^{p^\ell}F^*)$ generates $\langle \overline{v_B}(j_0F^*)\rangle \cap \overline{v_B}(\mathcal{H})$. So, $\ell \leq r_1 - m$. Note that

$$v(j_0^{p^\ell}) = \frac{p^\ell}{p^{r_1}}v(c^{-1}b_1) = -\frac{p^\ell}{p^{r_1}}v(c) + p^\ell v(j_1).$$

We saw above that $\overline{v_B}(\mathcal{H}) \subseteq \Gamma_T/\Gamma_F$. By assumption, $\overline{v_B}(j_0^{p^\ell}F^*) \in \overline{v_B}(\mathcal{H})$, so $v(j_0^{p^\ell}) \in \Gamma_T$. Also, $v(j_1) \in \Gamma_T$, whence $\frac{p^\ell}{p^{r_1}}v(c) \in \Gamma_T$. But we assumed that $\frac{1}{p^m}v(c) + \Gamma_F$ generates the cyclic subgroup of $\frac{1}{p^n}v(c) + \Gamma_F$ contained in Γ_T. Thus, $\frac{1}{p^m} \mid \frac{p^\ell}{p^{r_1}}$, whence $p^{r_1-m} \mid p^\ell$, so $r_1 - m \leq \ell$. So $\ell = r_1 - m$.

Therefore, we conclude that $\mathcal{K} = \langle \kappa F^*\rangle$, where $\kappa = j_0^{p^{r_1-m}} i_0^{s_1} i_2^{s_2} j_2^{t_2} \ldots i_d^{s_d} j_d^{t_d}$. Since j_1 is a leading term of τ and $o(\tau F^*) = p^m$, we must have $i_2^{s_2}F^*, j_2^{t_2}F^*, \ldots, i_d^{s_d}F^*, j_d^{t_d}F^*$ all have order less than or equal to p^m. Also, $o(i_0^{s_1}) = o(i_1^{s_1}) \leq p^m$. Since $o(j_0^{p^{r_1-m}}) = p^m$, we have $|\mathcal{K}| = p^m$.

Using Theorem 2.2.1:

Since commutators of i_k, j_k are roots of unity in F^*, we have

$$\kappa^{p^m} = \left(i_0^{s_1} j_0^{p^{r_1-m}} i_2^{s_2} j_2^{t_2} \cdots i_d^{s_d} j_d^{t_d}\right)^{p^m} = \omega' i_0^{s_1 p^m} j_0^{p^{r_1}} i_2^{s_2 p^m} j_2^{t_2 p^m} \cdots i_d^{s_d p^m} j_d^{t_d p^m},$$

where $\omega' \in F^*$ is some root of unity. With the help of equation (2.7), we obtain

$$\begin{aligned}\omega' i_0^{s_1 p^m} j_0^{p^{r_1}} i_2^{s_2 p^m} j_2^{t_2 p^m} \ldots i_d^{s_d p^m} j_d^{t_d p^m} & \\ = \omega' a_1^{s_1 p^{m-r_1}} b_1 (xc)^{-1} a_2^{s_2 p^{m-r_2}} b_2^{t_2 p^{m-r_2}} \ldots a_d^{s_d p^{m-r_d}} b_d^{t_d p^{m-r_d}} & \\ = \omega' x^{-1} f^{-p^m}. & \quad (2.12)\end{aligned}$$

Now, we choose $x = \omega'$, so $\kappa^{p^m} = f^{-p^m} \in F^{*p^m}$ Since $p^m \mid p^{r_1} \mid exp(B)$, the hypotheses of Theorem 2.2.1 are fulfilled.

Thus, Theorem 2.2.1 shows that the underlying division algebra, D_1, of B is TTR, whence isomorphic to a tensor product of cyclic algebras. Since $\mathcal{K}$ is cyclic, $\mathcal{K} \cap \mathcal{K}^\perp = \mathcal{K}$, we have $|\mathcal{K}| \cdot |\mathcal{K} \cap \mathcal{K}^\perp| = |\mathcal{K}|^2 = p^{2m}$. Thus, by Theorem 2.2.1,

$$[D_1 : F] = \frac{|\mathcal{K}^\perp|}{|\mathcal{K} \cap \mathcal{K}^\perp|} = \frac{[B : F]}{|\mathcal{K}||\mathcal{K} \cap \mathcal{K}^\perp|} = \frac{[B : F]}{p^{2m}}.$$

Let $A = D_1 \otimes_F C$, so $A \sim N \otimes_F T$ via (2.10) and A is isomorphic to a tensor product of cyclic algebras. Since $deg(C) \leq p^n = deg(N)$ and $deg(B) = deg(T)$, we have

$$\begin{aligned} ind(N \otimes_F T) &= ind(A) \leq deg(A) \\ &= deg(D_1) deg(C) = \frac{deg(B)}{p^m} deg(C) \leq \frac{deg(T) deg(N)}{p^m}. \end{aligned}$$

Yet, $|\Lambda_N \cap \Lambda_T| = p^m$, so Corollary 2.1.5 tells us that $ind(N \otimes_F T) = deg(N) deg(T)/p^m$. Thus, $deg(A) = deg(N) deg(T)/p^m$ and A is the underlying division algebra of $N \otimes_F T$. □

Remark 2.4.2. In the proof of Theorem 2.4.1, we showed that the underlying division algebra, D, of $N \otimes_F T$ is a tensor product of cyclic algebras by explicitly producing D. This gives us the following corollary:

Corollary 2.4.3. *Let F be a GLF. Let N be an NSR division algebra over F and let T be a TTR division algebra over F. Then we can compute D, the underlying division algebra of $N \otimes_F T$ using the method given in the proof of Theorem 2.4.1.*

Remark 2.4.4. Note that [JW90, Theorem 6.3] and the remarks following Prop. 2.1.4 allow us to compute the degree, value group and residue field of D independent of the theorem. In fact, $deg(D) = p^{n-m}deg(T)$, $\Gamma_D = \Gamma_N + \Gamma_T$, and $[\overline{D} : \overline{F}] = p^{n-m}$.

Remark 2.4.5. Note that Theorem 2.4.1 shows that, for $D \in \mathcal{D}(F)$ tame and F GLF, $D \cong C \otimes_F T$ where C is a cyclic algebra and T is TTR. Suppose F is a GLF with $dim_{\mathbb{Z}_p}\Gamma_F/p\Gamma_F \geq 2$. This holds, for example, if $\Gamma_F \cong \mathbb{Z}^n$ for $n \geq 2$. We can use value group and degree information to construct a division algebra D over F such that $D \ncong N \otimes_F T$ for any choice of N NSR and T TTR over F. Let $a, b \in F$ be elements whose images have independent values in $\Gamma_F/p\Gamma_F$. Let L be the unramified extension of F of degree p^2 and let σ be a generator for $Gal(L/F)$. Now let D be the underlying division algebra of $N \otimes_F T$ where $N = (L/F, \sigma, b)_{p^2}$ and $T = (a, b)_p$. Then $\Gamma_N \cap \Gamma_T = \langle \frac{1}{p}v(b)\rangle + \Gamma_F$, so by Remark 2.4.4, $deg(D) = p^2$, $[\overline{D} : \overline{F}] = p$, and

$$\Gamma_D = \Gamma_N + \Gamma_T = \langle (1/p)v(a), (1/p^2)v(b)\rangle + \Gamma_F,$$

which has exponent p^2 mod Γ_F. Suppose

$$D \cong N' \otimes_F T', \tag{2.13}$$

where N' is NSR over F and T' is TTR over F. Since $[\overline{D} : \overline{F}] \neq deg(D)$, we have D is not an NSR division algebra over F. Similarly, $[\overline{D} : \overline{F}] \neq 1$, so D is not TTR over F. Thus, N' and T' in (2.13) are both non-split. Since $deg(D) = p^2$, we must have $deg(N) = p = deg(T)$. So $exp(\Lambda_N), exp(\Lambda_T) \mid p$, whence $exp(\Lambda_D) \mid p$ as $\Gamma_D = \Gamma_N + \Gamma_T$. But $exp(\Lambda_D) = p^2$, which is a contradiction. Thus, D is not isomorphic to $N' \otimes_F T'$ for any choice of N' NSR and T TTR over F. Note that this D is a cyclic algebra.

Chapter 3

Restriction

In this chapter, we describe an algorithm for computing the restriction of a (tame) division algebra over a GLF. A classification of subfields of TTR algebras was given by Tignol and Wadsworth in [TW87, Th. 3.8]. Over a strictly Henselian field, i.e. F Henselian with $\overline{F}$ separably closed, every tame division algebra is TTR, so [TW87, Th. 3.8] essentially gives a classification for subfields of all tame division algebras over strictly Henselian fields. In the GLF situation, not every division algebra is TTR, but will be a product of a TTR algebra with an NSR algebra. Thus, the situation is more complicated.

The starting point is a description of our algebras in the form $N \otimes_F T$ where N is NSR and T is TTR over F (cf. Cor. 2.1.2). Let $K \supseteq F$ be a finite degree field extension and take $D \in \mathcal{D}(F)$. Then K is isomorphic to a subfield of D if and only if D_K has degree $deg(D)/[K : F]$ (cf. Prop. 1.2.2). Thus, we may detect subfields of D by computing $deg(D_K)$.

Let $K \supseteq F$ be a finite-degree extension of GLF's. If $K \supseteq F$ is a tame, then we may realize K as an unramified extension of F followed by a tame and totally ramified extension. The unramified case is handled in Theorem 3.3.1. If $K \supseteq F$ is TTR, then by [Sch50, p. 64, Theorem 3], K is totally ramified of radical type (TRRT) (cf. Section 1.3). This case is handled in Theorem 3.3.3. If K is not a tame extension of F (so $char(\overline{F}) \mid [K:F]$), then the formula given in Lemma 3.1.1 computes $ind(D_K)$ (see Section 3.2).

The chapter is organized as follows. First, in Section 3.1, we prove a lemma on inertially split algebras using the character theory developed in [JW90, §5]. Then, in Section 3.2 we define several constants for an algebra presented as $N \otimes_F T$ where N is NSR and T is TTR over F. Finally, in Section 3.3, we give formulas for computing D_K where $D \in \mathcal{D}(F)$ is tame and $K \supseteq F$ is any finite-degree extension.

3.1 A Sum Formula

We begin this chapter by proving a lemma which utilizes the character theory developed for inertially split algebras by Jacob and Wadsworth (cf. [JW90, §5]).

Let (F, v) be a Henselian valued field and suppose $N_1, \ldots, N_k$ are (tame) algebras over F with $N_i \cong (L_i/F, \sigma_i, c_i)_{n_i}$, where L_i is unramified over F, i.e. N_i are inertially split algebras. Suppose further that there exists a finite degree cyclic field extension $L \supseteq F$ with $L_i \subseteq L$ for $1 \leq i \leq k$. Let σ be a generator for $Gal(L/F)$ and set $n = [L:F]$.

Lemma 3.1.1. *Let F, L, N_1, ..., N_k be as described above. If D is the underlying division algebra of $N_1 \otimes_F \ldots \otimes_F N_k$, then D is similar to a cyclic algebra and Γ_D is generated over Γ_F by*

$$\frac{\ell_1}{n_1} v(c_1) + \cdots + \frac{\ell_k}{n_k} v(c_k),$$

where, for $1 \leq i \leq k$, the ℓ_i satisfy $\sigma_i^{\ell_i} = \sigma\big|_{L_i}$.

Proof. Since σ is a generator for $Gal(L/F)$, we have $\sigma_i^{\ell_i} = \sigma\big|_{L_i}$ is a generator for $Gal(L_i/F)$. Thus, ℓ_i is prime to n_i. Thus, using the cyclic algebra identities in Prop. 1.2.3 $N_i \cong (L_i/F, \sigma_i, c_i)_{n_i} \cong (L_i/F, \sigma_i^{\ell_i}, c_i^{\ell_i})_{n_i} \sim (L/F, \sigma, c_i^{\ell_i n/n_i})_n$. Thus,

$$D \ \sim \ N_1 \otimes_F \ldots \otimes_F N_k \ \sim \ (L/F, \sigma, \prod_{i=1}^{k} c_i^{\ell_i n/n_i})_n.$$

Now, let $\gamma : H^2(G_{\overline{F}}, F^*_{nr}) \to Hom_c(G_{\overline{F}}, \Delta/\Gamma_F)$ be the map described in [JW90, §5]. Let $\overline{\sigma}$ be the image of σ in $Gal(\overline{L}/\overline{F})$. Set $h = \gamma([D])$. It was shown in [JW90, §5] that $im(h) = \Gamma_D/\Gamma_F$, so Γ_D is generated over Γ_F by $h(\overline{\sigma}) = \frac{1}{n} v\big(\prod_{i=1}^{k} c_i^{\ell_i n/n_i}\big) = \sum_{i=1}^{k} \frac{\ell_i}{n_i} v(c_i)$. □

Remark 3.1.2. The hypothesis about the existence of L is always fulfilled if F is a generalized local field and $N_1, \dots, N_k$ are inertially split. In this case, we may take L to be the unique unramified field extension of F of degree $lcm(n_1, \dots, n_k)$; cf. Prop. 2.1.3. In addition, $\overline{F}$ is finite and D is inertially split, so D is actually NSR.

Remark 3.1.3. Using the same notation as in Lemma 3.1.1, we have $\ell_i \in \overline{comp}(\sigma_i, \sigma)$ (cf. Section 1.7). If σ_1 extends to a generator, $\overline{\sigma_1}$, of $Gal(L/F)$, then we can choose $\ell_1 = 1$ by setting $\sigma = \overline{\sigma_1}$. In this case, $\ell_i \in \overline{comp}(\sigma_i, \sigma_1)$ for $i > 1$.

3.2 Notation

The following notation will be valid for the rest of this chapter.

Let F be a generalized local field and let $D \in \mathcal{D}(F)$ be tame division algebra. By primary decomposition (cf. Prop. 1.2.1), $D \cong D_1 \otimes_F \dots \otimes_F D_k$, where D_i is p_i-primary. Recall that, for K a field containing F, we write D_K for the underlying division algebra of $D \otimes_F K$. Then $D_K \cong (D_1)_K \otimes_F \dots \otimes_F (D_k)_K$, so we may reduce to the case that D is p-primary. By Cor. 2.1.2, $D \sim N \otimes_F T$, where N is NSR and T is TTR and both N and T are p-primary for some prime p. Since D is tame, D is inertially split or $p \neq char(\overline{F})$. If $p = char(\overline{F})$, then $D \cong N$ and the scalar extensions of D are easily understood (e.g. by using Prop. 1.2.5 and Lemma 3.1.1 with $k = 1$). Therefore, for the rest of the chapter, we will focus on the more interesting case: we will assume throughout that $p \neq char(\overline{F})$.

For some $c \in F$ with $v(c) \notin p\Gamma_F$,

$$N \cong (L/F, \sigma, c)_{p^n},$$

where L/F is the unramified extension of F of degree p^n. Also,

$$T \cong (a_1, b_1)_{p^{r_1}} \otimes_F \ldots \otimes_F (a_d, b_d)_{p^{r_d}},$$

where $a_1, b_1, \ldots, a_d, b_d$ map to independent elements in $\Gamma_F/p\Gamma_F$ and $\mu_{p^{r_i}} \subseteq F$. Let $p^r = exp(T) = lcm\{p^{r_1}, \ldots, p^{r_d}\}$ and let ω be a primitive p^r root of unity in F. For $1 \leq k \leq d$, we let i_k, j_k be standard generators of $(a_k, b_k)_{p^{r_k}}$, i.e.

$$i_k^{p^{r_k}} = a_k, \; j_k^{p^{r_k}} = b_k, \; i_k j_k = \omega^{p^{r-r_k}} j_k i_k.$$

Also, let $\mathcal{T}$ denote the armature of T generated by $i_1F^*, j_1F^*, \ldots, i_dF^*, j_dF^*$. We let $\langle -, - \rangle$ denote the armature pairing $\langle -, - \rangle : \mathcal{T} \times \mathcal{T} \to \mu_{p^r}$ given by $\langle \theta F^*, \tau F^* \rangle = \theta\tau\theta^{-1}\tau^{-1}$. We will identify μ_{p^r} with $\frac{1}{p^r}\mathbb{Z}/\mathbb{Z}$ by identifying ω with $\frac{1}{p^r} + \mathbb{Z}$.

Finally, let $\Gamma_N \cap \Gamma_T = \langle \frac{1}{p^m} v(c) \rangle + \Gamma_F$, where $n \geq m \geq 0$. Thus, by Proposition 2.1.4,

$$ind\ D = \frac{1}{p^m}(ind\ N)(ind\ T).$$

3.3 Restriction Calculations

We maintain the notation and hypotheses set up in the previous section. So F is a generalized local field and $p \neq char(\overline{F})$.

Proposition 3.3.1. *Suppose $K \supseteq F$ is the unramified field extension with $[K : F] = p^k$. Then $ind\ D = p^{\ell_0} \cdot ind\ D_K$, where $\ell_0 = \min\{n - m,\ k\}$. Also, $\Gamma_{D_K} = [K : F]\Gamma_N + \Gamma_T$ and $[\overline{D_K} : \overline{K}] = p^{n-m-\ell_0}$.*

Proof. Because T is TTR, we have that T_K is also TTR and has the same degree and value group as T.

Suppose $k < n - m$. Then $K \subseteq L \subseteq N$ by the uniqueness of unramified field extensions over a generalized local field. So $N_K = C_N(K) \cong (L/K, \sigma^{p^k}, c)_{p^{n-k}}$ (cf.

Prop. 1.2.5). Also, $n-k>m$, so $\frac{1}{p^m}v(c)\in\Gamma_{N_K}$, thus, $\Gamma_{N_K}\cap\Gamma_{T_K}=\langle\frac{1}{p^m}v(c)\rangle+\Gamma_F$, since $(\langle\frac{1}{p^n}v(c)\rangle+\Gamma_F)\cap\Gamma_T=\langle\frac{1}{p^m}v(c)\rangle+\Gamma_F$. So, by Prop. 2.1.4

$$ind\ D_K=\frac{ind\ N_K\cdot ind\ T_K}{p^m}=\frac{ind\ N\cdot ind\ T}{p^{m+k}}=\frac{ind\ D}{p^k}.$$

Now suppose instead that $k\geq n-m$. Either N_K is split or $N_K\cong(L/K,\sigma^{p^k},c)_{p^{n-k}}$ as before. However, $n-k\leq m$, so, in either case, $\Gamma_{N_K}\subseteq\langle\frac{1}{p^m}v(c)\rangle+\Gamma_F\subseteq\Gamma_{T_K}$, thus, by Remark 2.1.6, $D_K\sim N_K\otimes_F T_K$ is TTR with the same value group and index as T_K. Therefore,

$$ind\ D_K=ind\ T_K=ind\ T=\frac{ind\ D}{p^{n-m}}.$$

Since $\Gamma_{N_K}=[K:F]\Gamma_N$ and $\Gamma_{T_K}=\Gamma_T$, we have $\Gamma_{D_K}=\Gamma_{N_K}+\Gamma_{T_K}=[K:F]\Gamma_N+\Gamma_T$. Finally, $[\overline{D_K}:\overline{K}]=ind(N_K)/|(\Gamma_{N_K}\cap\Gamma_{T_K}):\Gamma_F|=p^n/p^{m-\ell_0}=p^{n-m-\ell_0}$. □

Remark 3.3.2. If I is a field unramified over F with $[I:F]$ prime to p, then L and I are linearly disjoint over F. Then, by Prop. 1.2.5, $N_I=(LI/I,\overline{\sigma},c)_{p^n}$, where $\overline{\sigma}$ is an extension of σ to LI; note that N_I has the same value group and residue degree as N. Similarly, T_I is TTR and has the same degree and value group as T. Thus, $D_I=N_I\otimes_F T_I$ has the same degree, value group, and residue degree as D.

Proposition 3.3.1 and Remark 3.3.2 allows us to obtain index, value group, and residue information after extending scalars to an arbitrary finite-degree unramified field extension of F. For, if K/F is unramified, then K/F is cyclic Galois (by Prop. 2.1.3), whence there exists a field I such that $[I:F]$ is prime to p and $[K:I]$ is a power of p. Recall that every tame finite-degree extension of Henselian fields can be realized as an unramified extension followed by a totally ramified extension. We now turn to the totally ramified case.

Suppose $K\supseteq F$ is a totally ramified extension with $\Gamma_K\subseteq\Gamma_N\cap\Gamma_T=\langle\frac{1}{p^n}v(c)\rangle+\Gamma_T$. Then $|\Gamma_K:\Gamma_F|=[K:F]$ is a power of p, so $char(\overline{F})\nmid[K:F]$ and $K\supseteq F$ is tame. By [Sch50, p. 64, Theorem 3], every TTR field extension is a totally ramified extension of radical type (TRRT) (cf. Section 1.3). The rest of this section will be devoted to giving an index formula for the case where K is a cyclic TRRT extension of F.

Combined with Prop. 3.3.1, this provides a way of computing D_K for an arbitrary field K tame over F by breaking the extension from K to F into a succession of unramified or cyclic TRRT extensions.

Set $K = F(\sqrt[p^k]{\pi})$, where $\pi \in F$ and $v(\pi) \notin p\Gamma_F$. Since $\frac{1}{p^k}v(\pi) \in \langle \frac{1}{p^n}v(c)\rangle + \Gamma_T$, there exist non-negative integers α and β such that $\alpha \leq n,\ \ \beta \leq r$, and g with $0 < g < p$, we have

$$\frac{1}{p^k}v(\pi) = \frac{g}{p^\alpha}v(c) + \frac{1}{p^\beta}v(t), \tag{3.1}$$

where $t \in F$ satisfies $\frac{1}{p^\beta}v(t) \in \Gamma_T$ and $v(t) \notin p\Gamma_F$. This decomposition is not unique; in fact, we may alter the last two terms by elements from $\Gamma_N \cap \Gamma_T$. If $\alpha \leq m$, then $\frac{1}{p^\alpha}v(c) \in \Gamma_T$, whence $\frac{1}{p^k}v(\pi) \in \Gamma_T$, so $\Gamma_K \subseteq \Gamma_T$. In this case, we may eliminate the term involving α in (3.1). However, if $\alpha > m$, then α is unique in expression (3.1), even though g, β, and t are not. For, suppose we had two decompositions of $\frac{1}{p^k}v(\pi)$,

$$\frac{g}{p^\alpha}v(c) + \frac{1}{p^\beta}v(t) = \frac{g'}{p^{\alpha'}}v(c) + \frac{1}{p^{\beta'}}v(t').$$

Since $\frac{1}{p^\beta}v(t)$ and $\frac{1}{p^{\beta'}}v(t')$ are in Γ_T, we must have $\frac{g}{p^\alpha}v(c) - \frac{g'}{p^{\alpha'}}v(c) \in \Gamma_T$. Also, we assumed in (3.1) that $\alpha, \alpha' \leq n$, so $\frac{g}{p^\alpha}v(c) - \frac{g'}{p^{\alpha'}}v(c) \in \Gamma_N \cap \Gamma_T = \langle \frac{1}{p^m}v(c)\rangle + \Gamma_F$. Thus, $\max\{\alpha, \alpha'\} \leq m$ or $\alpha = \alpha'$; i.e. $\alpha = \alpha'$.

We know from [TW87, Th. 3.8] that subalgebras of TTR algebras are classified up to isomorphism by their value group. Let $E \supseteq F$ be the subfield of K satisfying $\Gamma_E = \Gamma_K \cap \Gamma_T$. Say $E = F(\sqrt[p^e]{\pi})$, where $0 \leq e \leq k$. Write $\pi = x\pi_0$, where $x \in U_F$ and $F(\sqrt[p^e]{\pi_0}) \subseteq T$. Here, π_0 is determined up to p^e powers in F^* by the classification of subalgebras of T, thus, so is x. Let $\tau \in T$ be an armature element such that

$$\tau^{p^e} = \pi_0.$$

As discussed in Section 1.4.2, τ always has a leading term; say i_1. Suppose that i_1 appears with exponent $s_1 = qp^s$ in (1.1) from Section 1.4.2, where q is prime to p. Let z be any multiplicative inverse of q modulo p^{r_1}. Now replace π, x, π_0, τ, g, and t with π^z, x^z, π_0^z, τ^z, zg, and t^z. Since z is prime to p, we still have $K = F(\sqrt[p^k]{\pi})$,

$\pi = x\pi_0$, $\tau^{p^e} = \pi_0$. However, the factor of i_1 appearing in (1.1) now becomes p^s. Let γ be the largest integer such that $x \in U_F^{p^\gamma}$ and $\gamma \le r_1$; so $x = x_0^{p^\gamma}$ for some $x_0 \in F^*$ and $p^\gamma \mid exp(T) = p^r$. Referring to the decomposition of $v(\pi)$ in (3.1), let $\theta, \rho \in T$ be armature elements such that

$$v(\theta) = \frac{1}{p^m} v(c) \text{ and } v(\rho) = \frac{1}{p^\beta} v(t). \tag{3.2}$$

Note that $p^e = o(i_1^{p^s} F^*) = p^{r_1 - s}$, which gives us the following inequalities

$$0 \le e = r_1 - s \le r_1 \le r. \tag{3.3}$$

Also,

$$\begin{aligned} p^{k-e} = |\Gamma_K : (\Gamma_K \cap \Gamma_T)| &= |(\Gamma_K + \Gamma_T) : \Gamma_T| \\ &\le |(\Gamma_N + \Gamma_T) : \Gamma_T| = |\Gamma_N : (\Gamma_N \cap \Gamma_T)| = p^{n-m}. \end{aligned} \tag{3.4}$$

Let $M = F(\sqrt[p^{r_1}]{x})$; this is an unramified Kummer extension of F of degree $p^{r_1 - \gamma}$. Also, let $\sigma_\omega \in Gal(M/F)$ be defined by $\sigma_\omega(\sqrt[p^{r_1}]{x}) = \omega^{p^\gamma}(\sqrt[p^{r_1}]{x})$. Recall that $\sigma \in Gal(L/F)$ and $N \cong (L/F, \sigma, c)_{p^n}$.

Theorem 3.3.3. *Suppose K is a cyclic TTR field extension of F with $\Gamma_K \subseteq \Gamma_D$. Let k, n, m, γ, θ, and ρ be defined as above and let $\langle -, - \rangle$ denote the armature pairing on $\mathcal{T}$. Then,*

$$ind\ D_K = \frac{\ell}{p^k} \cdot ind\ D,$$

where

$$\ell = \operatorname{ord}_{\mathbb{Q}/\mathbb{Z}}\left(\langle \widetilde{\theta}, \widetilde{\rho} \rangle + \lambda p^{n-m+\gamma-k} \right), \tag{3.5}$$

and $\lambda \in \overline{\text{comp}}(\sigma_\omega, \sigma)$ is prime to p. Moreover, if $K_0 \subseteq K$ is the largest subfield of K lying in D, then K_0 is determined by $[K_0 : F] = p^k/\ell$.

Theorem 3.3.3 is proved after Corollary 3.3.8 below.

Remark 3.3.4. For any decomposition into (3.1), $\alpha \le m$ if and only if $\Gamma_K \subseteq \Gamma_T$. For, clearly, if $\alpha \le m$, then $\Gamma_K \subseteq \Gamma_T$. We assumed that $n \ge \alpha$, so if $\alpha > m$, then $\frac{1}{p^\alpha} v(c) \in \Gamma_N \backslash \Gamma_T$, whence $\Gamma_K \nsubseteq \Gamma_T$.

Remark 3.3.5. We want to explain how (3.5) is well-defined and independent of our (cumbersome) notational setup. We know $n = deg(N)$, $m = |(\Gamma_N \cap \Gamma_T) : \Gamma_F|$, and $k = [K : F]$ are uniquely defined. The constant γ depends uniquely on the choice of x. However, x is determined from T up to p^e-th powers in F^*, and our convention when $x \in U_F^{p^i}$ for all i is to set $p^\gamma = p^{r_1}$. Thus, if $\gamma \geq e$, then γ is not well-defined, since we may alter x by a p^e-th power in F^* and perhaps force $\gamma = e$. However, whenever $\gamma \geq e$, the $\lambda p^{n-m+\gamma-k}$ term in (3.5) drops out, whence (3.5) is independent of the choice of x and γ. For, by (3.4), $k - e \leq n - m$. If $\gamma \geq e$, then $n - m \geq k - \gamma$, whence $n - m + \gamma - k \geq 0$, so $\lambda p^{n-m+\gamma-k} \in \mathbb{Z}$ and (3.5) is independent of the choice of x and γ. Note that $\gamma \geq e$ if and only if $E \subseteq T$. So (3.5) reduces to $\ell = ord_{\mathbb{Q}/\mathbb{Z}}\left(\langle \widetilde{\theta}, \widetilde{\rho} \rangle\right)$ when $\gamma \geq e$. Thus, we obtain the following corollary to Theorem 3.3.3.

Corollary 3.3.6. *If $n - m \geq k - \gamma$, then $ind(D_K) = \frac{\ell}{p^k} ind(D)$ where $\ell = ord_{\mathbb{Q}/\mathbb{Z}}(\langle \widetilde{\theta}, \widetilde{\rho} \rangle)$. This occurs if $E \subseteq T$ (which is equivalent to $\gamma \geq e$).*

Now we will show that (3.5) is independent of the choice of $\lambda \in \overline{comp}(\sigma_\omega, \sigma)$. Since (3.5) depends on λ only if $ord_{\mathbb{Q}/\mathbb{Z}}(\langle \widetilde{\theta}, \widetilde{\rho} \rangle) = ord_{\mathbb{Q}/\mathbb{Z}}(p^{n-m+\gamma-k})$, we may assume that $ord_{\mathbb{Q}/\mathbb{Z}}(\langle \widetilde{\theta}, \widetilde{\rho} \rangle) = ord_{\mathbb{Q}/\mathbb{Z}}(p^{n-m+\gamma-k}) = p^b$ for some b. Note that $b = \max\{-(n - m + \gamma - k), 0\}$. Also, since $\widetilde{\theta}$ has order p^m, we must have $b \leq m$. So, $n - m + \gamma - k \geq -m$, i.e. $n + \gamma - k \geq 0$.

Recall $\langle \sigma \rangle = Gal(L/F) \cong G_F/G_L$ and $\langle \sigma_\omega \rangle = Gal(M/F) \cong G_F/G_M$. Since F is a GLF and L, M are unramified over F of p-power degree, either $L \subseteq M$ or $M \subseteq L$. Thus, $G_F/G_LG_M \cong Gal((L \cap M)/F)$ and $|G_F : G_LG_M| = p^a$ where $a = \min\{n, r_1 - \gamma\}$. By Remark 1.7.2, we have $\overline{comp}(\sigma_o m, \sigma)$ is a coset of $p^a\mathbb{Z}$, thus λ is determined up to $p^a\mathbb{Z}$. Recall from (3.3) that $r_1 \geq e$, so

$$\begin{aligned} a + (n - m + \gamma - k) &= \min\{n + n - m + \gamma - k, n - m + r_1 - k\} \\ &= \min\{(n + \gamma - k) + (n - m), (n - m + e - k) + (r_1 - e)\} \geq 0, \end{aligned}$$

as all the terms in the parentheses are non-negative. Thus, $p^a p^{n-m+\gamma-k} \in \mathbb{Z}$ and the different choices for λ change $\langle \widetilde{\theta}, \widetilde{\rho} \rangle) - \lambda p^{n-m+\gamma-k}$ by an integer, whence (3.5) is independent of the choice of λ.

Finally, we will show that (3.5) is well-defined with respect to ρ. Recall $v(\rho) = \frac{1}{p^\beta}v(t)$. Suppose we have two decompositions as in (3.1)

$$\frac{g_2}{p^{\alpha_2}}v(c) + \frac{1}{p^{\beta_2}}v(t_2) = \frac{g_1}{p^{\alpha_1}}v(c) + \frac{1}{p^{\beta_1}}v(t_1).$$

Let ρ_2 and ρ_1 be armature elements of T such that $v(\rho_i) = \frac{1}{p^{\beta_i}}v(t_i)$. Then

$$v(\rho_1\rho_2^{-1}) = \left(\frac{g_1}{p^{\alpha_1}} - \frac{g_2}{p^{\alpha_2}}\right)v(c) \in \Gamma_N \cap \Gamma_T = \langle v(\theta)\rangle + \Gamma_F.$$

Thus, $1 = \langle\widetilde{\theta}, \widetilde{\rho_1\rho_2^{-1}}\rangle$, so $\langle\widetilde{\theta}, \widetilde{\rho_1}\rangle = \langle\widetilde{\theta}, \widetilde{\rho_2}\rangle$, whence (3.5) is independent of the choice of ρ.

Remark 3.3.7. There are some cases where (3.5) simplifies. We observed above in Corollary 3.3.6 that $\lambda p^{n-m+\gamma-k} \in \mathbb{Z}$ if $E \subseteq T$. In this case, we get full index reduction (i.e. $K \subseteq D$) only if $\langle\widetilde{\theta}, \widetilde{\rho}\rangle = 1$.

Now set $H = F(\theta)$, so $H \subseteq T$ and $T_H = C_T(H)$. Then, Γ_{T_H} is generated by values of armature elements of T whose images in $\mathcal{T}$ are orthogonal to $\widetilde{\theta}$. So $\langle\widetilde{\theta}, \widetilde{\rho}\rangle = 1$ if and only if $v(\rho) \in \Gamma_{T_H}$. By (3.1), Γ_K is generated by $\frac{1}{p^k}v(\pi) = \frac{g}{p^\alpha}v(c) + \frac{1}{p^\beta}v(t) = \frac{g}{p^{\alpha-m}}v(\theta) + v(\rho)$, so $v(\rho) \in \Gamma_{T_H}$ if and only if $\Gamma_K \subseteq \Gamma_N + \Gamma_{T_H}$. This yields the following corollary to Theorem 3.3.3

Corollary 3.3.8. *Say* $\Gamma_K \subseteq \Gamma_N + \Gamma_{T_H}$ *where* $H = F(\theta)$. *Let* $\ell = ord_{\mathbb{Q}/\mathbb{Z}}(p^{n-m+\gamma-k})$. *Then* $ind(D_K) = \frac{\ell}{p^k} ind(D)$. *This occurs if* $\Gamma_N \cap \Gamma_T = \Gamma_F$ *(i.e.* $D \cong N \otimes_F T$*).*

The formula in Corollary 3.3.8 is similar to the formula in Proposition 3.3.1 in the following manner. Set $p^{\ell_0} = \frac{p^k}{\ell}$. . Then, $\ell = ord_{\mathbb{Q}/\mathbb{Z}}(p^{n-m+\gamma-k})$, so

$$\ell = \begin{cases} p^{k-(n-m+\gamma)}, & \text{if } k > n-m+\gamma; \\ 1, & \text{if } k \leq n-m+\gamma. \end{cases}$$

This gives us

$$p^{\ell_0} = \frac{\ell}{p^k} = \begin{cases} p^{-(n-m+\gamma)}, & \text{if } k > n-m+\gamma; \\ p^{-k}, & \text{if } k \leq n-m+\gamma. \end{cases}$$

So, $ind(D) = p^{\ell_0} ind(D_K)$ where $\ell_0 = \min\{k, n - m + \gamma\}$.

Note that when $\Gamma_N \cap \Gamma_T = \Gamma_F$, then $\theta \in F^*$, so $H = F$ and $T = T_H$. So, in this case, the corollary applies to any K with $\Gamma_K \subseteq \Gamma_N + \Gamma_T$. Also, $m = 0$, so the formula reduces to $ind(D) = p^{\ell_0} ind(D_K)$ where $\ell_0 = \min\{k, n + \gamma\}$.

We will now prove Theorem 3.3.3.

Proof. There are three steps to the proof. First, we construct division algebras N' and T', with N' NSR and T' TTR, such that $D \sim N' \otimes_F T'$ and $E \subseteq T'$. We then extend scalars to K and compute the value group of the NSR and TTR parts of D_K. Finally, we compute the overlap in these value groups to get index information.

1. Computing N' and T'

We have $\tau \in T$ with $\tau^{p^e} = \pi_0$, so $\widetilde{\tau} = \tau F^*$ has order p^e in T^*/F^*. Recall from (1.1) in Section 1.4.2 that τ factors into

$$\tau = f i_1^{s_1} j_1^{t_1} \dots i_d^{s_d} j_d^{t_d}, \tag{3.6}$$

where $f \in F^*$. Also, we assumed that i_1 is the leading term for τ for which we arranged $s_1 = p^s$. Recall that $\widetilde{i_1}$ has order p^{r_1}, so $s + e = r_1$ (cf. equation (3.3)).

Let

$$T' = (xa_1, b_1)_{p^{r_1}} \otimes_F (a_2, b_2)_{p^{r_2}} \dots \otimes_F (a_d, b_d)_{p^{r_d}}.$$

Write $T \sim (x^{-1}, b_1)_{p^{r_1}} \otimes_F T'$. Note that $\Gamma_T = \Gamma_{T'}$ since $x \in U_F$. Let $i'_1, j'_1, \dots, i'_d, j'_d$ be the corresponding generators for T' and set $\tau' = f {i'_1}^{s_1} {j'_1}^{t_1} \dots {i'_d}^{s_d} {j'_d}^{t_d}$. Then, since T and T' have the same canonical pairing, we have, for some $\zeta \in \mu_{p^r}$ determined by the canonical pairing,

$$\begin{aligned}\tau'^{p^e} &= f^{p^e}\left(i_1'^{\,s_1} j_1'^{\,t_1} \dots i_d'^{\,s_d} j_d'^{\,t_d}\right)^{p^e} \\ &= \zeta f^{p^e} i_1'^{\,p^{s+e}}\left(j_1'^{\,t_1} i_2'^{\,s_2} j_2'^{\,t_2} \dots i_d'^{\,s_d} j_d'^{\,t_d}\right)^{p^e} \\ &= \zeta f^{p^e} x a_1 \left(j_1'^{\,t_1} i_2'^{\,s_2} j_2'^{\,t_2} \dots i_d'^{\,s_d} j_d'^{\,t_d}\right)^{p^e} \\ &= x\zeta f^{p^e} i_1^{p^{e+l}}\left(j_1^{\,t_1} i_2^{\,s_2} j_2^{\,t_2} \dots i_d^{\,s_d} j_d^{\,t_d}\right)^{p^e} \\ &= x f^{p^e}\left(i_1^{s_1} j_1^{\,t_1} \dots i_d^{\,s_d} j_d^{\,t_d}\right)^{p^e} \\ &= x\tau^{p^e} = x\pi_0 = \pi.\end{aligned}$$

So $E = F(\sqrt[p^e]{\pi}) \cong F(\tau') \subseteq T'$.

Let N' be the underlying division algebra of

$$N' \sim N \otimes_F (x^{-1}, b_1)_{p^{r_1}},$$

so $D \sim N \otimes_F T \sim N' \otimes_F T'$. Recall that we assumed $\gamma \leq r_1$. Since $p^{r_1} \mid exp(T) = p^r$, we have $p^\gamma \leq exp(T)$. Recall from before the statement of Theorem 3.3.3 that $x = x_0^{p^\gamma}$ and $M = F(\sqrt[p^{r_1}]{x}) = F(\sqrt[p^{r_1-\gamma}]{x_0})$. Using the symbol identity Prop. 1.2.4.4, we have $(x^{-1}, b_1)_{p^{r_1}} \sim (x_0, b_1^{-1})_{p^{r_1-\gamma}}$, where the last symbol is now NSR. Then N' is the underlying division algebra of $(L/F, \sigma, c)_{p^n} \otimes_F (M/F, \sigma_\omega, b_1^{-1})_{p^{r_1-\gamma}}$. Since F is a GLF, LM is a cyclic unramified extension of F which contains both L and M. Let σ' be a generator of $Gal(LM/F)$ such that $\sigma'|_L = \sigma$. Then, by Lemma 3.1.1, N' is NSR and $\Gamma_{N'}$ is generated over Γ_F by μ where

$$\mu = \frac{1}{p^n}v(c) - \frac{\lambda}{p^{r_1-\gamma}}v(b_1) = \frac{1}{p^n}v(c) - \lambda p^\gamma v(j_1), \tag{3.7}$$

and where $\lambda \in \overline{comp}(\sigma_\omega, \sigma)$ is chosen prime to p.

2. Extending scalars to K

Since N' is inertially split, we see from [JW90, Corollary 5.13] that

$$\Gamma_{N'_K} = \Gamma_{N'} + \Gamma_K = \langle \mu \rangle + \Gamma_K. \tag{3.8}$$

On the other hand $E \subseteq T'$, so $T'_E = C_{T'}(E)$. Also,

$$\Gamma_{T'_E} = \{v(\xi') \mid \xi' \text{ an armature element of } T' \text{ and } \langle \widetilde{\xi'}, \widetilde{\tau'} \rangle = 1\}.$$

By construction, T and T' have isometric armatures, and corresponding armature elements have the same value. Thus,

$$\Gamma_{T'_E} = \{v(\xi) \mid \xi \in T, \xi \text{ an armature element of } T' \text{ and } \langle\widetilde{\xi}, \widetilde{\tau}\rangle = 1\} \subseteq \Gamma_T. \tag{3.9}$$

Finally, $\Gamma_E \subseteq \Gamma_K \cap \Gamma_{T'_E} \subseteq \Gamma_K \cap \Gamma_T = \Gamma_E$, so $T'_E \otimes_E K$ is a division algebra by Theorem 1.3.2 with $D_1 = T'_E$, $D_2 = K$. Thus, $\Gamma_{T'_K} = \Gamma_{T'_E} + \Gamma_K$ and $ind(T'_K) = ind(T'_E)$.

3. Computing $\Gamma_{N'_K} \cap \Gamma_{T'_K}$

Let h be minimal among the z such that $z\mu \in \Gamma_{T'_K}$. In other words, $h = o(\mu + \Gamma_{T'_K})$ in $\Gamma_{N'_K}/(\Gamma_{N'_K} \cap \Gamma_{T'_K})$. Then, $h = [\Gamma_{N'_K} : (\Gamma_{N'_K} \cap \Gamma_{T'_K})]$. Thus,

$$\left[(\Gamma_{N'_K} \cap \Gamma_{T'_K}) : \Gamma_K\right] = [\Gamma_{N'_K} : \Gamma_K]/h. \tag{3.10}$$

Case 1: Suppose $\alpha \leq m$.

From (3.8), we have $\Gamma_{N'_K}/\Gamma_K = \langle \mu + \Gamma_K \rangle$. Note that $ind(N'_K)$ is a power of p and coincides with the order of $\mu + \Gamma_K$. By the definition of h, we have $h\mu \in \Gamma_{T'_K} \subseteq \Gamma_{T'} = \Gamma_T$. However, by (3.7), $h\mu = \frac{h}{p^n}v(c) - h\lambda p^\gamma v(j_1)$. Since $v(j_1) \in \Gamma_T$, we must have $\frac{h}{p^n}v(c) \in \Gamma_T$. Also, $\frac{1}{p^n}v(c) \in \Gamma_N$, so $\frac{h}{p^n}v(c) \in \Gamma_N \cap \Gamma_T = \langle \frac{1}{p^m}v(c)\rangle + \Gamma_F$ (by the definition of p^m in Section 3.2). Thus, $p^{n-m} \mid h$.

Let $h = p^{n-m}h'$ with $h' \in \mathbb{Z}$. Note that

$$h\mu = \frac{h'}{p^m}v(c) - h'\lambda p^{n-m+\gamma}v(j_1) = h'v(\theta) - h'\lambda p^{n-m+\gamma}v(j_1) = h'v\left(\theta j_1^{-\lambda p^{n-m+\gamma}}\right).$$

Since $\alpha \leq m$, we saw in the paragraphs following (3.1) that $\Gamma_K \subseteq \Gamma_T$, $K = E$, and $k = e$. In this case, $\Gamma_{T'_K} = \Gamma_{T'_E} \subseteq \Gamma_T$.

Let C_T denote the canonical pairing on $(\Gamma_T/\Gamma_F) \times (\Gamma_T/\Gamma_F)$. Recall from (3.3) and (3.6) that $e + r_1 = s$ and $\tau = f i_1^{s_1} j_1^{t_1} \ldots i_d^{s_d} j_d^{t_d}$. Then, by [TW87, Proposition 3.3] (see Prop. 1.4.4 above), we have

$$\begin{aligned} C_T(h\mu, v(\tau)) &= h'\langle \widetilde{\theta \widetilde{j_1}^{-\lambda p^{n-m+\gamma}}}, \widetilde{\tau}\rangle \\ &= h'\big(\langle\widetilde{\theta},\widetilde{\tau}\rangle - \lambda p^{n-m+\gamma}\langle\widetilde{j_1},\widetilde{\tau}\rangle\big) \\ &= h'\big(\langle\widetilde{\theta},\widetilde{\tau}\rangle - \lambda p^{n-m+\gamma}\langle\widetilde{j_1},\widetilde{i_1}^{p^s}\rangle\big) \\ &= h'\big(\langle\widetilde{\theta},\widetilde{\tau}\rangle + \lambda p^{n-m+\gamma+s-r_1}\big) \\ &= h'\big(\langle\widetilde{\theta},\widetilde{\tau}\rangle + \lambda p^{n-m+\gamma-e}\big) \\ &= h'\big(\langle\widetilde{\theta},\widetilde{\tau}\rangle + \lambda p^{n-m+\gamma-k}\big). \end{aligned}$$

Set $\ell' = ord_{\mathbb{Q}/\mathbb{Z}}\big(\langle\widetilde{\theta},\widetilde{\tau}\rangle + \lambda p^{n-m+\gamma-k}\big)$. From (3.1), we obtain

$$v(\tau) = \frac{1}{p^e}v(\pi) = \frac{1}{p^k}v(\pi) = \frac{g}{p^\alpha}v(c) + \frac{1}{p^\beta}v(t) = v(\theta^{gp^{m-\alpha}}\rho),$$

so $\langle\widetilde{\theta},\widetilde{\tau}\rangle = \langle\widetilde{\theta},\widetilde{\theta}^{gp^{m-\alpha}}\widetilde{\rho}\rangle = \langle\widetilde{\theta},\widetilde{\rho}\rangle$, thus $\ell' = ord_{\mathbb{Q}/\mathbb{Z}}\big(\langle\widetilde{\theta},\widetilde{\rho}\rangle + \lambda p^{n-m+\gamma-k}\big) = \ell$, where ℓ is defined in the statement of Theorem 3.3.3. By (3.9), $h\mu \in \Gamma_{T'_K} = \Gamma_{T'_E}$ if and only if $C_T(h\mu, v(\tau)) = 1$ if and only if $h'\big(\langle\widetilde{\theta},\widetilde{\tau}\rangle + \lambda p^{n-m+\gamma-k}\big) = 1$. Now h is minimal when h' is minimal, which occurs when $h' = \ell$. Therefore, $h = \ell p^{n-m}$. Thus,

$$h/p^e = \ell p^{n-m-k}, \tag{3.11}$$

as $e = k$. We will show later in (3.14) that (3.11) and (3.10) imply $ind\, D_K = \frac{\ell}{p^k}\cdot ind\, D$.

Case 2: Suppose $\alpha > m$.

Recall we defined m by $\langle\frac{1}{p^n}v(c) + \Gamma_F\rangle \cap \Gamma_T = \langle\frac{1}{p^m}v(c) + \Gamma_F\rangle$. Thus, by (3.1) and (3.4),

$$p^{\alpha-m} = o\big(\frac{g}{p^\alpha}v(c) + \Gamma_T\big) = o\big(\frac{1}{p^k}v(\pi) + \Gamma_T\big) = |(\Gamma_K + \Gamma_T) : \Gamma_T| = p^{k-e}.$$

So,

$$e = k - (\alpha - m), \tag{3.12}$$

whence, by equation (3.1) and (3.2), we get

$$v(\tau) = \frac{1}{p^e}v(\pi) = \frac{1}{p^{k-(\alpha-m)}}v(\pi) = \frac{g}{p^m}v(c) + \frac{1}{p^{\beta-(\alpha-m)}}v(t) = v(\theta^g\rho^{p^{\alpha-m}}). \tag{3.13}$$

Set $\kappa = \frac{1}{p^k}v(\pi)$, so $\Gamma_K = \langle\kappa\rangle + \Gamma_F$. Recall that we defined $h = o(\mu + \Gamma_{T'_K})$. Since $\Gamma_{T'_K} = \Gamma_{T'_E} + \Gamma_K$, there exists an $z \in \mathbb{Z}$ such that $h\mu + z\kappa \in \Gamma_{T'_E}$. From part *2*, $\Gamma_{T'_E} \subseteq \Gamma_{T'} = \Gamma_T$, so we use (3.7) and (3.1) to see that Γ_T contains

$$\begin{aligned} h\mu + z\kappa &= \frac{h}{p^n}v(c) - h\lambda p^\gamma v(j_1) + \frac{gz}{p^\alpha}v(c) + \frac{z}{p^\beta}v(t) \\ &= \frac{h + gzp^{n-\alpha}}{p^n}v(c) - h\lambda p^\gamma v(j_1) + zv(\rho). \end{aligned}$$

Since $v(j_1), v(\rho) \in \Gamma_T$, we must have $\frac{h+gzp^{n-\alpha}}{p^n}v(c) \in \Gamma_T$, whence $p^{n-m} \mid (h + gzp^{n-\alpha})$. Also, $\alpha > m$, so $p^{n-\alpha} \mid p^{n-m} \mid (h + gzp^{n-\alpha})$. This gives us $p^{n-\alpha} \mid h$.

Let $h = p^{n-\alpha}h'$. Since $p^{n-m} \mid (h+gzp^{n-\alpha}) = p^{n-\alpha}(h'+gz)$, we see that $p^{\alpha-m} \mid (h'+gz)$. Thus, by (3.2),

$$\begin{aligned} h\mu + z\kappa &= \frac{h + gzp^{n-\alpha}}{p^n}v(c) - h\lambda p^\gamma v(j_1) + zv(\rho) \\ &= \frac{h' + gz}{p^{\alpha-m}} \cdot \frac{1}{p^m}v(c) - h'\lambda p^{\gamma+n-\alpha}v(j_1) + zv(\rho) \\ &= v(\theta^{(h'+gz)p^{m-\alpha}} j_1^{-h'\lambda p^{\gamma+n-\alpha}} \rho^z). \end{aligned}$$

Again, let C_T denote the canonical pairing on $(\Gamma_T/\Gamma_F) \times (\Gamma_T/\Gamma_F)$. Recall from (3.3) and (3.6) that $e + s = r_1$ and $\tau = fi_1^{s_1}j_1^{t_1}\dots i_d^{s_d}j_d^{t_d}$. Then, by (3.13), (3.12), and [TW87, Proposition 3.3] (see Prop. 1.4.4), we have

$$\begin{aligned} C_T(h\mu + z\kappa, v(\tau)) &= \langle\widetilde{\theta}^{(h'+gz)p^{m-\alpha}} \widetilde{j}_1^{-h'\lambda p^{\gamma+n-\alpha}} \widetilde{\rho}^z, \widetilde{\tau}\rangle \\ &= \frac{h' + gz}{p^{\alpha-m}}\langle\widetilde{\theta}, \widetilde{\tau}\rangle - h'\lambda p^{\gamma+n-\alpha}\langle\widetilde{j}_1, \widetilde{\tau}\rangle + z\langle\widetilde{\rho}, \widetilde{\tau}\rangle \\ &= \frac{h' + gz}{p^{\alpha-m}}\langle\widetilde{\theta}, \widetilde{\theta}^g\widetilde{\rho}^{p^{\alpha-m}}\rangle - h'\lambda p^{\gamma+n-\alpha}\langle\widetilde{j}_1, \widetilde{i}_1^{p^s}\rangle + z\langle\widetilde{\rho}, \widetilde{\theta}^g\widetilde{\rho}^{p^{\alpha-m}}\rangle \\ &= (h' + gz)\langle\widetilde{\theta}, \widetilde{\rho}\rangle + h'\lambda p^{\gamma+n-\alpha-e} + gz\langle\widetilde{\rho}, \widetilde{\theta}\rangle \\ &= h'\big(\langle\widetilde{\theta}, \widetilde{\rho}\rangle + \lambda p^{\gamma+n-\alpha-(k-(\alpha-m))}\big) \\ &= h'\big(\langle\widetilde{\theta}, \widetilde{\rho}\rangle + \lambda p^{n-m+\gamma-k}\big). \end{aligned}$$

Now $h\mu + z\kappa \in \Gamma_{T'_E}$ if and only if $C_T(h\mu + z\kappa, v(\tau)) = 1$ if and only if $h'\big(\langle\widetilde{\theta}, \widetilde{\rho}\rangle + \lambda p^{n-m+\gamma-k}\big) = 1$. From the statement of the theorem,

$$\ell = \mathrm{ord}_{\mathbb{Q}/\mathbb{Z}}\left(\langle\widetilde{\theta}, \widetilde{\rho}\rangle + \lambda p^{n-m+\gamma-k}\right).$$

Now h is minimal when h' is minimal, whence $h' = \ell$ and $h = \ell p^{n-\alpha}$. Thus, we again have (cf. equation (3.11)),

$$h/p^e = \ell p^{n-m-k}.$$

This completes Case *2*.

Recall from (3.10) that $\left[(\Gamma_{N'_K} \cap \Gamma_{T'_K}) : \Gamma_K\right] = [\Gamma_{N'_K} : \Gamma_K]/h$. Recall also that $T'_E = C_{T'}(E)$, so $ind(T'_E) = ind(T')/p^e$. Thus, by (3.11), which we have seen holds in Case *1* and in Case *2*,

$$\begin{aligned} ind\ D_K &= \frac{ind\ N'_K \cdot ind\ T'_K}{\left[(\Gamma_{N'_K} \cap \Gamma_{T'_K}) : \Gamma_K\right]} \\ &= \frac{[\Gamma_{N'_K} : \Gamma_K] \cdot ind(T'_E)}{[\Gamma_{N'_K} : \Gamma_K]/h} \\ &= h\, ind(T')/p^e \\ &= \ell p^{n-m-k} ind(T) \\ &= \frac{\ell}{p^k} \cdot \frac{ind\ N \cdot ind\ T}{|(\Gamma_N \cap \Gamma_T) : \Gamma_F|} \\ &= \frac{\ell}{p^k} \cdot ind(D). \end{aligned} \tag{3.14}$$

It remains to determine the largest subfield of K lying in D. Let $K_i = F(\sqrt[p^{k-i}]{\pi})$ where $0 \leq i \leq k$. Let us apply the part of Theorem 3.3.3 which we have already proven to K_i over F. We must recompute the constants k, n, m, γ, θ, and ρ for K_i in place of K.

The constants $n = deg(N)$ and $m = |(\Gamma_N \cap \Gamma_T) : \Gamma_F|$ remain the same. We defined θ as any armature element of T such that $v(\theta) = \frac{1}{p^m} v(c)$, so we may leave θ unchanged. Also, the uniformizer π has not changed. Since x is determined from π and T (by $\pi = x\pi_0$ where π_0 has some p-power root in T), we may make the same choice of x, whence γ does not change. However, we let $p^{k_i} = [K_i : F] = p^k/[K : K_i] = p^{k-i}$. Also, the decomposition (3.1) becomes

$$\frac{1}{p^{k-i}} v(\pi) = \frac{g}{p^{\alpha-i}} v(c) + \frac{1}{p^{\beta-i}} v(t). \tag{3.15}$$

Then, so we may choose $\rho_i = \rho^{p^i} \in T$ as our armature element with value $\frac{1}{p^{\beta-i}}v(t)$. Then

$$ind\ D_{K_i} = \frac{\ell_i}{p^{k_i}} \cdot ind\ D = \ell_i \frac{ind(D)}{[K_i : F]}, \tag{3.16}$$

where

$$\begin{aligned}\ell_i &= ord_{\mathbb{Q}/\mathbb{Z}}\Big(\langle\widetilde{\theta}, \widetilde{\rho}_i\rangle + \lambda p^{n-m+\gamma-k_i}\Big)\\ &= ord_{\mathbb{Q}/\mathbb{Z}}\Big(p^i\langle\widetilde{\theta}, \widetilde{\rho}\rangle + p^i\lambda p^{n-m+\gamma-k}\Big)\\ &= \max\Big(p^{-i} ord_{\mathbb{Q}/\mathbb{Z}}\Big(\langle\widetilde{\theta}, \widetilde{\rho}\rangle + \lambda p^{n-m+\gamma-k}\Big), 1\Big)\\ &= \max(l/p^i, 1).\end{aligned}$$

Thus, (3.16) shows K_i is isomorphic to a subfield of D if and only if $\ell_i = 1$, if and only if $\ell \le p^i$, if and only if $[K_i : F] = p^{k-i} \le p^k/\ell$. The largest such subfield is $F(\sqrt[p^k/\ell]{\pi})$.

Note that this "accounts for" all the index reduction from D to D_K, in that, if we let $K_0 = F(\sqrt[p^k/\ell]{\pi})$, then $ind(D_{K_0}) = ind(D)/[K_0 : F]$ (as $K_0 \subseteq D$) and $ind(D_K) = ind(D_{K_0})$. □

Remark 3.3.9. We have another description of the constant γ defined preceding (3.2). Apply Theorem 3.3.3 to T in place of D. Then $n = m = 0$, $k = e$, and $\theta \in F^*$, however, π, π_0 remain the same, so γ remains unchanged. The ℓ of Theorem 3.3.3 reduces to $\ell = ord_{\mathbb{Q}/\mathbb{Z}}(p^{\gamma-k})$. Then Theorem 3.3.3 shows that $ind(T_K) = \frac{\ell}{p^e} ind(T)$. Let $\ell_0 = \min\{e, \gamma\}$, so $p^e/\ell = p_0^\ell$ and p^{ℓ_0} is the degree of the largest subfield, K_0, of K lying in T, i.e. for $\gamma \le e$, $[K_0 : F] = p^\gamma$.

Remark 3.3.10. In the proof of Theorem 3.3.3, we gave a decomposition of D_K into $N_K' \otimes_F T_K'$, with N_K' NSR and T_K' TTR. First, this allows us to compute the value group of D_K. By [JW90, Theorem 6.3], $\Gamma_{D_K} = \Gamma_{N_K'} + \Gamma_{T_K'}$, where $\Gamma_{N_K'} = \langle\mu\rangle + \Gamma_K$ for μ described in (3.7) and $\Gamma_{T_K'} = \Gamma_{T_E'} + \Gamma_K$ with $\Gamma_{T_E'}$ described in (3.9). Second, this allows us to compute the residue, $\overline{D}$; by applying Corollary 2.1.5 and (3.14) above, $\overline{D}$ is the unique extension of $\overline{F}$ of degree

$$\frac{ind\ N_K'}{\big[(\Gamma_{N_K'} \cap \Gamma_{T_K'}) : \Gamma_K\big]} = \frac{[\Gamma_{N_K'} : \Gamma_K]}{[\Gamma_{N_K'} : \Gamma_K]/h} = h = \frac{\ell p^n}{p^{\max\{m,\alpha\}}}.$$

Remark 3.3.11. We may generalize Theorem 3.3.3 by dropping the assumption that $\Gamma_K \subseteq \Gamma_D = \Gamma_N + \Gamma_T$. For, if $\Gamma_K \nsubseteq \Gamma_N + \Gamma_T$, let K' be the subfield of K with $\Gamma_{K'} = \Gamma_K \cap (\Gamma_N + \Gamma_T)$. Then $ind(D_K) = ind(D_{K'})$, since, by applying Theorem 1.3.2 with $D_1 = D_{K'}$ and $D_2 = K$, we have $D_{K'} \otimes_{K'} K$ is a division algebra. Note that $ind(D_{K'})$ is computable by Theorem 3.3.3. In addition, $\Gamma_{D_K} = \Gamma_{D_{K'}} + \Gamma_K$ and $\overline{D_K} = \overline{D_{K'}}$.

Remark 3.3.12. Let K be any finite degree TRRT field extension of F. There exist fields K_i with $F = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{n-1} \subseteq K_n = K$, such that K_i is TTR cyclic over K_{i-1}. By applying the theorem iteratively to $D_{K_i} \sim N_{K_i} \otimes_F T_{K_i}$, we are able compute $ind(D_K)$. So the theorem allows us, in principle, to compute restriction over arbitrary finite degree TRRT extensions of F.

Chapter 4

Corestriction

As mentioned in the introduction, the corestriction map is not very well-understood. In [RT83], Rosset and Tate give a complicated recursive formula for corestriction. In a few cases, the formula simplifies; Merkurjev gives a few basic corestriction formulas in [Mer85]. In the case where F is Henselian, Hwang gave extensive calculations concerning corestriction (cf. [Hwa95a], [Hwa95b]).

The chapter is organized as follows. The first seven sections concern corestriction of algebras over a field that does not necessarily have a valuation. In Section 4.1, we show how symbol algebras can be decomposed into a triple cup product. Using this decomposition, we prove the following projection-type formula (Theorem 4.2.4)

$$cor_{L/F}\,(a, b; L, \zeta)_n = \left(a, b; F, \eta^{n/d}\right)_d,$$

where $\zeta \in \mu_n^*(L)$, $L = F(\mu_n)$, $a, b \in F$, $d = o(N_{L/F}(\zeta))$ and $N_{L/F}(\eta) = \zeta^{n/d}$. In Section 4.2, we prove Theorem 4.2.4 and give various norm formulas. Next, in Section 4.3 and Section 4.4, we show how to compute the corestriction of characters over a quadratic or abelian extension. These formulas allow us, in Section 4.5, to compute $cor_{L/F}(\chi, b)$, where $b \in L$, $\chi \in X(L)$ and L/F is a cyclotomic extension. In Section 4.6, we review some basic material on radical extensions, and prove two propositions about intersections of radical extensions.

In Section 4.7, we show how to compute $cor_{N/F}\,(t_1, t_2; N)_n$ where N/F is a finite degree extension, $\mu_n \subseteq N$, and $t_1, t_2 \in N$ have finite order in N^*/F^* (cf. Theorem 4.7.4); this is the main result in this chapter. We first look at the case where n is a prime power. By the projection-type formula, Theorem 4.2.4, we can reduce to the case where $N = F(t_1, t_2)$. Then, using results on radical extensions from Section 4.6, we compute $cor_{N/F(\mu_q)}(t_1, t_2; N)_{p^n}$, where, if p is odd, then $q = p$, otherwise, $q = 4$. Finally, the formulas in Section 4.5 finish the computation.

Now let F be a valued field and let L be a finite-degree extension of F. For $D \in \mathcal{D}(L)$, let ${}^cD$ stand for the underlying division algebra of $cor_{L/F}[D]$. The remaining sections, 4.8 and 4.9, show how Theorem 4.7.2 can be used to compute ${}^cD$, $\Gamma_{{}^cD}$ and $\overline{{}^cD}$. In Section 4.8, we give a generalization to one of Hwang's results (cf. Theorem 4.8.6 and Corollary 4.8.8). In Section 4.9, we give corestriction calculations for NSR and TTR division algebras over an extension of GLF's.

4.1 Decomposition of symbol algebras

Take $n \in \mathbb{N}$ with $char(F) \nmid n$ and suppose $\mu_n \cap F = \mu_k$ for some $k \mid n$. Let $A = (a, b; \zeta)_k$ be a degree k symbol algebra over F. We will assume that aF^{*k} has order k in F^*/F^{*k} (i.e. $[F(\sqrt[k]{a}) : F] = k$ by Kummer theory).

Let $K = F(\sqrt[k]{a})$ and let $\sigma_\zeta \in Gal(K/F)$ be the element such that $\sigma_\zeta(\sqrt[k]{a}) = \zeta\sqrt[k]{a}$. Then $A \cong (K/F, \sigma_\zeta, b)$, so A corresponds to a semi-symbol (χ, b) where $\chi \in H^1(G_F, \mathbb{Q}/\mathbb{Z})$ has order k with $F(\chi) = K$ and $\sigma_\chi = \sigma_\zeta$. If we identify $(\frac{1}{n}\mathbb{Z})/\mathbb{Z}$ with $\mathbb{Z}_n$, then we may consider χ as an element of $H^1(G_F, \mathbb{Z}_n)$ with $im(\chi) \subseteq n/k\mathbb{Z}_n$. Define $\widehat{\mu}_n = Hom(\mu_n, \mathbb{Z}_n)$. Our goal is to construct $f \in H^0(G_F, \widehat{\mu}_n)$ and $g \in Z^1(G_F, \mu_n)$ such that χ corresponds to $f \cup [g]$ (see Theorem 4.1.2). Thus, A can be realized as a triple cup product.

For the remainder of this section, we will abbreviate $H^i(G_F, \cdot)$ to $H^i(\cdot)$. Take $\sigma \in G_F$, $\omega \in \mu_n$, and $f \in \widehat{\mu}_n$. We make $\widehat{\mu}_n$ into a G_F-module by defining

$$\sigma f(\omega) = \sigma\left(f\left(\sigma^{-1}(\omega)\right)\right) = f\left(\sigma^{-1}(\omega)\right), \qquad (4.1)$$

where the last equality holds because G_F acts trivially on $\mathbb{Z}_n$. Then, $H^0(\widehat{\mu}_n) = \widehat{\mu}_n^{G_F} = \{f \in \widehat{\mu}_n : \sigma f = f \text{ for all } \sigma \in G_F\} = \{f \in \widehat{\mu}_n : f = f \circ \sigma^{-1} \text{ for all } \sigma \in G_F\}$.

Lemma 4.1.1. *Take $f \in \widehat{\mu}_n$ and suppose $\mu_n \cap F = \mu_k$. Then $f \in H^0(\widehat{\mu}_n)$ if and only if $im(f) \subseteq (n/k)\mathbb{Z}_n$. Furthermore, $|H^0(\widehat{\mu}_n)| = k$.*

Proof. Fix $\zeta \in \mu_n^*$ and take $f \in \widehat{\mu}_n$. Note that f is completely determined by $f(\zeta)$. Since $\zeta^l \in F^*$ if and only if $(n/k) \mid l$, it is enough to show that $f \in H^0(\widehat{\mu}_n)$ if and only if $\zeta^{f(\zeta)} \in F^*$. For, if this holds, then $im(f) \subseteq (n/k)\mathbb{Z}_n$ and $|H^0(\widehat{\mu}_n)| = |\{f(\zeta) : f \in H^0(\widehat{\mu}_n)\}| = n/(n/k) = k$.

First, for $\sigma \in G_F$, let $\sigma(\zeta) = \zeta^{k_\sigma}$, where k_σ is determined modulo n. Now, if $f \in H^0(\widehat{\mu}_n)$, then, for all $\sigma \in G_F$, we have $f(\zeta) = f\left(\sigma^{-1}(\zeta)\right) = f(\zeta^{k_{\sigma^{-1}}}) = k_{\sigma^{-1}} f(\zeta)$, whence

$$\sigma\left(\zeta^{f(\zeta)}\right) = \sigma(\zeta^{k_{\sigma^{-1}} f(\zeta)}) = \sigma(\sigma^{-1}(\zeta)^{f(\zeta)}) = \zeta^{f(\zeta)}.$$

Thus, $\zeta^{f(\zeta)} \in \mathcal{F}(G_F) = F$. On the other hand, if $\zeta^{f(\zeta)} \in F^*$, then for all $\sigma \in G_F$, we have $\zeta^{f(\zeta)} = \sigma^{-1}(\zeta^{f(\zeta)}) = \zeta^{k_{\sigma^{-1}} f(\zeta)}$, whence $f(\zeta) \equiv k_{\sigma^{-1}} f(\zeta)$ *mod* n. Thus, $f(\sigma^{-1}(\zeta)) = f(\zeta^{k_{\sigma^{-1}}}) = k_{\sigma^{-1}} f(\zeta) = f(\zeta)$ modulo n. So $f \in H^0(\widehat{\mu}_n)$, which completes the proof. □

Now identify the G_F-modules $\widehat{\mu}_n \otimes \mu_n$ and $\mathbb{Z}_n$ via $f \otimes \zeta \mapsto f(\zeta)$. The cup product $\cup : H^0(\widehat{\mu}_n) \otimes H^1(\mu_n) \to H^1(\mathbb{Z}_n)$ is computed by

$$(f \cup [g])(\sigma) = f \otimes g(\sigma) = f(g(\sigma)),$$

where $\sigma \in G_F, f \in H^0(\widehat{\mu}_n)$, and $g \in Z^1(\mu_n)$ (cf. [Ser79, Appendix to Ch. XI, p.176]). However, Lemma 4.1.1 tells us that $Im(f) \subseteq (n/k)\mathbb{Z}_n$, as $\mu_n \cap F = \mu_k$, so $(f \cup g) : G_F \to (n/k)\mathbb{Z}_n$. This shows that the number of roots of unity in F gives a constraint on the order of characters obtained as cup products in this manner.

Consider the exact sequence $0 \to \mu_n \to F_{sep}^* \to F_{sep}^* \to 0$, where the maps are inclusion and the n-th power map. Since $H^0(F_{sep}^*) = F^*$ and $H^1(F_{sep}^*) = 0$ by Hilbert's Theorem 90, we get the exact sequence $F^* \to F^* \to H^1(\mu_n) \to 0$, where the first map is again the n-th power map. So $F^*/F^{*n} \cong H^1(\mu_n)$, with the isomorphism given by

$tF^{*n} \mapsto [\alpha_{n,t}]$, where $\alpha_{n,t}$ is the 1-cocycle given by $\alpha_{n,t}(\sigma) = \sigma(\sqrt[n]{t})/\sqrt[n]{t}$ for $\sigma \in G_F$ and any fixed n-th root of t.

We will now decompose χ as a cup product.

Theorem 4.1.2. *Let $\chi \in H^1(\mathbb{Z}_n)$ and suppose $o(\chi) = k$, $F(\chi) = F(\sqrt[k]{a})$, and $\zeta = \sigma_\chi(\sqrt[k]{a})/\sqrt[k]{a} \in \mu_k^*$. Let $\alpha_{n,a} \in Z^1(\mu_n)$ be as described just above and let $\omega \in \mu_n^*$ be any n/k-th root of ζ. Then $\chi = f_\chi \cup [\alpha_{n,a}]$, where $f_\chi \in H^0(\widehat{\mu}_n)$ is determined by $f_\chi(\omega) = n/k$.*

Proof. Take $\tau \in G_F$. Since $\tau(\sqrt[n]{a})/\sqrt[n]{a} = \omega^i$ for some i, we have $\tau(\sqrt[k]{a})/\sqrt[k]{a} = (\omega^{n/k})^i = \zeta^i$. So $\tau|_{F(\chi)} = \sigma_\chi^i$, whence $\chi(\tau) = \chi(\sigma_\chi^i) = i \cdot n/k$. By Lemma 4.1.1, $f_\chi \in H^0(\widehat{\mu}_n)$. We have $(f_\chi \cup [\alpha_{n,a}])(\tau) = f_\chi(\tau(\sqrt[n]{a})/\sqrt[n]{a}) = f_\chi(\omega^i) = i \cdot n/k = \chi(\tau)$. Thus, $f_\chi \cup [\alpha_{n,a}] = \chi$. □

4.2 Projection Formulas and Norms

Our main goal in this section is to give a few basic projection formulas. All of the formulas involving symbol algebras essentially come from the projection formula for cup products, which can be found in [Bro94, Ch. V, 3.8], [CF67, Ch. IV, Prop. 9], or [NSW00, Prop. 1.5.3]. We will give formulas for $cor_{L/F}\,(a, b; L)_n$ and $cor_{L/F}\,(\omega, b; L)_n$, where $a, b \in F$ and $\omega \in \mu(L)$. We begin the section by stating the projection formula for cup products.

Theorem 4.2.1. *Fix $p, q \geq 0$ and let G be a profinite group with $H \subseteq G$ a subgroup of finite index. If A, B are discrete G-modules, then for $a \in H^p(H, A)$ and $b \in H^q(G, B)$, we have $cor_H^G\left(a \cup res_H^G(b)\right) = cor_H^G(a) \cup b$.*

Remark 4.2.2. In [CF67], the result is proven for G finite, however, we can use inverse limits to obtain the result for the case where G is profinite (cf. [Ser79, Ch. X, §3]). The result in [Bro94] does not assume that G is finite, but is in the context of group cohomology and not continuous group cohomology.

Theorem 4.2.3 is a Brauer group version of the previous projection formula; this formula can be found in [Dra83, p.88], [Ser79, Ch. XIV], or [Tig87].

Theorem 4.2.3. *Let L/F be a finite-dimensional separable field extension with $\mu_n \subseteq F$. If $a \in F^*$ and $b \in L^*$, then*

$$cor_{L/F}(a, b; L)_n = (a, N_{L/F}(b); F)_n.$$

Theorem 4.2.3 is well-known and deducible from Theorem 4.2.1, but the author cannot find a good reference for such a cohomological proof. A thorough proof that does not use cohomological machinery can be found in [Tig87]. Tignol points out that the exposition in [Dra83] contains a mistake in the proof of a key proposition (cf. [Dra83, line 3, p.55]) which could be easily amended (cf. [Tig87, Theorem 2.5]). Serre gives 4.2.3 as an exercise (cf. [Ser79, Ch. XIV, §1]).

In Section 4.1, we showed how to decompose a symbol algebra into a triple cup product. We may think of the components of the product as representing the slots of the symbol and the root of unity which relates how elements in the algebra commute. Above, we saw that corestriction corresponds to a norm when one of the slots lies in F and $\mu_n \subseteq F$. We now show what happens when $\mu_n \not\subseteq F$, but $a, b \in F^*$.

Theorem 4.2.4. *Let F be a field with $\mathrm{char}(F) \nmid n$ and let $L = F(\mu_n)$. Then for $a, b \in F^*$ and $\zeta \in \mu_n^*$, we have*

$$cor_{L/F}\,(a, b; L, \zeta)_n = \left(a, b; F, \eta^{n/d}\right)_d,$$

where d is the order of $N_{L/F}(\zeta)$ and $\eta \in \mu_n^*$ satisfies $N_{L/F}(\eta) = \zeta^{n/d}$.

Remark 4.2.5. Note that $\eta^{n/d}$ and $\zeta^{n/d}$ are both primitive d-th roots of unity, so there is a c prime to d such that $\eta^{cn/d} = \zeta^{n/d}$. Thus,

$$cor_{L/F}\,(a, b; L, \zeta)_n = \left(a, b; F, \eta^{n/d}\right)_d = \left(a, b^c; F, \zeta^{n/d}\right)_d.$$

Also, d is independent of ζ, since for any m prime to n, we have $N_{L/F}(\zeta^m) = (N_{L/F}(\zeta))^m \in \mu_d^*$, since m is necessarily prime to d. This allows us to determine d by $N_{L/F}(\mu_n) = \mu_d$.

Proof. Assume first that $[L(\sqrt[n]{a}) : L] = n$. Let $A = (a,b;L,\zeta)_n$ correspond to the semi-symbol (χ, b) and let θ be a fixed n-th root of a, so $L(\chi) = L(\theta)$ and $\sigma_\chi(\theta) = \zeta\theta$. By Theorem 4.1.2, $\chi = f_\zeta \cup [\alpha_{n,a}]$, where $f_\zeta \in H^0(G_L, \widehat{\mu}_n)$ and $\alpha_{n,a} \in Z^1(G_L, \mu_n)$ are defined by $f_\zeta(\zeta) = 1 \in \mathbb{Z}_n$ and $\alpha_{n,a}(\sigma) = \sigma(\theta)/\theta$. Since $a, b \in F^*$, both $\alpha_{n,a}$ and $b \in H^0(G_L, L^*_{sep})$ are in the image of $res^{G_F}_{G_L}$; let $[\alpha_{n,a}] = res_{L/F}[\alpha'_{n,a}]$, where $\alpha'_{n,a}(\tau) = \tau(\theta)/\theta$ for $\tau \in G_F$. Using Theorem 4.2.1 and the commutativity of corestriction with the connecting homomorphism ∂ (cf. Prop. 1.6.2), we get

$$\begin{aligned} cor_{L/F}(A) =& cor_{L/F}(\partial\chi \cup b) = \partial(cor_{L/F}(\chi)) \cup b \\ &= \partial(cor_{L/F}(f_\zeta \cup res_{F/L}[\alpha'_{n,a}])) \cup b = \partial\left(cor_{L/F}(f_\zeta) \cup [\alpha'_{n,a}]\right) \cup b, \end{aligned}$$

where we have identified $Br(F)$ with $H^2(G_F, F^*_{sep})$.

Let $\chi' = cor_{L/F}(f_\zeta) \cup [\alpha'_{n,a}]$. For $\sigma \in G_F$, we have $\sigma f_\zeta = f_\zeta \circ \sigma^{-1}$ (cf. equation (4.1)). Since $f_\zeta \in H^0(G_L, \widehat{\mu}_n)$, we get $cor_{L/F}(f_\zeta) = \sum_{\sigma \in G(L/F)} \sigma f_\zeta = f_\zeta \circ N_{L/F}$ (cf. Definition 1.6.1). Let $f' = f_\zeta \circ N_{L/F}$, so $\chi' = f' \cup [\alpha'_{n,a}]$.

Let $d = o(N_{L/F}(\zeta))$, so the norm map maps onto μ_d in F^*. Take $\eta \in \mu_n^*$ such that $N_{L/F}(\eta) = \zeta^{n/d}$. We claim that $F(\chi') = F(\theta^{n/d})$. Since $\mu_d = \langle N_{L/F}(\zeta)\rangle \subseteq F$, we have $F(\theta^{n/d}) = F(\sqrt[d]{a})$ is a Kummer extension of F. Then, for $\tau \in G_F$, if $\tau(\theta)/\theta = \eta^j$, then $\chi'(\tau) = f'(\alpha'_{n,a}(\tau)) = f'(\tau(\theta)/\theta) = f_\zeta(N_{L/F}(\eta^j)) = f_\zeta(\zeta^{jn/d}) = jn/d \in \mathbb{Z}_n$. Since j ranges over all congruence classes mod n, as $[F(\theta) : F] = [L(\sqrt[n]{a}) : L] = n$, we have $im(\chi') = \langle n/d\rangle \mathbb{Z}_n$, so χ' has order d. Let $\gamma = \theta^{n/d}$. When $\tau(\theta)/\theta = \eta^j$, we have $\tau(\gamma)/\gamma = \eta^{jn/d}$ and $\chi'(\tau) = jn/d \in \mathbb{Z}_n$. Therefore, $\tau \in ker(\chi')$ iff $d \mid j$ iff $\tau(\gamma) = \gamma$, so $F(\chi') = F(\gamma)$, as claimed.

Now choose $\tau \in G_F$ with $\tau(\theta) = \eta\theta$. Since $\chi'(\tau) = n/d$, we have $\tau|_{F(\chi')} = \sigma_{\chi'}$, so $\sigma_{\chi'}(\gamma)/\gamma = \tau(\gamma)/\gamma = \eta^{n/d}$. Thus, $\partial\chi' \cup b$ corresponds to $(F(\sqrt[d]{a})/F, \sigma_{\chi'}, b) \cong \left(a, b; F, \eta^{n/d}\right)_d$.

If $[L(\sqrt[n]{a}) : L] \neq n$, then we pass to the rational function field $L(x)$ and write $res_{L(x)/L}(A) \sim (ax, b; L(x), \zeta)_n \otimes (x^{-1}, b; L(x), \zeta)_n$. We have $[L(x, \sqrt[n]{ax}) : L(x)] =$

$[L(x, \sqrt[n]{x^{-1}}) : L(x)] = n$ since ax and x are both irreducible in $L[x]$. Thus,

$$\begin{aligned} cor_{L(x)/F(x)} res_{L(x)/L}(A) &= \left(ax, b; F(x), \eta^{n/d}\right)_d \otimes_{F(x)} \left(x^{-1}, b; F(x), \eta^{n/d}\right)_d \\ &= \left(a, b; F(x), \eta^{n/d}\right)_d \\ &= res_{F(x)/F} \left(a, b; F, \eta^{n/d}\right)_d . \end{aligned}$$

By Proposition 1.6.3, $cor_{L/F}(A) = \left(a, b; F, \eta^{n/d}\right)_d$. □

Remark 4.2.6. In Theorem 4.2.4, we sometimes have $\eta^{n/d} = N_{L/F}(\zeta)$, so the result can then be stated purely in terms of ζ. For $j \in \mathbb{Z}$, let φ_j denote the j-th power map. Let $N_{L/F}(\zeta) = \zeta^{tn/d}$, for some $t \in \mathbb{Z}$ which is determined mod d. If we write $\eta = \zeta^i$, then $\zeta^{n/d} = N_{L/F}(\eta) = \zeta^{itn/d}$, so $it \equiv 1 \ mod \ d$. The condition $\eta^{n/d} = N_{L/F}(\zeta)$ is equivalent to $\zeta^{in/d} = \zeta^{tn/d}$, i.e. $i \equiv t \ mod \ d$. This holds if and only if $t^2 \equiv 1 \ mod \ d$.

We will give an example below in 4.2.10 of when the formula in 4.2.4 does not simplify in the manner described in Remark 4.2.6. We need a basic norm formula.

Proposition 4.2.7. *Let p be a prime and F be a field with $p \nmid char(F)$. Suppose $\mu_{p^k} \cap F = \mu_{p^r}$ for some $k \geq r \geq 0$, and take $\zeta \in \mu_{p^k}^*$. If p is odd, or, if $p = 2$ and $r \geq 2$ (i.e. $\mu_4 \subseteq F$), then $N_{F(\zeta)/F}(\zeta) = (-1)^{p^{k-r}-1}\zeta^{p^{k-r}} = -(-\zeta)^{p^{k-r}}$. If $p = 2$ and $r = 1$ (i.e. $\mu_4 \nsubseteq F$), then $N_{F(\zeta)/F}(\zeta) \in \{-1, 1\}$.*

Proof. Let $L = F(\zeta)$. If p is odd and $r \geq 1$ (i.e. $\mu_p \subseteq F$), or, $p = 2$ and $r \geq 2$ (i.e. $\mu_4 \subseteq F$), then $x^{p^{k-r}} - \zeta^{p^{k-r}}$ is the minimal polynomial of ζ over F (cf. Proposition 4.6.3). In this case, $N_{L/F}(\zeta) = (-1)^{p^{k-r}-1}\zeta^{p^{k-r}}$. On the other hand, if p is odd and $r = 0$ (i.e. $\mu_p \nsubseteq F$), or, $p = 2$ and $r = 1$ (i.e. $\mu_4 \nsubseteq F$), then $N_{L/F}(\zeta) \in F^*$ is a product of elements from μ_{p^k}. If p is odd, the only such product lying in F is 1, so $N_{L/F}(\zeta) = 1 = \zeta^{p^{k-r}} = (-1)^{p^{k-r}-1}\zeta^{p^{k-r}}$. If $p = 2$, then the product could be 1 or -1, so $N_{L/F}(\zeta) \in \{1, -1\}$. □

Remark 4.2.8. Here is an explicit description of $N_{F(\zeta)/F}(\zeta)$ in Proposition 4.2.7 for the case $p = 2$ and $r = 1$. (We omit the proof.) $N_{F(\zeta)/F}(\zeta) = -1$, if and only if ζ has maximal order in the 2-torsion of $F(\zeta)^*$ and either F has prime characteristic or *char*$(F) = 0$ and $F \cap \mathbb{Q}(\zeta) = \mathbb{R} \cap \mathbb{Q}(\zeta)$. Otherwise $N_{F(\zeta)/F}(\zeta) = 1$. Thanks to Adrian Wadsworth for pointing this out.

Corollary 4.2.9. *Let F be a field with $\mathrm{char}(F) \nmid n$ and let $L = F(\mu_n)$. Suppose n has prime factorization $p_1^{a_1} \dots p_l^{a_l}$, and $\mu_n \cap F = \mu_m$ with $m = p_1^{b_1} \dots p_l^{b_l}$. For $\zeta \in \mu_n^*$ with $\zeta = \zeta_1 \dots \zeta_l$, where $\zeta_i \in \mu^*_{p_i{}^{a_i}}$, we have*

$$N_{L/F}(\zeta) = \epsilon \prod_{i=1}^{l} \zeta_i^{[F(\zeta):F(\zeta_i)]p^{a_i - b_i}}.$$

If p_i are all odd, then $\epsilon = 1$. Otherwise, assume that $p_1 = 2$. Then

$$\epsilon = \frac{N_{F(\zeta_1)/F}(\zeta_1)^{[F(\zeta):F(\zeta_1)]}}{\zeta_1^{[F(\zeta):F]}}.$$

Proof. The result follows by applying Proposition 4.2.7 to each ζ_i. □

Example 4.2.10. Suppose $\zeta \in \mu^*_{35}$ and $\zeta = \alpha\beta$, where $\alpha \in \mu^*_5$ and $\beta \in \mu^*_7$. Let $F = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\zeta)$, so $[L : F] = 6$. Now $N_{L/F}(\zeta) = \alpha^6 = \alpha$, so $n = 35$ and $d = o(N_{L/F}(\zeta)) = 5$ in the setup of Theorem 4.2.4. If we set $\eta = \zeta^2$, then $N_{L/F}(\eta) = \alpha^2 = \zeta^{35/5}$, so $N_{L/F}(\eta) = \zeta^{n/d}$. But $\eta^{n/d} = \eta^{35/5} = \zeta^{14} = \alpha^4 \neq N_{L/F}(\zeta)$. So $N_{L/F}(\eta) = \zeta^{n/d}$, but $N_{L/F}(\zeta) \neq \eta^{n/d}$. In the context of Remark 4.2.6, $N_{L/F}(\zeta) = \alpha = (\zeta^{35/5})^3$, so $t = 3$, but $3^2 \not\equiv 1$ *mod* 5.

If n is a prime power, the formula in Theorem 4.2.4 simplifies as follows because $\eta^{n/d} = N_{L/F}(\zeta)$. This result is not new and could be proved by induction on $[L : F]$ using [Mer85, 1.7] (although, one should perhaps be careful if $[F(\sqrt[p^k]{a}) : F] < p^k$).

Corollary 4.2.11. *Let p be a prime and F be a field with $p \nmid \mathrm{char}(F)$. Take $\zeta \in \mu^*_{p^k}$ and let $L = F(\zeta)$ and $d = o(N_{L/F}(\zeta))$. Suppose $\mu_{p^k} \cap F = \mu_{p^r}$. Then, for $a, b \in F^*$,*

$$\mathrm{cor}_{L/F}\,(a, b; L, \zeta)_{p^k} = \Big(a, b; F, N_{L/F}(\zeta)\Big)_d = \Big(a, b^e; F, \zeta^{p^{k-r}}\Big)_{p^r}, \tag{4.2}$$

where $e = 1$ unless $p = 2$ and either $k > r \geq 2$ or $N_{L/F}(\zeta) = 1$ (so $r = 1$), in which case $e = 1 + 2^{r-1}$.

Remark 4.2.12. If $p = 2$ and $N_{L/F}(\zeta) = 1$, then $\Big(a, b; F, N_{L/F}(\zeta)\Big)_d$ is split. It may seem redundant to write $\Big(a, b; F, N_{L/F}(\zeta)\Big)_d = \Big(a, b^e; F, \zeta^{p^{k-r}}\Big)_{p^r}$ where $e = 2$. (Note that $N_{L/F}(\zeta) = 1$ only occurs when $p^r = 2^1 = 2$, cf. Proposition 4.2.7.) However, we need a formula which gives symbols in terms of compatible roots of unity.

Proof. Set $n = p^k$ and set $d = o(N_{L/F}(\zeta))$. If $k = r$, then $L = F$ and the result is clear. Assume now that $k > r$.

By Proposition 4.2.7, if p is odd, then $N_{L/F}(\zeta) = \zeta^{p^{k-r}}$. So $d = o(\zeta^{p^{k-r}}) = p^r$. Thus, $N_{L/F}(\zeta) = \zeta^{n/d}$. If $p = 2$ but $\mu_4 \nsubseteq F$ (i.e. $r = 1$), then, by Proposition 4.2.7, $N_{L/F}(\zeta) \in \{1, -1\}$. Then $d = 1$ or 2, and, in either case, $N_{L/F}(\zeta) = \zeta^{n/d}$. Take $\eta = \zeta$, so $N_{L/F}(\eta) = N_{L/F}(\zeta) = \zeta^{p^{k-r}} = \zeta^{n/d} = \eta^{n/d}$. The first equality in equation (4.2) then follows from Theorem 4.2.4.

If instead $p = 2$ and $\mu_4 \subseteq F$, then $r \geq 2$ and $N_{L/F}(\zeta) = (-1)^{p^{k-r}-1}\zeta^{p^{k-r}} = -\zeta^{p^{k-r}}$ by Proposition 4.2.7. Since $o(\zeta^{p^{k-r}}) = p^r > 2 = o(-1)$, we have $d = o(-\zeta^{p^{k-r}}) = p^r$. Now let $\eta = \zeta^{1+2^{r-1}}$. Since $r \geq 2$, we have $1 + 2^{r-1}$ is odd. Then, $N_{L/F}(\eta) = \Big(N_{L/F}(\zeta)\Big)^{1+2^{r-1}} = (-\zeta^{2^{k-r}})^{1+2^{r-1}} = -\zeta^{2^{k-r}}\zeta^{2^{k-1}} = \zeta^{2^{k-r}}$, as $\zeta^{2^{k-1}} = -1$. So $N_{L/F}(\eta) = \zeta^{2^{k-r}} = \zeta^{n/d}$ and $\eta^{n/d} = \eta^{2^{k-r}} = \zeta^{2^{k-r}(1+2^{r-1})} = -\zeta^{2^{k-r}} = N_{L/F}(\zeta)$, and the first equality in equation (4.2) follows from Theorem 4.2.4.

Finally, the last equality in equation (4.2) is clear when p is odd. If $p = 2$ and $N_{L/F}(\zeta) = 1$, then $r = 1$ (cf. Proposition 4.2.7), whence $1 + 2^{r-1} = 2$, so $\Big(a, b^e; F, \zeta^{p^{k-r}}\Big)_{p^r}$ is split by Proposition 1.2.4.4; this gives the last equality in (4.2) in this case. If $p = 2$ and $r \geq 2$, then $N_{L/F}(\zeta) = -\zeta^{2^{k-r}} = \zeta^{2^{k-r}(1+2^{r-1})}$. Since $(1 + 2^{r-1})^2 \equiv 1 \ mod\ 2^r$, the last equality in equation (4.2) is a consequence of a basic symbol algebra identity (cf. Proposition 1.2.4.3). $\square$

Corollary 4.2.13. *Let $F \subseteq K$ be a finite degree field extension and suppose $\mu_n \subseteq K$ for some n. Then for $a, b \in F^*$ and $\zeta \in \mu_n^*$, we have*

$$\mathrm{cor}_{K/F}\,(a, b; K, \zeta)_n = \big(a, b; F, \eta^{n/d}\big)_d^{[K:F(\mu_n)]},$$

where d is the order of $N_{F(\mu_n)/F}(\zeta)$ and $\eta \in \mu_n^*$ satisfies $N_{F(\mu_n)/F}(\eta) = \zeta^{n/d}$.

Proof. Let $L = F(\mu_n)$. Theorem 4.2.3 tells us that

$$\mathrm{cor}_{K/L}\,(a,b;K,\zeta)_n = (a,b;L,\zeta)_n^{[K:L]}\,.$$

We then apply Theorem 4.2.4 (or the simpler Corollary 4.2.11 if n is a prime power) to get the result. □

The next few results concern cyclic algebras. In Proposition 4.2.15, we see how the corestriction of a symbol algebra is not necessarily another symbol algebra when the smaller field has fewer roots of unity.

Lemma 4.2.14. *Let $F \subseteq L \subseteq M$ be fields where $F \subseteq M$ is cyclic. For any generator σ of $Gal(M/F)$ and any $b \in F$,*

$$\mathrm{cor}_{L/F}(M/L, \sigma^{[L:F]}, b) = (E/F, \sigma|_E, b),$$

where E is determined by $F \subseteq E \subseteq M$ and $[E : F] = [M : L]$.

Proof. By Proposition 1.2.5, $(M/L, \sigma^{[L:F]}, b) = \mathrm{res}_{L/F}(M/F, \sigma, b)$. Because $F \subseteq M$ is cyclic, there is a unique field E satisfying $F \subseteq E \subseteq M$ and $[E : F] = [M : L]$, so, by Proposition 1.2.6, we get

$$\mathrm{cor}_{L/F}(M/L, \sigma^{[L:F]}, b) = \\ \mathrm{cor}_{L/F}\mathrm{res}_{L/F}(M/F, \sigma, b) = (M/F, \sigma, b)^{[L:F]} = (E/F, \sigma|_E, b).$$

□

Proposition 4.2.15. *Let F be a field and p be a prime. If $p = 2$, assume $\mu_4 \subseteq F$. Take $\zeta \in \mu_{p^k}^*$ for some $k \geq 1$ and let $L = F(\zeta)$. Let $\omega \in \mu_{p^\infty}(L)$ and let θ be any p^k-th root of ω. Suppose $\mu_{p^k} \cap F = \mu_{p^r}$ and let $p^l = [L(\theta) : L]$. Then for any $b \in F^*$,*

$$\mathrm{cor}_{L/F}\,(\omega, b; L, \zeta)_{p^k} = (E/F,\ \sigma|_E,\ b)\,,$$

where E is determined by $F \subseteq E \subseteq L(\theta)$ and $[E : F] = p^l$, and σ is a generator of $Gal(L(\theta)/F)$ which satisfies $\sigma^{[L:F]}(\theta) = \zeta^{p^{k-l}}\theta$.

Remark 4.2.16. We show later that we can obtain similar formulas to Proposition 4.2.15 when $p = 2$ and $\mu_4 \not\subseteq F$ (cf. Remark 4.3.10). These formulas, together with the primary decomposition and projection formulas, make it possible to compute $cor_{L/F}(\omega, b; L, \zeta)_n$, where $n \geq 1$, L is any finite degree extension of F, $\omega \in \mu_{p^\infty}(L)$, and $b \in F^*$.

Proof. Let θ be any p^k-th root of ω and set $M = L(\theta) = F(\theta)$. Then $[M : L] = p^l$ for some $l \leq k$. Because, $\mu_{p^k} \subseteq L$, we have M is a p^l-Kummer extension of L. Now M is a cyclotomic extension of F so M is a cyclic extension of F (This uses $\mu_4 \subseteq F$ if $p = 2$). Thus, $Gal(M/F)$ maps onto $Gal(M/L)$ via the $[L : F]$ power map. So there exists a generator, σ, of $Gal(M/F)$ such that $\sigma^{[L:F]}(\theta) = \zeta^{p^{k-l}}\theta$, as $\zeta^{p^{k-l}} \in \mu^*_{p^l}$. So $\sigma^{[L:F]}$ is a generator of $Gal(M/L)$. Then in $Br(L)$,

$$\begin{aligned}(\omega, b; L, \zeta)_{p^k} &= \left(\theta^{p^k}, b; L, \zeta\right)_{p^k} \\ &= \left(\theta^{p^l}, b; L, \zeta^{p^{k-l}}\right)_{p^l} \\ &= (M/L, \sigma^{[L:F]}, b),\end{aligned}$$

where the second equality comes from the symbol algebra identity given in Proposition 1.2.4.4. Apply Lemma 4.2.14 to obtain

$$cor_{L/F}(\omega, b; L, \zeta)_{p^k} = \left(E/F,\ \sigma|_E,\ b\right),$$

where $F \subseteq E \subseteq M$ and $[E : F] = [M : L] = p^l$. Thus, $E = F(\mu_{p^{r+l}})$. □

4.3 Quadratic Corestriction of Characters

In this section, we discuss the corestriction of characters over a separable quadratic extension $L \supseteq F$. Take $\chi \in X(L)$. If $\chi = \chi_1 \dots \chi_k$ is the primary decomposition of χ, then $cor_{L/F}(\chi) = cor_{L/F}(\chi_1) \dots cor_{L/F}(\chi_k)$. Thus, we need only consider the case where $o(\chi) = p^m$, where p is prime. We will only handle the cases where either $L(\chi)$ is Kummer over L (i.e. $\mu_{p^m} \subseteq L$) or $L(\chi)$ is a cyclotomic extension of F.

4.3.1 Case: $L(\chi) \supseteq L$ is a Kummer Extension

Let $M = L(\chi)$ and suppose $\mu_{p^m} \subseteq L$. Let τ generate $Gal(L/F)$. Set $M' = \tau(M)$, $K = MM'$, and $L' = M \cap M'$; we are not ruling out the possibility $M = M'$. Then K is the normal closure of M over F. Set $r = [M : L'] = [M' : L'] = [K : M]$ and $s = [L' : L]$. Then $rs = [M : L] = p^m$ and $r^2 s = [K : L]$.

Suppose that $a \in L^*/L^{*rs}$ generates the Kummer group corresponding to M (so $M = L(\sqrt[rs]{\tilde{a}})$, where $a = \tilde{a}L^{*rs}$). Since $\tau(L^*) \subseteq L^*$ and $\tau(L^{*rs}) \subseteq L^{*rs}$, we have a well-defined action of τ on L^*/L^{*rs}. Set $b = \tau(a)$. Then $\langle a^r \rangle$ and $\langle b^r \rangle$ each correspond to L', whence $\langle a^r \rangle = \langle b^r \rangle$, so $a^{ru} = b^r$ for some u with $u^2 \equiv 1 \ mod\ s$. There are up to four possible values for u determined mod s. We will choose $u \in \mathbb{Z}$ from the set $\{1, -1, 1 + (s/2), -1 + (s/2)\}$ where $u \in \{1 + (s/2), -1 + (s/2)\}$ can only occur if $8 \mid s$. Furthermore, if $s \leq 2$, then we set $u = 1$, and if $s = 4$, then we will choose $u \in \{1, -1\}$. Let E_u be the field corresponding to $\langle a^{-u} b \rangle$ and let $B = \langle a, b \rangle$.

4.3.2 Determining $Gal(K/L)$ and $Gal(K/F)$

Let G denote the abelian group $\mathbb{Z}_{rs} \times \mathbb{Z}_{rs}$ with generators $a_0 = (1, 0)$, $b_0 = (0, 1)$. Make G into a $\langle \tau \rangle$-module by setting $\tau(a_0) = b_0$ and $\tau(b_0) = a_0$. The map $\pi : G \to B$ defined by $\pi(a_0) = a$, $\pi(b_0) = b$ is a $\langle \tau \rangle$-module homomorphism. Let $H = ker(\pi)$. Then $H = \langle a_0^{-ur} b_0^r \rangle$ is a $\langle \tau \rangle$-submodule of G. We have a short exact sequence of

$\langle\tau\rangle$-modules

$$1 \longrightarrow H \xrightarrow{\iota} G \xrightarrow{\pi} B \longrightarrow 1.$$

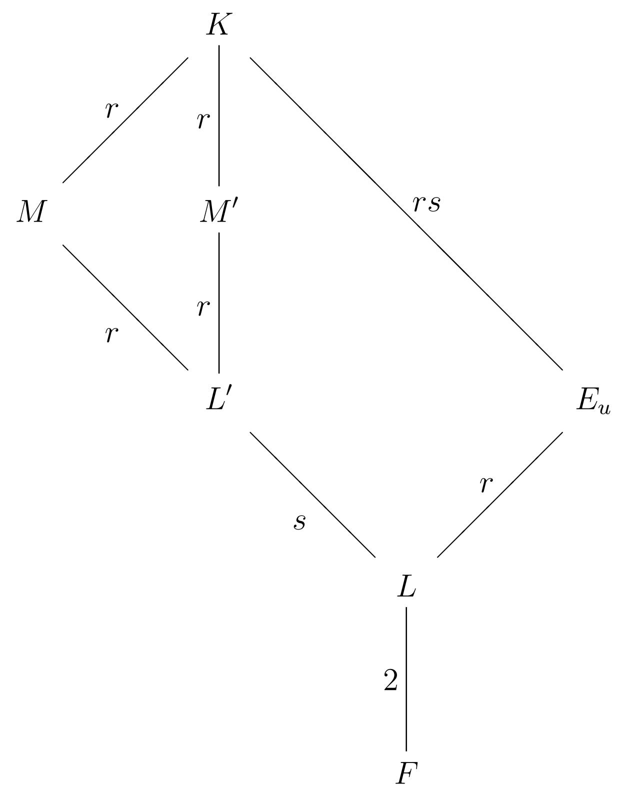
For A, an abelian group, let $A^* = Hom(A, \mu_{rs})$. If A is a $\langle\tau\rangle$-module, we may make A^* into a $\langle\tau\rangle$-module by setting $(\tau\cdot\gamma)(g) = \tau(\gamma(\tau^{-1}(g)))$ for $\gamma \in A^*$ and $g \in A$. Applying $Hom(-, \mu_{rs})$ to the previous sequence, we obtain

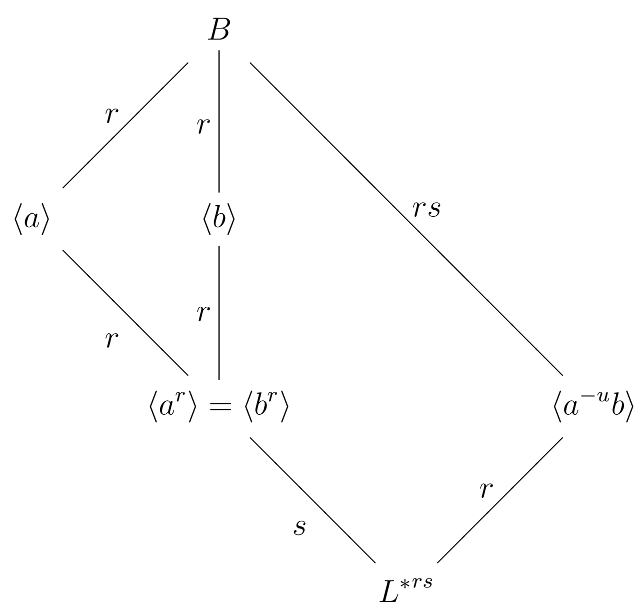
$$1 \longrightarrow B^* \xrightarrow{\pi^*} G^* \xrightarrow{\iota^*} H^* \longrightarrow 1 \qquad (\dagger)$$

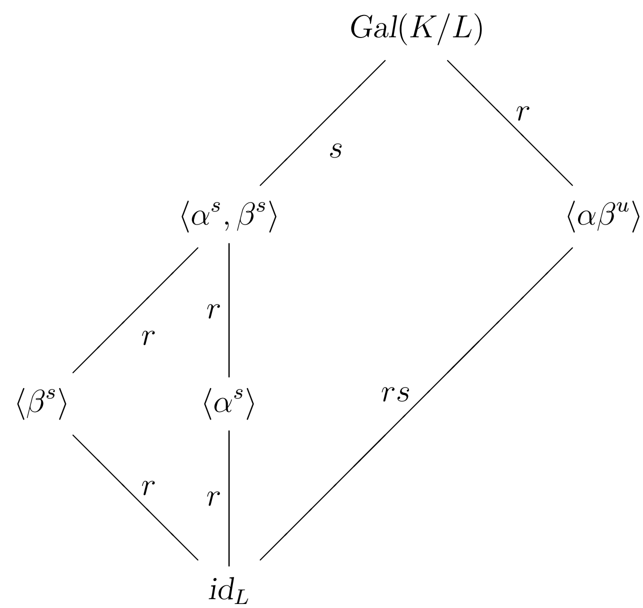
This last sequence is exact. For, we can identify μ_{rs} with a subgroup of $\mathbb{Q}/\mathbb{Z}$;, then the exactness follows from [Rot79, Lemma 3.51] as G is rs-torsion. (Alternatively, we could apply the Fundamental Theorem of Modules over a PID to see $|B^*| = |B|$, $|G^*| = |G|$, $|H^*| = |H|$. Together with the left exactness of $Hom(-, \mu_{rs})$, this gives exactness at the right end in (†).) One checks easily that π^* and ι^* are each $\langle\tau\rangle$-module homomorphisms. Fix $\zeta_{rs} \in \mu_{rs}^*$ and define $\alpha, \beta \in G^*$ by $\alpha(a_0) = \zeta_{rs}$, $\alpha(b_0) = 1$ and $\beta(a_0) = 1$, $\beta(b_0) = \zeta_{rs}$ (i.e. $\{\alpha, \beta\}$ is dual to $\{a_0, b_0\}$). Then $\{\alpha, \beta\}$ generates G^* as an abelian group (and as a free $\mathbb{Z}_{rs}$-module).

Suppose $\tau(\zeta_{rs}) = \zeta_{rs}^v$. Since $\mu_{rs} \subseteq L$ and $\tau \in Gal(L/F)$ has order 2, we must have $v^2 \equiv 1 \ mod \ rs$. Again, there are up to four possible values of v determined mod rs. We will choose $v \in \mathbb{Z}$ in the same manner that we chose u, i.e. from the set $\{1, -1, 1 + \frac{rs}{2}, -1 + \frac{rs}{2}\}$ with $v \in \{1 + \frac{rs}{2}, -1 + \frac{rs}{2}\}$ occurring only if $8 \mid rs$. Then $(\tau\cdot\alpha)(a_0) = \tau\alpha\tau^{-1}(a_0) = \tau\alpha(b_0) = 1$ and $(\tau\cdot\alpha)(b_0) = \tau\alpha\tau^{-1}(b_0) = \tau\alpha(a_0) = \tau(\zeta_{rs}) = \zeta_{rs}^v$, whence $\tau(\alpha) = \beta^v$. Similarly, $\tau(\beta) = \alpha^v$.

Note that $B^* = \{\alpha^i\beta^j : \iota^*(\alpha^i\beta^j) = 1\} = \{\alpha^i\beta^j : \alpha^i\beta^j(a_0^{-ur}b_0^r) = 1\} = \{\alpha^i\beta^j : j \equiv iu \ mod \ s\}$. The last equality holds because $\alpha^i\beta^j(a_0^{-ur}b_0^r) = \zeta_{rs}^{r(j-iu)}$, whence $\alpha^i\beta^j(a_0^{-ur}b_0^r) = 1$ if and only if $rs \mid r(j - iu)$, i.e. $s \mid j - iu$. So B^* is generated as a group by $\{\alpha^s, \beta^s, \alpha\beta^u\}$. Since B is the Kummer subgroup of L^*/L^{*rs} corresponding to K, we will identify B^* with $Gal(K/L)$. We get the following diagrams of fields, Kummer groups, and Galois groups.


K
r
r
r
rs
M
M'
r
r
L'
E_u
s
r
L
2
F


B
r
r
rs
$\langle a \rangle$
$\langle b \rangle$
r
r
$\langle a^r \rangle = \langle b^r \rangle$
$\langle a^{-u} b \rangle$
s
r
L^{*rs}



Now, we wish to describe $Gal(K/F)$ as an extension of $Gal(K/L)$ by $\langle \tau \rangle$. These extensions are classified by $H^2(\langle \tau \rangle, B^*)$.

For A, a $\langle \tau \rangle$-module, we define $N(a) = \tau(a)a$ for $a \in A$, $N(A) = \{N(a) : a \in A\}$, and $A^\tau = \{a \in A : \tau(a) = a\}$. Also, we will abbreviate $H^2(\langle \tau \rangle, A)$ to $H^2(A)$. By [Rot79, Theorem 10.35], $H^2(A) \cong A^\tau / N(A)$.

Returning to B^*, recall that $B^* = \langle \alpha^s, \beta^s, \alpha\beta^u \rangle = \langle \alpha^s, \alpha\beta^u \rangle$. Thus, $N(B^*) = \langle (\alpha\beta^v)^s, \alpha^{uv+1}\beta^{u+v} \rangle$. Since $v(uv+1) \equiv u+v \ mod\, rs$, we have $\alpha^{uv+1}\beta^{u+v} = (\alpha\beta^v)^{uv+1}$, whence

$$N(B^*) = \langle (\alpha\beta^v)^d \rangle, \qquad \text{where } d = gcd(s, uv+1).$$

Also, $B^{*\tau} = B^* \cap G^{*\tau} = B^* \cap \langle \alpha\beta^v \rangle$. Set $e = s/gcd(s, u-v)$. Since u is a unit mod s, we have $gcd(s, u-v) = gcd(s, u(u-v)) = gcd(s, u^2 - uv) = gcd(s, 1-uv)$. Thus, $e = s/gcd(s, 1-uv)$. Since $\langle (\alpha\beta^v)^s \rangle \subseteq B^{*\tau}$, we may ask if there is an $i < s$ with $(\alpha\beta^v)^i \in B^{*\tau}$. If so, then necessarily $(\alpha\beta^v)^i = (\alpha\beta^u)^i \beta^{sk}$ for some k. Comparing exponents of β on both sides shows $s \mid (v-u)i$, or $e \mid i$. Thus, $B^{*\tau} \subseteq \langle (\alpha\beta^v)^e \rangle$. On the other hand, $(v-u)e = (v-u)s/gcd(s, u-v) \in s\mathbb{Z}$, so $(\alpha\beta^v)^e = (\alpha\beta^u)^e \beta^{(v-u)e} \in B^{*\tau}$, whence,

$$B^{*\tau} = \langle (\alpha\beta^v)^e \rangle, \qquad \text{where } e = gcd(s, uv-1).$$

Theorem 4.3.1. *We have the following table for* $B^{*\tau}, N(B^*)$, *and* $|H^2(B^*)|$

s	uv mod s	e	$B^{*\tau}$	d	$N(B^*)$	$\|H^2(B^*)\|$
s, *odd*	1	1	$\langle\alpha\beta^v\rangle$	1	$\langle\alpha\beta^v\rangle$	1
s, *even*	1	1	$\langle\alpha\beta^v\rangle$	2	$\langle(\alpha\beta^v)^2\rangle$	2
s, *odd*	-1	s	$\langle(\alpha\beta^v)^s\rangle$	s	$\langle(\alpha\beta^v)^s\rangle$	1
s, *even*	-1	$s/2$	$\langle(\alpha\beta^v)^{s/2}\rangle$	s	$\langle(\alpha\beta^v)^s\rangle$	2
$8 \mid s$	$1+\frac{s}{2}$	2	$\langle(\alpha\beta^v)^2\rangle$	2	$\langle(\alpha\beta^v)^2\rangle$	1
$8 \mid s$	$-1+\frac{s}{2}$	$s/2$	$\langle(\alpha\beta^v)^{s/2}\rangle$	$s/2$	$\langle(\alpha\beta^v)^{s/2}\rangle$	1

Proof. Case $uv \equiv 1$ *mod* s

In this case, $d = gcd(s, uv+1) = gcd(s, 2)$ and $e = s/gcd(s, 1-uv) = s/gcd(s, 0) = s/s = 1$. If s is odd, then $d = 1$ and $e = 1$, whence $N(B^*) = \langle\alpha\beta^v\rangle = B^{*\tau}$ and $|H^2(B^*)| = 1$. On the other hand, if s is even, then $d = 2$ and $e = 1$ so $N(B^*) = \langle(\alpha\beta^v)^2\rangle$, $B^{*\tau} = \langle\alpha\beta^v\rangle$ and $|H^2(B^*)| = 2$.

Case $uv \equiv -1$ *mod* s

In this case, $d = gcd(s, uv + 1) = gcd(s, 0) = s$ and $e = s/gcd(s, 1 - uv) = s/gcd(s, 2)$. If s is odd, then $d = s = e$, whence $N(B^*) = \langle(\alpha\beta^v)^s\rangle = B^{*\tau}$ and $|H^2(B^*)| = 1$. On the other hand, if s is even, then $d = s$, but $e = s/2$ so $N(B^*) = \langle(\alpha\beta^v)^s\rangle$, $B^{*\tau} = \langle(\alpha\beta^v)^{s/2}\rangle$ and $|H^2(B^*)| = 2$.

Case $uv \equiv 1 + (s/2)$ *mod* s*;* $8 \mid s$

In this case, $d = gcd(s, uv+1) = gcd(s, 2+(s/2)) = 2$ and $e = s/gcd(s, 1-uv) = s/gcd(s, s/2) = 2$. Thus, $N(B^*) = \langle(\alpha\beta^v)^2\rangle = B^{*\tau}$ and $|H^2(B^*)| = 1$.

Case $uv = -1 + (s/2)$ *mod* s*;* $s \mid 8$

In this case, $d = gcd(s, uv + 1) = gcd(s, s/2) = s/2$ and $e = s/gcd(s, 1 - uv) = s/gcd(s, 2 - (s/2)) = s/2$. Thus, $N(B^*) = \langle(\alpha\beta^v)^{s/2}\rangle = B^{*\tau}$ and $|H^2(B^*)| = 1$. □

Let $1 \to B^* \to \Gamma_{uv,f} \to \langle\tau\rangle \to 1$ be the group extension corresponding to uv and a choice of $f \in H^2(B^*)$. We will write $H^2(B^*)$ multiplicatively. So $f \in \{-1, 1\}$ as $|H^2(B^*)| \leq 2$. Let $\overline{\tau}$ be any preimage of τ in $\Gamma_{uv,f}$. Since τ has order 2, we must have

$\overline{\tau}^2 \in B^* \cap (\Gamma_{uv,f})^\tau = B^{*\tau}$. If $f = 1$, then $\overline{\tau}^2 \in N(B^*)$ (cf. [Rot79, Th. 5.6ii, Cor 5.8]; if [,] is the factor set corresponding to the lift $\tau \mapsto \overline{\tau}$, then $[\tau, \tau] = \overline{\tau}^2 = \tau(c)c$ for some $c \in B^*$.) So whenever $f = 1$, we may choose $\overline{\tau}$ so that $\overline{\tau}^2 = 1$ (cf. [Rot79, Cor. 5.8]), and $\Gamma_{uv,f}$ is a semi-direct product. However, if $f \neq 1$, then $\overline{\tau}^2 \notin N(B^*)$, but $(\overline{\tau}^2)^2 = \overline{\tau}\overline{\tau}^2\overline{\tau}^{-1}\overline{\tau}^2 = \tau(\overline{\tau}^2) \cdot \overline{\tau}^2 \in N(B^*)$. Finally, in all cases, $\Gamma_{uv,f} = B^* \cup \overline{\tau}B^*$, so every element $g \in \Gamma_{uv,f}$ has the form $\overline{\tau}^i c$, where $c \in B^*$ and $i \in \{0, 1\}$.

Remark 4.3.2. We can compute u, v, and f (and hence $Gal(K/F)$) by the action of τ on L. Recall that $\tau(a^r) = (a^r)^u$ and $\tau(\zeta_{rs}) = \zeta_{rs}^v$. We saw in Theorem 4.3.1 that $f \in \{1, -1\}$ and $f = -1$ can only occur when $uv \equiv \pm 1$ *mod* rs and $2 \mid s$. The next proposition distinguishes which of the two values of f occurs.

Proposition 4.3.3. *Let* $a_1 \in L^*$ *be any pre-image of* $a \in L^*/L^{*rs}$. *Suppose that* $Gal(K/F) \cong \Gamma_{uv,f}$. *Then*

1. *There exists* $y \in L^*$ *such that* $y^s a_1^u = \tau(a_1)$.
2. $f = 1$ *if and only if* $a_1^{(u^2-1)/s} y^u \tau(y) \in \mu_{s/d}$ *(for any* y *from 1.), where* $d = gcd(s, u + v)$

Remark 4.3.4. If y_1, y_2 each satisfy $y_i^s a_1^u = \tau(a_1)$, then $y_1 = \zeta y_2$ for some $\zeta \in \mu_s$. Then $a_1^{(u^2-1)/s} y_1^u \tau(y_1) = a_1^{(u^2-1)/s} y_2^u \tau(y_2) \zeta^u \tau(\zeta) = a_1^{(u^2-1)/s} y_2^u \tau(y_2) \zeta^{u+v}$. Note that $o(\zeta^{u+v}) \mid s/d$, where $d = gcd(s, u + v)$, i.e. $\zeta^{u+v} \in \mu_{s/d}$, so the condition in 2. is independent of the choice of y.

Remark 4.3.5. The first step in the proof of Proposition 4.3.3 is to reduce to $Gal(L'/F)$. This reduction can be viewed homologically. Let A be the Kummer group corresponding to L'. Set $C = B/A \cong \mathbb{Z}_r \times \mathbb{Z}_r$ and we get the short exact sequence $1 \to A \to B \to C \to 1$. Apply $Hom(-, \mu_{rs})$ to the sequence, and we obtain $1 \to C^* \to B^* \to A^* \to 1$. We can show that $H^2(C^*) = 1$, whence, $H^2(B^*) \cong H^2(A^*)$. Thus, we can compute f by looking at the corresponding extension of A^*, i.e. $Gal(L'/F)$.

After this reduction, we could just apply [HLW03, Theorem 3.4(3)] to get the result, since L' is now a Kummer extension of L which is Galois over F.

Proof. Note that $f = 1$ if and only if there is an extension $\overline{\tau}$ of τ to $Gal(K/F)$ such that $\overline{\tau}$ has order 2. This condition is equivalent to $\overline{\tau}^2|_{L'} = id_{L'}$. For, suppose $\overline{\tau}$ is any extension of τ. If $\overline{\tau}^2|_{L'} = id_{L'}$, then $\overline{\tau}^2 \in \langle \alpha^s, \beta^s \rangle$ and $\overline{\tau}^2 \in \langle \alpha\beta^v \rangle$. Thus, $\overline{\tau}^2 \in \langle (\alpha\beta^v)^s \rangle \subseteq N(B^*)$, i.e. $f = 1$. On the other hand, if $f = 1$, then there is an extension of $\overline{\tau}$ of τ with $\overline{\tau}^2 = id_K$, so $\overline{\tau}^2|_{L'} = id_{L'}$.

Recall that u was defined by $a^{ru} = \tau(a^r) \in L^*/L^{*rs}$. Then there exists $y_0 \in L^*$ such that $y_0^{rs} a_1^{ru} = \tau(a_1^r)$. Taking r-th roots, we obtain $y_0^s \omega a_1^u = \tau(a_1)$ for some $\omega \in \mu_r(L)$. But $\mu_{rs} \subseteq L$ by assumption, so $y_0^s \omega = y^s$ for some $y \in L^*$. This proves 1.

Now suppose $\theta \in L'$ is any s-th root of a_1. Note that $L' = L(\theta)$. Let $\overline{\tau}$ be an extension of τ to L'. By part 1., we obtain $\overline{\tau}(\theta)^s = y^s a_1^u$ for some $y \in L^*$. Note that $\overline{\tau}$ is completely determined by its action on θ as $L' = F(\theta)$. Pick an arbitrary $\zeta \in \mu_s$. Then,

$$\overline{\tau}_\zeta(\theta) = y\theta^u\zeta$$

defines an extension of τ to L'; note that $[L' : L] = s$, so by Galois theory, there are s distinct extensions of τ to L'. We observed that $f = 1$ if and only if there exists a ζ such that $\overline{\tau}_\zeta^2$ is trivial on L' (i.e. $\overline{\tau}_\zeta^2(\theta) = \theta$). Applying $\overline{\tau}_\zeta$ to the displayed equation above gives

$$\overline{\tau}_\zeta^2(\theta) = \overline{\tau}_\zeta(y)\overline{\tau}_\zeta(\theta)^u\overline{\tau}_\zeta(\zeta) = \tau(y)(y\theta^u\zeta)^u\zeta^v.$$

Then $\overline{\tau}_\zeta^2(\theta)/\theta = \tau(y)y^u\theta^{u^2-1}\zeta^{u+v}$. Note that $u^2 \equiv 1 \ mod\ s$, so $(u^2-1)/s \in \mathbb{Z}$. Hence, $f = 1$ if and only if there exists a $\zeta \in \mu_s$ such that $1 = \tau(y)y^u\theta^{u^2-1}\zeta^{u+v}$, i.e. $\zeta^{-u-v} = a_1^{(u^2-1)/s}\tau(y)y$. Now $-u-v$ has order $d = gcd(s, u+v)$ in $\mathbb{Z}_s$, so $\mu_s^{u+v} = \mu_{s/d}$. Therefore, $f = 1$ if and only if $a_1^{(u^2-1)/s}\tau(y)y \in \mu_{s/d}$. □

4.3.3 Corestriction in the Kummer Extension Case

We continue to assume $\chi \in X(L)$ with $M = L(\chi)$ and $|\chi| = [M : L] = rs$, where r, s are both powers of p, a prime number. View $\chi : Gal(K/L) \to \mathbb{Z}_{rs}$. We identify τ with a fixed preimage of τ in $\Gamma_{uv,f}$. Then $\{1, \tau\}$ maps to a complete set of coset representatives of $Gal(K/L)$ in $Gal(K/F)$. Let $\chi' = cor_{L/F}(\chi)$. For $\sigma \in Gal(K/F)$, Proposition 1.6.4 (=[Mer85, 1.3]) says that $\chi'(\sigma) = \sum_{i \in \{\tau,1\}} \chi(i\sigma i_1^{-1})$, where $i_1 \in \{\tau, 1\}$ is chosen so that $i\sigma i_1^{-1} \in Gal(K/L)$. This gives us the two equations, for $c \in Gal(K/L)$

$$\chi'(c) = \chi(\tau c \tau^{-1}) + \chi(c) \tag{4.3}$$

$$\chi'(\tau c) = \chi(\tau\tau c) + \chi(\tau c \tau^{-1}) \tag{4.4}$$

$$= \chi(\tau^2) + \chi'(c).$$

Recall that, for $k \in K$, $\tau c \tau^{-1}(k) = \tau \cdot c(k)$, so $\chi'(c) = \chi(N(c))$ (where N is the $\langle\tau\rangle$-module norm on B^*). Now $B^* \cong Gal(K/L)$ via the correspondence $\sigma \mapsto \begin{cases} \sqrt[rs]{a} \mapsto \sigma(a) \sqrt[rs]{a} \\ \sqrt[rs]{b} \mapsto \sigma(b) \sqrt[rs]{b}. \end{cases}$. We use this isomorphism to identify $Gal(K/L)$ with B^*. Since $M = L(\sqrt[rs]{a})$, $\sigma|_M$ is determined by $\sigma(a)$. Let $\zeta_{rs} = \sigma_\chi(a)/a \in \mu_{rs}^*$. Identify μ_{rs} with $\mathbb{Z}_{rs}$ via $\zeta_{rs} \leftrightarrow 1$. Then $\chi(\alpha^i\beta^j) = i$, as $\alpha^i\beta^j(a) = i$. Let $\tau^2 = (\alpha\beta^v)^l$. Using equation (4.3), we have,

$$\chi'(\alpha\beta^u) = \chi(\alpha^{uv}\beta^v) + \chi(\alpha\beta^u) = uv + 1 \tag{4.5}$$

$$\chi'(\alpha^s) = \chi(\beta^{sv}) + \chi(\alpha^s) = s$$

$$\chi'(\beta^s) = \chi(\alpha^{sv}) + \chi(\beta^s) = sv$$

$$\chi'(\tau) = \chi(\tau^2) = l$$

Since $\Gamma_{uv,f}$ is generated by $\alpha\beta^u, \alpha^s$, and τ, it is enough to compute $\chi'(\alpha\beta^u), \chi'(\alpha^s)$, and $\chi'(\tau)$ to determine $im(\chi')$. Set $d = gcd(uv+1, s)$. Because $v^2 \equiv 1 \; mod \; s$, we have $d = gcd(uv+1, s) = gcd((uv+1)v, s) = gcd(u+v, s)$. Also, set $g = s/gcd(s, u+v) = s/d$. We next determine the orders of $\chi'(\alpha\beta^u), \chi'(\alpha^s), \chi'(\tau)$.

Let us make a convention about choosing extensions of τ. Whenever $f = 1$, i.e. $\Gamma_{uv,f}$ is a semi-direct product, we will choose τ such that $\tau^2 = 1$. In this case, $l = 0$, so $\chi'(\tau) = 0$ and $|\chi'(\tau)| = 1$. On the other hand, if $f = -1$, we know from Theorem 4.3.1 that $\tau^2 \in (\alpha\beta^v)^{d/2}\langle(\alpha\beta^v)^d\rangle$. In this case, we choose τ such that $\tau^2 = (\alpha\beta^v)^{d/2}$, whence $l = d/2$, so $\chi'(\tau) = d/2$ and $|\chi'(\tau)| = rs/(d/2) = 2rs/d = 2rg$.

Since $\chi'(\alpha^s) = s$, we always have $|\chi'(\alpha^s)| = r$. Now either $d = s$ or $d \neq s$. If $d \neq s$, then d and $uv+1$ generate the same ideal in $\mathbb{Z}_s$ and in $\mathbb{Z}_{rs}$. Thus, there is a q prime to rs such that $q(uv+1) \equiv d \; mod \; rs$. Then,

$$\chi'((\alpha\beta^u)^q) = q(uv+1) \equiv d \; mod \; rs. \tag{4.6}$$

Finally, if $d \neq s$, then $\chi'(\alpha\beta^u) = uv+1$ has order $g = s/d > 1$ in $\mathbb{Z}_s$, whence $\chi'(\alpha\beta^u)$has order rg in $\mathbb{Z}_{rs}$. Also, $d = s$ if and only if $g = 1$ and $d \neq s$ if and only if $g > 1$ (as $g = s/d$).

Now $(u+v)g = (u+v)s/gcd(u+v,s) \in s\mathbb{Z}$, so $(\alpha\beta^{-v})^g = (\alpha\beta^u)^g\beta^{-(u+v)g} = (\alpha\beta^u)^g(\beta^s)^{-(u+v)g/s} \in B^*$. So, by (4.5), $\chi'((\alpha\beta^{-v})^g) = \chi'((\alpha\beta^u)^g(\beta^s)^{-(u+v)g/s}) = g(uv+1) - (u+v)gvs \equiv 0 \; mod \; rs$, since $v^2 \equiv 1 \; mod \; rs$. Thus, $\langle(\alpha\beta^{-v})^g\rangle \subseteq ker(\chi')$. Since g is a divisor of s, we have $|(\alpha\beta^{-v})^g| = rs/g$. Also, whenever $f = 1$, we have $\tau^2 = 1$ and $\tau \in ker(\chi')$. Now $Gal(K/F)$ has order $2r^2s$, so $|ker(\chi')| = 2r^2s/|\sigma_{\chi'}|$. This gives us the following chart for the orders of $\chi'(\alpha\beta^u), \chi'(\alpha^s), \chi'(\tau), \sigma_{\chi'}$, and $ker(\chi')$. To avoid extra subscripts, we give $\sigma_{\chi'}$ in terms of an element in $Gal(K/F)$ instead of its restriction to $F(\chi')$.

	$f = 1$		$f = -1$	
	$g = 1$	$g > 1$	$g = 1$	$g > 1$
$\lvert\chi'(\alpha\beta^u)\rvert$	$\leq r$	rg	$\leq r$	rg
$\lvert\chi'(\alpha^s)\rvert$	r	r	r	r
$\lvert\chi'(\tau)\rvert$	0	0	$2r$	$2rg$
$\sigma_{\chi'}$	α^s	$(\alpha\beta^u)^q$	τ	τ
$\lvert\chi'\rvert$	r	rg	$2r$	$2rg$
$ker(\chi')$	$\langle\tau, \alpha\beta^{-v}\rangle$	$\langle\tau, (\alpha\beta^{-v})^g\rangle$	$\langle\alpha\beta^{-v}\rangle$	$\langle(\alpha\beta^{-v})^g\rangle$

This shows that χ' depends completely on the cocycle class f and the constant g, which is determined by $uv+1$ and s. We may translate this information to see what happens to χ' depending on $Gal(K/F)$ and s.

Theorem 4.3.6. *We have the following data on χ' for corresponding values of s, uv and cocycle class $f \in H^2(B^*)$*

$Gal(K/F)$	s	τ^2	$\sigma_{\chi'}$	$\lvert\chi'\rvert$	$ker(\chi')$
$\Gamma_{1,1}$	$s \leq 2$	1	α^s	r	$\tau, \alpha\beta^{-v}$
$\Gamma_{1,1}$	s, *odd and* $s \geq 3$	1	$(\alpha\beta^u)^q$	rs	$\langle\tau, \alpha\beta^{-v}\rangle$
$\Gamma_{1,1}$	s, *even and* $s \geq 4$	1	$(\alpha\beta^u)^q$	$\frac{rs}{2}$	$\langle\tau, (\alpha\beta^{-v})^{s/2}\rangle$
$\Gamma_{1,-1}$	s, *even*	$\alpha\beta^v$	τ	rs	$\langle(\alpha\beta^{-v})^{s/2}\rangle$
$\Gamma_{-1,1}$	*any* s	1	α^s	r	$\langle\tau, \alpha\beta^{-v}\rangle$
$\Gamma_{-1,-1}$	s, *even*	$(\alpha\beta^v)^{s/2}$	τ	$2r$	$\langle\alpha\beta^{-v}\rangle$
$\Gamma_{1+(s/2),1}$	$s \geq 8$	1	$(\alpha\beta^u)^{q_1}$	$\frac{rs}{2}$	$\langle\tau, (\alpha\beta^{-v})^{s/2}\rangle$
$\Gamma_{-1+(s/2),1}$	$s \geq 8$	1	$(\alpha\beta^u)^{q_2}$	$2r$	$\langle\tau, (\alpha\beta^{-v})^2\rangle$

where, for $d = gcd(uv + 1, s)$, we have $(uv + 1)q \equiv d \ mod \ rs$.

Proof. We need only compute g for each case. Note that if $f = -1$, then the result is essentially independent of g; we always have $\sigma_{\chi'} = \tau$, $|\chi'| = 2rg$ and $ker(\chi') = \langle(\alpha\beta^{-v})^g\rangle$. We know from Theorem 4.3.1 that s is even and $uv \equiv \pm 1 \ mod \ s$. If $uv \equiv 1 \ mod \ s$, then $uv + 1 \equiv 2 \ mod \ s$ and $d = 2$, $g = s/2$. If $uv \equiv -1 \ mod \ s$, then $s \mid uv + 1$, so $d = s$ and $g = 1$. This handles all the cases where $f = -1$.

Suppose first that $Gal(K/F) \cong \Gamma_{1,1}$, i.e. $uv \equiv 1 \ mod \ s$ and $f = 1$. If $s \leq 2$, then $uv + 1 \equiv 0 \ mod \ s$, whence $d = s$ and $g = 1$. If $s \geq 3$ and s is odd, then $uv + 1$ is prime to s, whence $d = 1$ and $g = s$. If $s \geq 4$ and s is even, then $uv + 1 \equiv 2 \ mod \ s$, whence $d = 2$ and $g = s/2$.

Next, suppose $Gal(K/F) \cong \Gamma_{-1,1}$, i.e. $uv \equiv -1 \ mod \ s$. Then $s \mid uv + 1$, so $d = s$ and $g = 1$.

Next, suppose $Gal(K/F) \cong \Gamma_{1+(s/2),1}$, i.e. $uv \equiv 1 + (s/2) \ mod \ s$. By Theorem 4.3.1, we must have $8 \mid s$. Also, $uv + 1 \equiv 2 + (s/2) \ mod \ s$ so $d = 2$ and $g = s/2$.

Finally, suppose $Gal(K/F) \cong \Gamma_{-1+(s/2),1}$, i.e. $uv \equiv -1 + (s/2) \ mod \ s$. By Theorem 4.3.1, we must have $8 \mid s$. Also, $uv + 1 \equiv s/2 \ mod \ s$ so $d = s/2$ and $g = 2$. □

4.3.4 Case: $L(\chi) \supseteq L$ is a 2-ary Cyclotomic Extension

We continue to assume that L is a separable quadratic extension of F. Suppose now that $L(\chi) = F(\mu_{2^\alpha})$ for some α and χ has order 2^m for some $m \geq 1$. If $\mu_4 \subseteq F$, then $L(\chi)$ is cyclic over F so χ is in the image of $res_{L/F}$ so the corestriction is easy to compute (cf. Proposition 4.3.7 below). Thus, we may assume $\mu_4 \nsubseteq F$ and $L = F(\mu_4)$. Let $M = L(\chi)$ so $[M : L] = 2^m$, where $m \geq 1$. We will first give a condition on when M is cyclic over F. (If M is not cyclic over F, then necessarily, $Gal(M/F) \cong Gal(M/L) \times \mathbb{Z}_2$). This condition is most likely well-known, but the author is unaware of a reference.

Proposition 4.3.7. *Let $F \subseteq E$ be fields with $\chi \in X(E)$. Suppose $E(\chi)$ is a cyclic extension of F. Let $\chi' = cor_{E/F}(\chi)$. Let σ be a generator of $Gal(E(\chi)/F)$ such that $\sigma_\chi = \sigma^{[E:F]}$. Then, $F(\chi')$ is the field determined by $F \subseteq F(\chi') \subseteq E(\chi)$ and $[F(\chi') : F] = [E(\chi) : E]$. Also, $\sigma_{\chi'} = \sigma|_{F(\chi')}$.*

Proof. Define $\chi_0 \in X(E(\chi)/F)$ by $\chi_0(\sigma) = 1/[E(\chi) : F] \in \mathbb{Q}/\mathbb{Z}$, where σ is defined in the statement of the Proposition. Then $res_{E/F}(\chi_0) = \chi$ since $res_{E/F}(\chi_0)(\sigma_\chi) = [E : F]/[E(\chi) : F] = 1/[E(\chi) : E]$. So $\chi' = cor_{E/F}(\chi) = cor_{E/F} res_{E/F}(\chi_0) = [E : F]\chi_0$. Thus, χ' has order $[E(\chi) : F]/[E : F] = [E(\chi) : E]$. Since $E(\chi)$ is cyclic over F, this shows that $F(\chi')$ is the field determined by $F \subseteq F(\chi') \subseteq E(\chi)$ and $[F(\chi') : F] = [E(\chi) : E]$. Finally, $\chi'(\sigma) = [E : F]\chi_0(\sigma) = 1/[E(\chi') : E] = 1/[F(\chi') : F]$, which shows $\sigma_{\chi'} = \sigma|_{F(\chi')}$. □

Define k by $\mu_{2^\infty} \cap L = \mu_{2^k}$. Note that $k \geq 2$ as $\mu_4 \subseteq L$. Since $[M : L] = 2^r$, we have $M = L(\mu_{2^{k+r}})$. Take $\zeta \in \mu^*_{2^{k+r}}$. The minimal polynomial of ζ over L is $x^{2^r} - \zeta^{2^r}$. Let τ generate $Gal(L/F)$ and let f be the minimal polynomial of ζ over F. Then $f = (x^{2^r} - \zeta^{2^r})(x^{2^r} - \tau(\zeta^{2^r}))$.

We may realize $Gal(M/F)$ as a group extension of $Gal(M/L)$ by $\langle\tau\rangle$, i.e. there is a short exact sequence of $\langle\tau\rangle$-modules $1 \to Gal(M/L) \to Gal(M/F) \to \langle\tau\rangle \to 1$. It is enough to check whether τ has a lift $\overline{\tau} \in Gal(M/F)$ such that $\overline{\tau}$ has order 2. If a lift exists, then the extension is split and $Gal(M/F) \cong Gal(M/L) \times \mathbb{Z}_2$. Otherwise $Gal(M/F)$ is cyclic.

Proposition 4.3.8. *M is cyclic over F if and only if $N_{M/F}(\zeta) = -1$.*

Proof. Note that $N_{M/F}(\zeta) = N_{L/F}(\zeta^{2^r})$. For, by Proposition 4.2.7, $N_{M/L}(\zeta) = -\zeta^{2^r}$; the equality then follows because $N_{L/F}(-1) = 1$. By the same proposition, $N_{M/F}(\zeta) \in \{1, -1\}$.

If $N_{L/F}(\zeta^{2^r}) = 1$, then $\tau(\zeta^{2^r}) = \zeta^{-2^r}$, whence $f = (x^{2^r} - \zeta^{2^r})(x^{2^r} - \zeta^{-2^r}))$ and $f(\zeta^{-1}) = 0$. So $\overline{\tau} : \zeta \mapsto \zeta^{-1}$ is an element of $Gal(M/L)$ extending τ with order 2, whence $Gal(M/F)$ is not cyclic.

On the other hand, if $N_{L/F}(\zeta^{2^r}) = -1$, then $\tau(\zeta^{2^r}) = -\zeta^{-2^r}$. If $k = 2$, then $\zeta^{2^r} \in \mu_{2^k} = \mu_4^*$, whence $\zeta^{2^r} = -\zeta^{-2^r}$. Since we assumed that τ is non-trivial, we must have $k \neq 2$, i.e. $k \geq 3$. Let $\overline{\tau}$ be any extension of τ to M. Then $\overline{\tau}(\zeta^{2^r}) = -\zeta^{-2^r}$ implies that, for some $\omega \in \mu^*_{2^{r+1}}$, we have $\overline{\tau}(\zeta) = \omega\zeta^{-1}$. Since $\mu_{2^{r+1}} = \langle \zeta^{2^{k-1}} \rangle$, there is an odd $m \in \mathbb{Z}$ with $\omega = \zeta^{2^{k-1}m}$. So, $\overline{\tau}(\zeta) = \zeta^{2^{k-1}m-1}$, hence, $\overline{\tau}^2(\zeta) = \zeta^{(2^{k-1}m-1)^2} = \zeta^{2^{2k-2}m^2-2^km+1}$. We see that $\overline{\tau}$ has order 2 if and only if $2^{2k-2}m^2 - 2^km \equiv 0 \ mod\ 2^{r+k}$, i.e. $2^{k-2}m - 1 \equiv 0 \ mod\ 2^r$, since m is odd. But $k \geq 3$ and $r \geq 1$ by assumption, so 2^{k-2} is even. Thus, there is no possible choice of m satisfying the last condition and τ has no lift of order 2. So M is cyclic over F. $\square$

Now, if M is cyclic over F, then $cor_{L/F}(\chi)$ has already been handled in Proposition 4.3.7 above. So we may assume that $Gal(M/F)$ is not cyclic. Identify τ with an extension to M which has order 2. Then $Gal(M/F) = \langle \sigma_\chi, \tau \rangle$ where σ_χ generates $Gal(M/L)$ and has order $[M : L]$. Let $\chi' = cor_{L/F}(\chi)$.

Theorem 4.3.9. *$\chi' \in X(F)$ has order 2^{r-1} and $ker(\chi') = \langle \tau, \sigma^{2^{r-1}} \rangle$. Also, $\sigma_{\chi'} = \sigma_\chi|_{F(\chi')}$.*

Proof. Note that $\{1, \tau\}$ is a complete set of coset representatives of $Gal(M/L)$ in

Gal(M/F). Using Proposition 1.6.4 ([Mer85, 1.3]), we see

$$\begin{aligned}\chi'(\sigma_\chi) &= \chi(\tau\sigma_\chi\tau^{-1}) + \chi(\sigma_\chi) = 2\chi(\sigma_\chi) = 2,\\ \chi'(\tau) &= \chi(\tau\tau) + \chi(\tau\tau^{-1}) = 0.\end{aligned}$$

Thus, χ' has order $2^r/2 = 2^{r-1}$, and $ker(\chi') = \langle \tau, \sigma_\chi^{2^{r-1}} \rangle$. Also, $\sigma_{\chi'} = \sigma|_{F(\chi')}$. □

Remark 4.3.10. Using Proposition 4.3.7 and Theorem 4.3.9, we may fill in the case $\mu_4 \not\subseteq F$ in Proposition 4.2.15. For, we can reduce to the case $L = F(\mu_4)$ (by using Proposition 4.2.15), then decompose the symbol algebra $(\omega, b; L, \zeta)_{p^k}$ into a cup product. We then use Theorem 4.2.1 to reduce to the character calculations handled in Proposition 4.3.7 and Theorem 4.3.9.

4.4 Abelian Corestriction of Characters

Let $F \subseteq L$ be a finite degree field extension and let $\chi \in X(L)$. In this section, we show that it is possible to compute $cor_{L/F}(\chi)$ whenever $L(\chi) \supseteq F$ is an abelian Galois extension. Suppose first that we can compute $cor_{L/F}(\chi)$ if $L \supseteq F$ is cyclic and $L(\chi) \supseteq F$ is abelian. There are intermediate subfields L_i such that $L = L_k \supseteq L_{k-1} \supseteq \ldots \supseteq L_1 \supseteq L_0 = F$ and L_i is cyclic over L_{i-1} for $i = 1, \ldots, k$. Suppose we have computed $\chi_i = cor_{L/L_i}(\chi)$ for some i. Now $L_i(\chi_i)$ is a subfield of $L(\chi)$, so $L_i(\chi_i)$ is abelian over L_{i-1}. Thus, the hypotheses are preserved at each step and we may proceed iteratively until we have compute $\chi_0 = cor_{L/F}(\chi)$.

We need two results in discrete linear algebra.

Lemma 4.4.1. *Let G be an abelian group and let $h : \mathbb{Z} \times \mathbb{Z} \to G$ be a group homomorphism. Let ι_1, ι_2 be the canonical inclusions of $\mathbb{Z}$ into $\mathbb{Z} \times \mathbb{Z}$. For $i = 1, 2$, define $h_i : \mathbb{Z} \to G$ by $h_i = h\iota_i$. Let $\ker(h_i) = \langle k_i \rangle$ and suppose $l_i \in \mathbb{Z}$ satisfy $h_1(l_1) = h_2(l_2)$ and $im(h_1) \cap im(h_2) = \langle h_i(l_i) \rangle$. If $l_2 \mid k_2$, then $\ker(h) = \langle (k_1, 0), (l_1, -l_2) \rangle$. Similarly, if $l_1 \mid k_1$, then $\ker(h) = \langle (0, k_2), (l_1, -l_2) \rangle$.*

Proof. We will show that $\langle (0, k_2), (l_1, -l_2) \rangle = ker(h)$ if $l_1 \mid k_1$; the argument for the other equality is analogous. Clearly, $\langle (0, k_2), (l_1, -l_2) \rangle \subseteq ker(h)$. Now suppose $(a, b) \in ker(h)$. Since $h(a, b) = 0$, we have $h_1(a) = h_2(-b) \in im(h_1) \cap im(h_2)$. Thus, for some $z \in \mathbb{Z}$, we have $h_1(a) = h_1(zl_1)$. So, $l_1 \mid k_1 \mid a - zl_1$, consequently, $l_1 \mid a$. Let $a = cl_1$, whence $0 = h_1(a - cl_1) = h_2(-b - cl_2)$ as $h_1(l_1) = h_2(l_2)$. So $-b - cl_2 \in ker(h_2) = \langle k_2 \rangle$ and there exists a $d \in \mathbb{Z}$ with $-b - cl_2 = dk_2$. Hence, $(a, b) = c(l_1, -l_2) - d(0, k_2) \in \langle (0, k_2), (l_1, -l_2) \rangle$. This shows $\langle (0, k_2), (l_1, -l_2) \rangle = ker(h)$. □

Corollary 4.4.2. *Fix $j, n \in \mathbb{N}$ and let d be any divisor of n. Let $l = lcm(j, d)$ and let M be the $\mathbb{Z}$-submodule of $\mathbb{Z} \times \mathbb{Z}$ generated by $(l/d, -l/j)$ and $(n/d, 0)$. Then $(a, b) \in M$ if and only if $ad + bj \in n\mathbb{Z}$.*

Proof. Define $h : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_n$ by $h(a, b) = ad + bj \in \mathbb{Z}_n$. Following the notation from Lemma 4.4.1, we have $h_1(a) = ad, h_2(b) = bj, k_1 = n/d$, and $k_2 = n/gcd(n, j)$.

Now $im(h_1) \cap im(h_2) = \langle d\rangle \cap \langle j\rangle$ in $\mathbb{Z}_n$. Since $d \mid n$, we have in $\mathbb{Z}$, $\langle d, n\rangle \cap \langle j, n\rangle = \langle d\rangle \cap (\langle j\rangle + \langle n\rangle) = (\langle d\rangle \cap \langle j\rangle) + \langle n\rangle$. So in $\mathbb{Z}_n$, $\langle d\rangle \cap \langle j\rangle = \langle lcm(j,d)\rangle = \langle l\rangle$. Thus, $h_2(l/j) = l = h_1(l/d)$, whence $l_2 = l/j$ in the notation of Lemma 4.4.1. Since $d \mid n$, we have $l\,gcd(n,j)/j \mid lcm(n,j)gcd(n,j)/j = n$, so $l/j \mid n/gcd(n,j)$. Thus, by Lemma 4.4.1 $ker(h) = \langle (n/d, 0), (l/d, -l/j)\rangle = M$. □

We now give a formula for $cor_{L/F}(\chi)$ when $L \supseteq F$ is cyclic and $L(\chi) \supseteq F$ is abelian. Set $n = [L(\chi) : L]$, $m = [L : F]$, $\sigma = \sigma_\chi$, and $d = gcd(m,n)$. Let k satisfy $km \equiv d \mod n$, i.e. $k = comp_{\mathbb{Z}_n}(m, d)$. Since $(d) = (m, n)$ as ideal in $\mathbb{Z}$, we have m and d generate the same ideal mod n, so we may choose k prime to n.

Theorem 4.4.3. *Let τ be any generator of $Gal(L/F)$ and let $\overline{\tau}$ be any extension of τ to $L(\chi)$. Suppose $\overline{\tau}^m = \sigma^j$. Let $e = gcd(m,n,j) = gcd(d,j)$ and suppose $ad + bj = e$ for some $a, b \in \mathbb{Z}$. Let $\chi' = \mathrm{cor}_{L/F}(\chi)$. Then $\sigma_{\chi'} = \sigma^{ka}\overline{\tau}^b$ and $\ker(\chi') = \langle \sigma^{n/d}, \sigma^{jk/e}\overline{\tau}^{-d/e}\rangle$.*

Proof. Let $I = \{id_{L(\chi)}, \overline{\tau}, \overline{\tau}^2, \ldots, \overline{\tau}^{m-1}\}$., which is a complete set of coset representatives for $Gal(L(\chi)/L)$ in $Gal(L(\chi)/F)$. By [Mer85, 1.3],

$$\chi'(\sigma) = \sum_{\alpha \in I} \chi(\alpha\sigma\alpha_1^{-1}),$$

where $\alpha_1 \in I$ is chosen so that $\alpha\sigma\alpha_1^{-1}$ is the identity on L. Since $L(\chi)$ is abelian over F, we have $\chi'(\sigma) = \sum_{\alpha\in I} \chi(\alpha\sigma\alpha_1^{-1}) = \sum_{\alpha\in I} \chi(\sigma) = |I| = m$ in $\mathbb{Z}_n$. Also,

$$\begin{aligned}
\chi'(\overline{\tau}) &= \sum_{\alpha\in I} \chi(\alpha\overline{\tau}\alpha_1^{-1}) \\
&= \chi(id_{L(\chi)}\overline{\tau}\overline{\tau}^{-1}) + \chi(\overline{\tau}\overline{\tau}\overline{\tau}^{-2}) + \cdots + \chi(\overline{\tau}^{m-2}\overline{\tau}\overline{\tau}^{-(m-1)}) + \chi(\overline{\tau}^{m-1}\overline{\tau}id_{L(\chi)}^{-1}) \\
&= \chi(\overline{\tau}^m) = \chi(\sigma^j) = j.
\end{aligned}$$

Since σ and $\overline{\tau}$ generate $Gal(L(\chi)/F)$, we have $im(\chi')$ is generated by m and j in $\mathbb{Z}_n$. Thus, $im(\chi')$ is generated by $e = gcd(m,n,j) = gcd(d,j)$ in $\mathbb{Z}_n$. Now $\chi'(\sigma^k) = km \equiv d \mod n$. If $ad + bj = e$, then $\chi'(\sigma^{ka}\overline{\tau}^b) = ad + bj = e$.

We chose k prime to n, so $Gal(L(\chi)/F)$ is also generated by σ^k and $\overline{\tau}$. Suppose for some $x, y \in \mathbb{Z}$, we have $\chi'(\sigma^{kx}\overline{\tau}^y) = xd + yj = 0$. By Lemma 4.4.2, this happens if and only if $(x, y) \in M$, where M is generated by $(j/e, -d/e)$ and $(n/d, 0)$. Thus, $ker(\chi')$ is generated by $\sigma^{kj/e}\overline{\tau}^{-d/e}$ and $\sigma^{kn/d}$. $\square$

4.5 Symbol and Cyclic Algebras Over A Cyclotomic Extension

Let F be a field with $char(F) \neq p$. Let $L = F(\mu_p)$, or, if $p = 2$, let $L = F(\mu_4)$. Suppose $L \neq F$. Let $a, b \in L^*$ be elements with $a^{p^k}, b^{p^k} \in F^*$ for some k. Our goal in this section is to describe how to compute $cor_{L/F}(A)$, where A is either of the form $(a, b; L)_{p^n}$ or $(M/F, \sigma, b)$, where $M = L(\mu_{p^n})$ for some $n \in \mathbb{N}$. These results will be useful later in Section 4.7.

4.5.1 Case: $L = F(\mu_4)$

Let $p = 2$. Suppose that L is any quadratic extension of F. Let $A_1 = (a, b; L)_{2^m}$, where $a \in L^*$ and $\mu_{2^m} \subseteq L$ and let $A_2 = (M/L, \sigma, b)$, where $M = L(\mu_{2^n})$ for some $m, n \in \mathbb{N}$. In light of Proposition 1.6.3, we may assume that $[L(\sqrt[2^n]{a}) : L] = 2^n$ (otherwise, we may pass to the function field $L(x)$, write $(A_1)_{L(x)} = (ax, b; L(x))_{2^m} \otimes_{L(x)} (x^{-1}, b; L(x))_{2^m}$, and handle one symbol at a time.) The results in Section 1.5 tell us that A_i corresponds to $\partial\chi_i \cup b$ via the isomorphism $Br(L) \cong H^2(G_L, L^*_{sep})$. Now $L(\chi_1)$ is a Kummer extension of L and $L(\chi_2) = M$ a 2-ary cyclotomic extension of L. The previous sections (4.3.3 and 4.3.4) describe how to compute $cor_{L/F}(\chi_i)$. If $b \in F^*$, then Theorem 4.2.1 and Prop. 1.6.2 apply and $cor_{L/F}(\partial\chi \cup b) = \partial(cor_{L/F}(\chi)) \cup b$, thus, we are able to compute $cor_{L/F}(A_i)$. So we may assume that $b \notin F^*$. We will factor A_i into a tensor product of algebras whose corestriction we can compute (specifically, those of the form described in the previous paragraph). We first need a lemma.

Lemma 4.5.1. *If $a, b \in L^*$ but $a, b \notin F$, then there exist $u, v \in F^*$ such that $ua = 1 - vb$ or $ua = b$.*

Proof. Since $[L : F] = 2$, we have $b = xa + y$ for some $x, y \in F$. We must have $x \neq 0$, as $b \notin F$. If $y = 0$, then set $u = x$, whence $b = ua$. If $y \neq 0$, then $-xy^{-1}a = 1 - y^{-1}b$. Set $u = -xy^{-1}$ and $v = y^{-1}$; then, $ua = 1 - vb$. □

If $a \in F^*$, then $A_1 = (b^{-1}, a; L)_{2^m}$. Suppose instead $a \notin F$. Then by the lemma, there exist $u, v \in F^*$ such that $ua = b$ or $ua = 1 - vb$. If $ua = b$, then, by Prop. 1.2.4.8,

$$A_1 = (a, ua; L)_{2^m} = (a, -u; L)_{2^m}\,.$$

If $ua = 1 - vb$, then, by Prop. 1.2.4.6 and the Steinberg relation (Prop. 1.2.4.7)

$$\begin{aligned} A_1 &= \big(u^{-1}(1-vb), b; L\big)_{2^m} \\ &\sim \big(u^{-1}, b; L\big)_{2^m} \otimes_L (1-vb, vb; L)_{2^m} \otimes_L \big(1-vb, v^{-1}; L\big)_{2^m} \\ &\sim (b, u; L)_{2^m} \otimes_L \big(ua, v^{-1}; L\big)_{2^m}\,. \end{aligned}$$

In either case, A_1 is a tensor product of algebras whose corestriction is computable, thus we can compute $cor_{L/F}(A_1)$. However, there does not appear to be a single formula covering all cases.

Now assume that $\mu_4 \subseteq L$ and that $b^{2^k} \in F^*$ for some $k \in \mathbb{N}$. Recall that $A_2 = (M/L, \sigma, b)$, where $M = L(\mu_{2^n})$ for some $n \in \mathbb{N}$. We can assume $M \neq L$, so $\mu_{2^n} \nsubseteq L$, since otherwise A_2 is split, whence $cor_{L/F}(A_2)$ is split. Since $\mu_4 \subseteq L$ by assumption, there exists a field M' such that $M' \supseteq L$ is cyclic, $M' = L(\mu_{2^m})$ for some $m \geq n$, and $[M' : M] = 2^k$. Then, by Prop. 1.2.6,

$$A_2 \sim (M'/L, \overline{\sigma}, b^{2^k}),$$

where $\overline{\sigma}$ is any extension of σ to M'. Since $M' = L(\mu_{2^m})$ and $b^{2^k} \in F^*$, we are able to compute $cor_{L/F}(A_2)$ via the projection formula (Theorem 4.2.1 and Prop. 1.6.2).

4.5.2 Case: $L = F(\mu_p)$ For Odd p

Let F be a field and let p be an odd prime with $p \nmid char(F)$ and $\mu_p \nsubseteq F$. Let $L = F(\mu_p)$.The following lemma can be found in [GV81], however, we have included a short proof.

Lemma 4.5.2. *Let F be a field and p be an odd prime with $p \nmid char(F)$ and $\mu_p \nsubseteq F$. Let $L = F(\mu_p)$. For $a \in L^*$, we have $a^{p^k} \in F^*$ for some $k \geq 0$ if and only if $a = b\omega$ for some $b \in F^*$ and $\omega \in \mu_{p^k}(L)$.*

Proof. If $a = b\omega$ for $b \in F^*$ and $\omega \in \mu_{p^k}$, then $a^{p^k} = b^{p^k} \in F^*$.

Now suppose $a^{p^k} \in F^*$ for some $k \geq 0$. Let f be the minimal polynomial of a over F and let $s = [L : F]$. Then f has degree s and splits over L (as L is Galois over F). Furthermore, $f \mid x^{p^k} - a^{p^k}$, so the conjugates of a all differ from one another by elements of $\mu_{p^k}(L)$. Thus, $N_{L/F}(a) = a^s\zeta$ for some $\zeta \in \mu_{p^k}(L)$. Since $p \nmid s$, there exist $x, y \in \mathbb{Z}$ such that $xs + yp^k = 1$. Then, $a = a^{xs+yp^k} = (N_{L/F}(a)\zeta^{-1})^x(a^{p^k})^y = b\omega$, where $\omega = \zeta^{-x} \in \mu_{p^k}(L)$ and $b = N_{L/F}(a^x)(a^{p^k})^y \in F^*$. □

Let $a, b \in L^*$ be elements satisfying $a^{p^k}, b^{p^k} \in F^*$ for some $k \in \mathbb{N}$. Let $A = (a, b; L, \zeta)_{p^n}$ where $\zeta \in \mu^*_{p^n}(L)$. By Lemma 4.5.2, $a = \omega_1 f_1$ and $b = \omega_2 f_2$ for certain $\omega_i \in \mu_{p^k}(L)$ and $f_i \in F$. There exists $\omega \in \mu_{p^k}$ and $c_1, c_2 \in \mathbb{Z}$ with $\omega^{c_i} = \omega_i$ for $i = 1, 2$. With this setup, we prove

Theorem 4.5.3. *Let θ be a p^n-th root of ω and let E be the field within $F \subseteq L(\theta)$ determined by $[L(\theta) : E] = [L : F]$ (as $F \subseteq L(\theta)$ is cyclic). Let σ be a generator of Gal$(L(\theta)/F)$ satisfying $\sigma^{[L:F]}(\theta) = \zeta\theta$. Then*

$$\mathrm{cor}_{L/F}(A) = (E/F, \sigma|_E, f_1^{-c_2} f_2^{c_1}).$$

Proof. From the setup above,

$$\begin{aligned} A &= (a, b; L, \zeta)_{p^n} \\ &= (\omega^{c_1} f_1, \omega^{c_2} f_2; L, \zeta)_{p^n} \\ &= (\omega, \omega; L, \zeta)_{p^n}^{c_1 c_2} \otimes_L (f_1, f_2; L, \zeta)_{p^n} \otimes_L \left(\omega, f_1^{-c_2} f_2^{c_1}; L, \zeta\right)_{p^n}. \end{aligned}$$

Since p is odd, $(\omega, \omega; L, \zeta)_{p^n}$ is split (cf. Proposition 1.2.4.8) and $cor_{L/F}(f_1, f_2; L, \zeta)_{p^n}$ is split (cf. Corollary 4.2.11 and Prop. 4.2.7). Let θ be any p^n-th root of ω and let $M = L(\theta)$. We then use Prop. 4.2.15 and obtain

$$\begin{aligned} \mathrm{cor}_{L/F}(A) &= \mathrm{cor}_{L/F}\left[(\omega, \omega; L, \zeta)_{p^n}^{c_1 c_2} \otimes_L (f_1, f_2; L, \zeta)_{p^n} \otimes_L \left(\omega, f_1^{-c_2} f_2^{c_1}; L, \zeta\right)_{p^n}\right] \\ &= \mathrm{cor}_{L/F}\left(\omega, f_1^{-c_2} f_2^{c_1}; L, \zeta\right)_{p^n} \\ &= (E/F, \sigma|_E, f_1^{-c_2} f_2^{c_1}), \end{aligned}$$

where E is the intermediate field in $F \subseteq M$ determined by $[M : E] = [L : F]$ and σ is a generator of $Gal(L(\theta)/F)$ satisfying $\sigma^{[L:F]}(\theta) = \zeta\theta$ (the existence of such a σ was shown in Prop. 4.2.15). $\square$

We continue to assume $p \nmid char(F)$, $\mu_p \not\subseteq F$ and $L = F(\mu_p)$ (p an odd prime). Now let $(M/L, \sigma, b)$ be a cyclic algebra where $M = L(\mu_{p^n})$ for some n and $a \in L^*$ satisfies $a^{p^k} \in F^*$ for some k. By Lemma 4.5.2, $a = b\omega$ for some $b \in F^*$ and $\omega \in \mu_{p^k}(L)$. Then, we have the following Theorem.

Theorem 4.5.4. *Let τ be a generator of $Gal(M/F)$ such that $\tau^{[L:F]} = \sigma$ and let E be the field determined by $F \subseteq E \subseteq M$ and $[M : E] = [L : F]$. Then*

$$cor_{L/F}(M/L, \sigma, a) = (E/F, \tau|_E, b),$$

Proof. If $\mu_{p^\infty} \subseteq L$, then $L = L(\mu_{p^n}) = M$. Then $(M/L, \sigma, a)$ is split, σ is the identity on F and $E = F$ is the unique field in $F \subseteq M$ such that $[M : E] = [L : F]$. Let τ be any generator of $Gal(M/F)$, then $\tau^{[L:F]} = \tau^{[M:F]}$ is the identity on F. Thus, $(E/F, \tau|_E, b)$ is split and the result holds (since $cor_{L/F}(L) = F$).

Now suppose $\mu_{p^\infty} \not\subseteq L$. Let $p^l = o(\omega)$. Since p is odd and $\mu_{p^\infty} \not\subseteq L$, there exists a field M' such that $M' = F(\mu_{p^m})$ for some m, M' is cyclic over F, and $[M' : M] = p^l$. Let $\sigma' \in Gal(M'/L)$ be any extension of $\sigma \in Gal(M/L)$ to M'. Then, by Prop. 1.2.6 $(M/L, \sigma, \omega) = (M'/L, \sigma', \omega^{p^l})$, which is split since $\omega^{p^l} = 1$. Thus, $(M/L, \sigma, a) = (M/L, \sigma, \omega) \otimes_L (M/L, \sigma, b) = (M/L, \sigma, b)$. Now let τ be a generator of $Gal(M/F)$ such that $\tau^{[L:F]} = \sigma$; such a τ exists as $Gal(M/F)$ maps onto $Gal(M/L)$ via the $[L : F]$ power map. We use Proposition 4.2.14 to get

$$cor_{L/F}(M/L, \sigma, a) = cor_{L/F}(M/L, \tau^{[L:F]}, a) = (E/F, \tau|_E, b),$$

where E is the field determined by $F \subseteq E \subseteq M$ and $[M : E] = [L : F]$. $\square$

4.6 Simple Radical Extensions

In this section, we will recall some results and prove two propositions which will be used in the next section for computing corestriction. Many of the basic results can be found multiple times in the literature (cf. [Alb03], [Kar89], [GV81], [dOV84]). Throughout this section, p will denote a prime number.

Definition 4.6.1. Let p be a prime, and let F be a field with $char(F) \neq p$. For $p \neq 2$, we say the field extension $F \subseteq K$ is *p-pure* if $\mu_p \subseteq F$ whenever $\mu_p \subseteq K$. If $p = 2$, then we say $F \subseteq K$ is *2-pure* if $\mu_4 \subseteq F$ whenever $\mu_4 \subseteq K$.

The p-pure extensions were first examined by Gay and Velez in [GV81], however, the term p-pure is not used. The author is not sure where the term originated, however, this is the term used in [Alb03]. In addition, the condition is sometimes written more succinctly as "$\mu_{2p} \subseteq F$ whenever $\mu_{2p} \subseteq K$", however, this may introduce the unnecessary assumption that $char(F) \neq 2$ in the case that p is odd.

Remark 4.6.2. The condition for p-purity can be written as $\mu_{p^r} \subseteq F$ if and only if $\mu_{p^r} \subseteq K$ where $r = 1$ if p is odd and $r = 2$ if $p = 2$. This shows that if $F \subseteq E \subseteq K$ are fields, then $F \subseteq K$ is p-pure if and only if both $F \subseteq E$ and $E \subseteq K$ are p-pure.

The following result is another statement of [GV81, Lem 1.5].

Proposition 4.6.3. *Let p be prime and suppose $F \subseteq K$ is p-pure. Let $t \in K^*$ be an element with $t^{p^m} \in F^*$. Then we have $o(tF^*) = [F(t) : F] = p^e$ for some $e \leq m$, and $x^{p^e} - t^{p^e}$ is irreducible over F, where $o(tF^*)$ denotes the order of tF^* in K^*/F^*. So $N_{F(t)/F}(t) = (-1)^{p^e-1} t^{p^e}$.*

We get an immediate corollary.

Corollary 4.6.4. *Let F, t, and $p^e = o(tF^*)$ be as in Proposition 4.6.3. Every field L with $F \subseteq L \subseteq F(t)$ has the form $L = F(t^{p^l})$ for some $l \leq e$ and $p^l = [F(t) : L] = o(tL^*)$.*

Proof. Suppose that $F \subseteq L \subseteq F(t)$. Now $o(tL^*) = p^l$, for some $0 \le l \le e$, whence $t^{p^l} \in L^*$ and $F(t^{p^l}) \subseteq L$. By Proposition 4.6.3, $[F(t) : L] = [L(t) : L] = o(tL^*) = p^l$, yet $[F(t) : F(t^{p^l})] \le p^l$, so we get $F(t^{p^l}) = L$. □

Remark 4.6.5. Proposition 4.6.3 may not hold if $F \subseteq K$ is not p-pure. For example, take $F = \mathbb{Q}$, $t = \zeta_p$, and $K = \mathbb{Q}(t)$, where ζ_p is a primitive p-th root of unity (p odd). We know that $o(tF^*) = p$, yet $[F(t) : F] = p - 1$ and $x^p - t^p = x^p - 1$ is reducible over $\mathbb{Q}$.

Simple radical extensions which are p-pure are determined by the corresponding subgroups modulo F^*. The next proposition shows that if $t_1, t_2 \in K^*$ are separable over F and have finite order in K^*/F^*, then $F(t_1) = F(t_2)$ if and only if $\langle t_1 F^* \rangle = \langle t_2 F^* \rangle$.

Proposition 4.6.6. *Let p be prime and suppose $F \subseteq K$ is p-pure and* $\mathrm{char}(F) \neq p$. *Let $t_1, t_2 \in K^*$ be elements where $t_i F^*$ has p power order in K^*/F^* for $i = 1, 2$. Suppose $t_2 \in F(t_1)$. Then there is an integer q such that $t_1^q t_2 \in F^*$, i.e. $\langle t_2 F^* \rangle \subseteq \langle t_1 F^* \rangle$.*

Proof. Let $p^{m_i} = o(t_i)$ for $i = 1, 2$. By Proposition 4.6.3, $[F(t_i) : F] = p^{m_i}$, whence $m_2 \le m_1$. We proceed by induction on m_1. If $m_1 = 0$, then $t_1, t_2 \in F^*$, so we are done. Now assume $m_1 > 0$.

By Corollary 4.6.4, $F(t_2) = F(t_1^{p^{m_1 - m_2}})$. If $m_1 > m_2$, then the induction hypothesis applies to $t_2 \in F(t_1^{p^{m_1 - m_2}})$, whence there is a $q \in \mathbb{Z}$ with $(t_1^{p^{m_1 - m_2}})^q t_2 \in F^*$.

Otherwise, $m_1 = m_2$, so $F(t_1) = F(t_2)$. Set $E = F(t_1^p)$, whence $E \subseteq E(t_1) = F(t_1)$ is p-pure, so $[E(t_1) : E] = o(t_1 E^*) = p$. Also, $E \subseteq E(t_1)$ is separable, so let N be the normal closure of $E(t_1)$ over E. There exists an E-monomorphism, $\varphi : E(t_1) \to N$, such that $\varphi(t_1) \neq t_1$. Since $t_i^p \in E$ for $i = 1, 2$, we have $\varphi(t_i)^p = \varphi(t_i^p) = t_i^p$, whence $\varphi(t_i) = \zeta_i t_i$, where $\zeta_i \in \mu_p^*(N)$. Thus, there exists an r such that $\varphi(t_1^r t_2) = t_1^r t_2$. Yet $[E(t_1) : E] = p$ and $E(t_1^r t_2)$ is intermediate field where φ is the identity. Since φ is not the identity map on $E(t_1)$, we must have $t_1^r t_2 \in E^*$. But $[E : F] < p^{m_1}$, so we may apply our induction hypothesis to t_1^p and $t_1^r t_2$ and obtain a $q' \in \mathbb{Z}$ such that $(t_1^p)^{q'} t_1^r t_2 = t_1^{pq'+r} t_2 \in F^*$. Since $q = pq' + r \in \mathbb{Z}$, we are done. □

Remark 4.6.7. Note that q is determined up to $p^{m_1} = o(t_1 F^*)$. For, if $t_1^q t_2, t_1^r t_2 \in F^*$, then clearly $t_1^{q-r} \in F^*$, whence $o(t_1 F^*) = p^{m_1} \mid q - r$.

Definition 4.6.8. For $F \subseteq E \subseteq K$, and $a, b \in K$, define $\lambda_{a,b}^E = [E(a,b) : E(b)]$. If aF^* and bF^* have finite order and $F \subseteq K$ is p-pure, then $\lambda_{a,b}^F$ describes the order of aF^* over the intersection $\langle aF^* \rangle \cap \langle bF^* \rangle$, as we shall see in Proposition 4.6.9 below.

Proposition 4.6.9. *Let p be prime and suppose $F \subseteq K$ is p-pure and* char$(F) \neq p$*. Let $t_1, t_2 \in K^*$ be elements where $t_i F^*$ has p power order in K^*/F^* for $i = 1, 2$. Let $p^{l_1} = \lambda_{t_1,t_2}^F = [F(t_1,t_2) : F(t_2)]$ and $p^{l_2} = \lambda_{t_2,t_1}^F = [F(t_1,t_2) : F(t_1)]$. Then,*

1. *$F(t_1) \cap F(t_2) = F(t_1^{\lambda_{t_1,t_2}^F}) = F(t_2^{\lambda_{t_2,t_1}^F})$.*
2. *$\langle t_1 F^* \rangle \cap \langle t_2 F^* \rangle = \langle t_1^{\lambda_{t_1,t_2}^F} F^* \rangle = \langle t_2^{\lambda_{t_2,t_1}^F} F^* \rangle$.*
3. *$t_1^{c\lambda_{t_1,t_2}^F} t_2^{-\lambda_{t_2,t_1}^F} \in F^*$ if and only if $c \in comp(t_1 F^*, t_2 F^*)$*
4. *If $t_1^{m_1} t_2^{-m_2} \in F^*$, then there exists $d \in \mathbb{Z}$ such that for any $c \in comp(t_1 F^*, t_2 F^*)$,*

   $$m_1 \equiv c\lambda_{t_1,t_2}^F d \bmod o(t_1 F^*) \quad \textit{and} \quad m_2 \equiv \lambda_{t_2,t_1}^F d \bmod o(t_2 F^*).$$

   If $m_i = a_i p^{e_i}$ with a_i prime to p, then $e_i \geq l_i$. Furthermore, if $p^{e_i} < o(t_i F^*)$, then $e_1 - l_1 = e_2 - l_2$.

Proof. For (1) and (2), we will only prove the first equality; the second equality follows by a symmetric argument replacing 1 with 2. From Proposition 4.6.3, $o(t_1 F(t_2)^*) = [F(t_2)(t_1) : F(t_2)] = \lambda_{t_1,t_2}^F$. Thus, for any n, we have $t_1^n \in F(t_2)$ if and only if $\lambda_{t_1,t_2}^F \mid n$. Since intermediate fields of $F \subseteq F(t_1)$ have the form $F(t_1^n)$, we must have $F(t_1) \cap F(t_2) = F(t_1^{\lambda_{t_1,t_2}^F})$. Also, for any n, we have $t_1^n \in F(t_2)$ if and only if $\langle t_1^n F^* \rangle \subseteq \langle t_2 F^* \rangle$ (cf. Prop 4.6.6 for the non-trivial implication), whence $\langle t_1^n F^* \rangle \subseteq \langle t_2 F^* \rangle$ if and only if $\lambda_{t_1,t_2}^F \mid n$. Thus, $\langle t_1 F^* \rangle \cap \langle t_2 F^* \rangle = \langle t_1^{\lambda_{t_1,t_2}^F} F^* \rangle$. This proves (1) and (2).

For $i = 1, 2$, set $G_i = \langle t_i F^* \rangle$, whence $|G_i : G_1 \cap G_2| = p^{l_i}$ by applying (2). By the definition of compatibility factor, $c \in comp(t_1F^*, t_2F^*)$ if and only if $t_1^{c|G_1:G_1\cap G_2|}F^* = t_2^{|G_2:G_1\cap G_2|}F^*$, i.e. $t_1^{c\lambda^F_{t_1,t_2}} t_2^{-\lambda^F_{t_2,t_1}} \in F^*$. This gives (3).

Suppose that $t_1^{m_1} t_2^{-m_2} \in F^*$. Then, $t_2^{m_2}F^* \in \langle t_1F^* \rangle \cap \langle t_2F^* \rangle = \langle t_2^{\lambda^F_{t_2,t_1}} F^* \rangle$, so there is a $d \in \mathbb{Z}$ such that $m_2 \equiv d\lambda^F_{t_2,t_1}$ mod $o(t_2F^*)$. Thus, $t_2^{d\lambda^F_{t_2,t_1} - m_2} \in F^*$. We proved above that $t_1^{-dc\lambda^F_{t_1,t_2}} t_2^{d\lambda^F_{t_2,t_1}} \in F^*$ for any $c \in comp(t_1F^*, t_2F^*)$, so $F^* = t_1^{-dc\lambda^F_{t_1,t_2}} t_2^{d\lambda^F_{t_2,t_1}} t_1^{m_1} t_2^{-m_2} F^* = t_1^{m_1 - dc\lambda^F_{t_1,t_2}} F^*$. Thus, $m_1 \equiv c\lambda^F_{t_1,t_2} d$ mod $o(t_1F^*)$.

Now if, for $i = 1, 2$, we have $m_i = a_i p^{e_i}$, where a_i is prime to p, then $t_i^{m_i}F^* \in \langle t_1F^* \rangle \cap \langle t_2F^* \rangle = \langle t_i^{p^{l_i}} F^* \rangle$, so $e_i \geq l_i$. Set $p^{n_i} = o(t_iF^*)$ and now assume $e_i < n_i$ for $i = 1, 2$. Because $m_2 \equiv dp^{l_2}$ mod $o(t_2F^*)$, there exists a $k \in \mathbb{Z}$ such that $a_2p^{e_2} + kp^{n_2} = dp^{l_2}$. Thus, $p^{e_2 - l_2}(a_2 + kp^{n_2 - e_2}) = d$. But $e_2 < n_2$ and a_2 is prime to p, so $a_2 + kp^{n_2 - e_2}$ is prime to p. A similar argument shows that $d = p^{e_1 - l_1} q$, where q is prime to p. Therefore, $e_1 - l_1 = e_2 - l_2$. □

4.7 Corestriction Of Symbol Algebras

Let p be prime and $F \subseteq N$ be a finite degree field extension with $char(F) \neq p$ and $\mu_{p^n} \subseteq N$. Let $t_1, t_2 \in N$ be elements whose images in N^*/F^* have p power order. Our goal in the next two sections is to compute $cor_{N/F}(t_1, t_2; N)_{p^n}$. We will assume that $\mu_p \in F$, or if $p = 2$, $\mu_4 \subseteq F$. Thus, for any field L such that $F \subseteq L \subseteq N$, the extension $F \subseteq L$ is p-pure.

Our first step will be to compute $cor_{N/K}(t_1, t_2; N)_{p^n}$ where $K = F(t_1, t_2)$.

Theorem 4.7.1. *Let p be prime and suppose $F \subseteq N$ with $\mathrm{char}(F) \neq p$ and $\mu_{p^n} \subseteq N$. Let $t_1, t_2 \in N^*$ be elements where t_iF^* have p-power order in N^*/F^* for $i = 1, 2$. Let $K = F(t_1, t_2)$. Suppose that $\mu_{p^n} \cap K = \mu_{p^k}$. Let $u = [N : K(\mu_{p^n})]$. Then*

$$\mathrm{cor}_{N/K}\left(t_1, t_2; N\right)_{p^n} = \left(t_1, t_2^{eu}; K\right)_{p^k},$$

where $e = 1$ unless $p = 2$ and $n > k$, in which case $e = 1 + 2^{k-1}$.

Proof. Set $M = K(\mu_{p^n})$. We apply the Projection Formula 4.2.3 to get

$$cor_{N/M}(t_1, t_2; N)_{p^n} = (t_1, t_2^u; M)_{p^n},$$

as $t_2 \in M$, so $\mathrm{N}_{N/M}(t_2) = t_2^{[N:M]} = t_2^u$. Note that $\mu_4 \subseteq F \subseteq K$, so $k \geq 2$. We apply Corollary 4.2.11 to get

$$cor_{M/K}\left(t_1, t_2^u; M\right)_{p^n} = \left(t_1, t_2^{eu}; K\right)_{p^k},$$

where $e = 1$ unless $p = 2$ and $n > k$ in which case $e = 1 - 2^{k-1}$. □

We continue with the notation established above. Let $\omega \in \mu^*_{p^k}(K)$. For $a, b \in K^*$ and $F \subseteq E \subseteq K$, recall from Definition 4.6.8 that $\lambda^E_{a,b} = [E(a,b) : E(b)]$, so, by Proposition 4.6.9, $\langle aE^* \rangle \cap \langle bE^* \rangle = \langle a^{\lambda^E_{a,b}} E^* \rangle = \langle b^{\lambda^E_{b,a}} E^* \rangle$. We define the following constants

$$p^{l_1} = [F(t_1, t_2) : F(t_2, \omega)] = o(t_1 F(t_2, \omega)^*) = \lambda_{t_1,\omega}^{F(t_2)}$$
$$p^{l_2} = [F(t_1, t_2) : F(t_1, \omega)] = o(t_2 F(t_1, \omega)^*) = \lambda_{t_2,\omega}^{F(t_1)}$$
$$p^{m_1} = [F(t_1, \omega) : F(\omega)] = o(t_1 F(\omega)^*) = \lambda_{t_1,\omega}^{F}$$
$$p^{m_2} = [F(t_2, \omega) : F(\omega)] = o(t_2 F(\omega)^*) = \lambda_{t_2,\omega}^{F}$$
$$p^{n_1} = [F(t_1, \omega) : F(t_1)] = o(\omega F(t_1)^*) = \lambda_{\omega,t_1}^{F}$$
$$p^{n_2} = [F(t_2, \omega) : F(t_2)] = o(\omega F(t_2)^*) = \lambda_{\omega,t_2}^{F}$$
$$p^{s} = [F(\omega) : F] = o(\omega F^*).$$

Note that $[F(\omega) : F]$ is indeed a power of p since we assumed $\mu_p \subseteq F$, or if $p = 2$, $\mu_4 \subseteq F$. Also, let us choose $c_1 \in comp(\omega F(t_2)^*, t_1 F(t_2)^*)$, $c_2 \in comp(\omega F^*, t_2 F^*)$, and $c_3 \in comp(t_2 F^*, t_1^{p^{l_1}} \omega^{-c_1} F^*)$. By Remark 1.7.2, we may choose the c_i prime to p for $i = 1, 2, 3$. If $n_1 = 0$ (i.e., $\omega \in F(t_1)$) and $m_1 = l_1$, then we require $c_1 \in comp(\omega F(t_2^*), t_1 F(t_2)^*)$ as well. We will show in Property 6 that such a choice of c_1 is possible.

Now we list or prove several properties.

1. For $i = 1, 2$, we have $m_i \geq l_i$ and $s \geq n_i \geq 0$.

2. $F(t_2, \omega) = F(t_2, t_1^{p^{l_1}})$.

Proof. By Corollary 4.6.4, intermediate fields of $F(t_2) \subseteq F(t_2, t_1)$ are determined by their index. $F(t_2, t_1^{p^{l_1}})$ is the unique subfield of index $p^{l_1} = [F(t_1, t_2) : F(t_2, \omega)]$, so $F(t_2, \omega) = F(t_2, t_1^{p^{l_1}})$. □

3. $\lambda_{\omega,t_1}^{F(t_2)} = \lambda_{\omega,t_2}^{F(t_1)} = 1$ (as $\omega \in F(t_1, t_2)$).

4. $t_1^{p^{l_1}} \omega^{-a} \in F(t_2)^*$ if and only if $a \in comp(\omega F(t_2)^*, t_1 F(t_2)^*)$.
$t_2^{p^{m_2}} \omega^{-ap^{n_2}} \in F^*$ if and only if $a \in comp(\omega F^*, t_2 F^*)$.
$t_1^{p^{m_1}} \omega^{-ap^{n_1}} \in F^*$ if and only if $a \in comp(\omega F^*, t_1 F^*)$.
In particular, $t_1^{p^{l_1}} \omega^{-c_1} \in F(t_2)^*$ and $t_2^{p^{m_2}} \omega^{-c_2 p^{n_2}} \in F^*$.

Proof. Use Proposition 4.6.9(3). □

5. For $i = 1, 2$, we have $o(t_iF^*) = p^{s-n_i+m_i}$.

Proof. By Proposition 4.6.9(2), $\langle t_i^{p^{m_i}} F^*\rangle = \langle \omega^{p^{n_i}} F^*\rangle$, so $o(t_i^{p^{m_i}} F^*) = o(\omega^{p^{n_i}} F^*) = p^{s-n_i}$. Thus, $o(t_iF^*) = p^{s-n_i+m_i}$. □

6. If $n_1 = 0$ and $m_1 = l_1$, then $comp(\omega F^*, t_1F^*) \subseteq comp(\omega F(t_2)^*, t_1F(t_2)^*)$.

Proof. If $d \in comp(\omega F^*, t_1F^*)$, then $t_1^{p^{l_1}} \omega^{-d} = t_1^{p^{m_1}} \omega^{-dp^{n_1}} \in F^* \subseteq F(t_2)^*$, so $d \in comp(\omega F(t_2)^*, t_1F(t_2)^*)$ by Property 4. □

Thus, if $n_1 = 0$ and $m_1 = l_1$, we may choose $c_1 \in comp(\omega F(t_2)^*, t_1F(t_2)^*)$ so that $c_1 \in comp(\omega F^*, t_1F^*)$ as well.

7. $t_1^{p^{l_1}} \omega^{-c_1} \in F^*$ if and only if $n_1 = 0$, $m_1 = l_1$.

Proof. If $n_1 = 0$, $m_1 = l_1$, then $c_1 \in comp(\omega F^*, t_1F^*)$, so $t_1^{p^{l_1}} \omega^{-c_1} = t_1^{p^{m_1}} \omega^{-c_1p^{n_1}} \in F^*$ by Property 4 above.

Now suppose $t_1^{p^{l_1}} \omega^{-c_1} \in F^*$. Recall that $p \nmid c_1$, so Proposition 4.6.9(4) gives us $l_1 \geq m_1$ and $0 \geq n_1$, whence, by Property 1, we have $l_1 = m_1$ and $0 = n_1$. □

8. $t_1^{p^{l_1}} \omega^{-c_1} t_2^d \in F^*$, where $d = \begin{cases} 0, & \text{if} \quad n_1 = 0,\ m_1 = l_1 \\ -c_3p^{l_2}, & \text{if} \quad n_1 > 0 \text{ or } m_1 > l_1 \end{cases}$

Proof. If $n_1 = 0$ and $m_1 = l_1$, then Property 7 tells us that $t_1^{p^{l_1}} \omega^{-c_1} \in F^*$. So assume $n_1 > 0$ or $m_1 > l_1$, whence $t_1^{p^{l_1}} \omega^{-c_1} \notin F^*$, by Property 7. From Property 4, $t_1^{p^{l_1}} \omega^{-c_1} \in F(t_2)^*$, so Proposition 4.6.6 tells us there is a $d \in \mathbb{Z}$ such that

$$t_1^{p^{l_1}} \omega^{-c_1} t_2^d \in F^*.$$

Since $t_1^{p^{l_1}} \omega^{-c_1} \notin F^*$, we have $d \neq 0$, so we may write $d = kp^e$, where k is prime to p. So we get

$$t_1^{p^{l_1}} \omega^{-c_1} t_2^{kp^e} \in F^*.$$

Assume first $n_1 > 0$. We have $\omega^{-c_1} t_2^{kp^e} \in F(t_1^{p^{l_1}})^* \subseteq F(t_1)^*$. Since $1 < p^{n_1} = o(\omega F(t_1)^*)$ and c_1 is prime to p, we have $\omega^{-c_1} \notin F(t_1)^*$. Thus, $t_2^{kp^e} \notin F(t_1)^*$, so $p^e < o(t_2 F(t_1)^*)$. So we have $\omega^{-c_1 p^0} t_2^{kp^e} \in F^*$ with $p^0 < o(\omega F(t_1)^*)$ and $p^e < o(t_2 F(t_1)^*)$. We may apply Proposition 4.6.9(4) to $e_1 = 0, e_2 = e$ and obtain $0 - \log_p(\lambda_{\omega,t_2}^{F(t_1)}) = 0 = e - \log_p(\lambda_{t_1,\omega}^{F(t_2)}) = e - l_2$. Thus, $e = l_2$.

Now assume instead that $m_1 > l_1$. We have $t_1^{p^{l_1}} t_2^{kp^e} \in F(\omega^{c_1})^* = F(\omega)^*$. Since $p^{l_1} < p^{m_1} = o(t_1 F(\omega)^*)$, we have $t_1^{p^{l_1}} \notin F(\omega)^*$. Thus, $t_2^{kp^e} \notin F(\omega)^*$, so $p^e < o(t_2 F(\omega)^*)$. So we have $t_1^{p^{l_1}} t_2^{kp^e} \in F(\omega)^*$ with $p^{l_1} < o(t_1 F(\omega)^*)$ and $p^e < o(t_2 F(\omega)^*)$. We may apply Proposition 4.6.9(4) to $e_1 = l_1, e_2 = e$ and obtain $l_1 - \log_p(\lambda_{t_1,t_2}^{F(\omega)}) = 0 = e - \log_p(\lambda_{t_2,t_1}^{F(\omega)}) = e - l_2$. Thus, $e = l_2$.

So $t_1^{p^{l_1}} \omega^{-c_1} t_2^{kp^e} \in F^*$ if and only if $e = l_2$, thus $\langle t_1^{p^{l_1}} \omega^{-c_1} F^* \rangle \cap \langle t_2 F^* \rangle = \langle t_2^{p^{l_2}} F^* \rangle$, whence $t_1^{p^{l_1}} \omega^{-c_1} t_2^{-c_3 p^{l_2}} \in F^*$, by definition of c_3. □

Continuing with the same notation, we have

Theorem 4.7.2. *Let $L = F(\omega) = F(\mu_k)$ and suppose $\mu_{p^k} \cap F = \mu_{p^r}$ for some $r \geq 1$ (if $p = 2$, then $r \geq 2$). Let $K = F(t_1, t_2)$ and let $\zeta \in \mu_{p^k}^*(K)$. Set*

$$d = \begin{cases} 0 & \text{if } n_1 = 0,\ m_1 = l_1; \\ -c_3 p^{l_2} & \text{if } n_1 > 0 \text{ or } m_1 > l_1, \end{cases}$$

$\epsilon_1 = p^{l_1} - 1 + d(p-1)$, $\epsilon_2 = p^{m_2} - 1$, and $\epsilon_3 = p^{n_2}(p - 1 + \epsilon_1) + \epsilon_2$. Then

$$cor_{K/L}(t_1, t_2; \zeta)_{p^k} = \left((-1)^{\epsilon_1} t_1^{p^{l_1}} t_2^d, (-1)^{\epsilon_2} t_2^{p^{m_2}}; L, \zeta\right)_{p^k}. \tag{4.7}$$

Let θ be any p^k-th root of ω and let E be the field determined by $F \subseteq E \subseteq L(\theta)$ and $[E : F] = [L(\theta) : L]$. Set $p^l = [L(\theta) : L]$. Then,

$$cor_{K/F}(t_1, t_2; \zeta)_{p^k} = \left((-1)^{\epsilon_1} t_1^{p^{l_1}} t_2^d \omega^{-c_1}, (-1)^{\epsilon_2} t_2^{ep^{m_2}} \omega^{-ec_2 p^{n_2}}; F, \zeta\right)_{p^r} \otimes_F \left(E/F, \sigma|_E, (-1)^{\epsilon_3} t_1^{-c_2 p^{l_1+n_2}} t_2^{c_1 p^{m_2} - dc_2 p^{n_2}}\right)_{p^k}, \tag{4.8}$$

where $\sigma \in Gal(L(\theta)/F)$ satisfies $\sigma^{p^{k-r}}(\theta) = \zeta^{p^{k-l}} \theta$.

Proof. Set $L = F(\omega)$, and $M = L(t_2)$. Recall $o(t_1 F(t_2,\omega)^*) = p^{l_1}$, whence by Proposition 4.6.3 $N_{K/M}(t_1) = (-1)^{p^{l_1}-1} t_1^{p^{l_1}}$. Since $t_2 \in M$, we may apply the Projection Formula 4.2.3 to obtain

$$cor_{K/M}(t_1, t_2; \zeta)_{p^k} = \Big((N_{K/M}(t_1), t_2; \zeta\Big)_{p^k} = \Big((-1)^{p^{l_1}-1} t_1^{p^{l_1}}, t_2; \zeta\Big)_{p^k}.$$

By Property 8 and our definition of d, we have $t_1^{p^{l_1}} \omega^{-c_1} t_2^d \in F^*$. So $t_1^{p^{l_1}} t_2^d = f_1 \omega^{c_1}$ for some $f_1 \in F^*$. Set

$$f_1' = (-1)^{\epsilon_1} f_1 = (-1)^{p^{l_1}-1+d(p-1)} t_1^{p^{l_1}} t_2^d \omega^{-c_1}.$$

Note that $((-1)^{p-1} t_2, t_2; \zeta)_{p^k}$ is split (cf. Proposition 1.2.4.8), so, in $Br(M)$, we have

$$\begin{aligned} cor_{K/M}(t_1, t_2; \zeta)_{p^k} &= \Big((-1)^{p^{l_1}-1} t_1^{p^{l_1}}, t_2; \zeta\Big)_{p^k} \\ &= \Big((-1)^{p^{l_1}-1} t_1^{p^{l_1}} (-1)^{(p-1)d} t_2^d, t_2; \zeta\Big)_{p^k} \\ &= \Big((-1)^{p^{l_1}-1+d(p-1)} t_1^{p^{l_1}} t_2^d, t_2; \zeta\Big)_{p^k} \\ &= (f_1' \omega^{c_1}, t_2; M, \zeta)_{p^k}. \end{aligned}$$

Recall that $o(t_2 F(\omega)^*) = p^{m_2}$, so by Proposition 4.6.3 $N_{M/L}(t_2) = (-1)^{p^{m_2}-1} t_2^{p^{m_2}}$. Again, $f_1' \omega^{c_1} \in F(\omega)^*$, so we apply the Projection Formula 4.2.3 to obtain

$$cor_{M/L}(f_1'\omega^{c_1}, t_2; \zeta, M)_{p^k} = \Big(f_1'\omega^{c_1}, N_{M/L}(t_2); \zeta, M\Big)_{p^k} = \Big(f_1'\omega^{c_1}, (-1)^{p^{m_2}-1} t_2^{p^{m_2}}; L, \zeta\Big)_{p^k}$$

Now we use Property 4 to get $f_2 \in F^*$ such that $t_2^{p^{m_2}} = f_2 \omega^{c_2 p^{n_2}}$. Set

$$f_2' = (-1)^{\epsilon_2} f_2 = (-1)^{p^{m_2}-1} t_2^{p^{m_2}} \omega^{-c_2 p^{n_2}},$$

so that, in $Br(L)$,

$$\begin{aligned} cor_{K/L}(t_1, t_2; \zeta)_{p^k} &= \Big(f_1'\omega^{c_1}, (-1)^{p^{m_2}-1} t_2^{p^{m_2}}; L, \zeta\Big)_{p^k} \\ &= \Big(f_1'\omega^{c_1}, f_2'\omega^{c_2 p^{n_2}}; L, \zeta\Big)_{p^k} \\ &= \Big((-1)^{\epsilon_1} t_1^{p^{l_1}} t_2^d, (-1)^{\epsilon_2} t_2^{p^{m_2}}; L, \zeta\Big)_{p^k}. \end{aligned}$$

This proves (4.7).

Now write

$$\left(f_1'\omega^{c_1}, f_2'\omega^{c_2p^{n_2}}; L, \zeta\right)_{p^k} = (f_1', f_2'; L, \zeta)_{p^k} \otimes_L \left(\omega, \omega^{c_1c_2p^{n_2}} f_2'^{c_1} f_1'^{-c_2p^{n_2}}; L, \zeta\right)_{p^k}$$
$$= (f_1', f_2'; L, \zeta)_{p^k} \otimes_L \left(\omega, (-1)^{c_1c_2p^{n_2}(p-1)} f_2'^{c_1} f_1'^{-c_2p^{n_2}}; L, \zeta\right)_{p^k}$$

where the last equality follows since $(\omega, (-1)^{p-1}\omega)_{p^k}$ is split (cf. Proposition 1.2.4.6), so that $(\omega, \omega^{c_1c_2p^{n_2}})_{p^k} = (\omega, (-1)^{(p-1)c_1c_2p^{n_2}})_{p^k}$. Recall $p^s = [L : F] = p^{k-r}$. Since $\mu_p \subseteq F$, and if $p = 2$, $\mu_4 \subseteq F$, we may apply Corollary 4.2.11 and Proposition 4.2.15 to obtain

$$\operatorname{cor}_{K/F}(t_1, t_2; K, \zeta)_{p^k}$$
$$= \operatorname{cor}_{L/F}\left[(f_1', f_2'; L, \zeta)_{p^k} \otimes_L \left(\omega, (-1)^{c_1c_2p^{n_2}(p-1)} f_2'^{c_1} f_1'^{-c_2p^{n_2}}; L, \zeta\right)_{p^k}\right]$$
$$= \left(f_1', f_2'^{e}; F, \zeta^{p^s}\right)_{p^r} \otimes_F \left(E/F, \sigma|_E, (-1)^{c_1c_2p^{n_2}(p-1)} f_2'^{c_1} f_1'^{-c_2p^{n_2}}\right)_{p^k},$$

where $e = 1$ unless $p = 2$ and $k > r$ in which case $e = 1 + 2^{r-1}$, and E and σ are described in the statement of the theorem. Note that $(-1)^e = -1$, as e is always odd. So

$$\left(f_1', f_2'^{e}; F, \zeta^{p^s}\right)_{p^r} = \left((-1)^{\epsilon_1} t_1^{p^{l_1}} t_2^{d} \omega^{-c_1}, (-1)^{\epsilon_2} t_2^{ep^{m_2}} \omega^{-ec_2p^{n_2}}; F, \zeta^{p^s}\right)_{p^r}.$$

Finally, for c prime to p and any integer $n \geq 0$, we have $(-1)^{c(p^n-1)} = (-1)^{p^n-1}$. Thus, as c_1, c_2 is prime to p, we have $f_2'^{c_1} = (-1)^{\epsilon_2} t_2^{c_1p^{m_2}} \omega^{-c_1c_2p^{n_2}}$ and $f_1'^{-c_2p^{n_2}} = (-1)^{p^{n_2}\epsilon_1} t_1^{-c_2p^{l_1+n_2}} \omega^{c_1c_2p^{n_2}} t_2^{-dc_2p^{n_2}}$, whence

$$(-1)^{c_1c_2p^{n_2}(p-1)} f_2'^{c_1} f_1'^{-c_2p^{n_2}} = (-1)^{p^{n_2}(p-1)} f_2'^{c_1} f_1'^{-c_2p^{n_2}}$$
$$= (-1)^{\epsilon_3} t_1^{-c_2p^{l_1+n_2}} t_2^{c_1p^{m_2} - dc_2p^{n_2}}.$$

This completes the proof. □

Remark 4.7.3. The formula in Theorem 4.7.2 simplifies greatly if p is odd, as $p^\alpha - 1$ is even for any $\alpha \geq 0$ and the factors of -1 disappear.

Recall that we had assumed $\mu_p \subseteq F$, or, if $p = 2$, $\mu_4 \subseteq F$. Now suppose that $\mu_p \nsubseteq F$ or, if $p = 2$, $\mu_4 \nsubseteq F$ and let F' be the field $F(\mu_p)$ or $F(\mu_4)$ according to whether p is odd or 2. By assumption, t_1, t_2, ω all have p-power order in K^*/F^*, thus, by Theorem 4.7.2

$$cor_{K/F'}(t_1, t_2)_{p^k} = (f_1', f_2'; \zeta)_{p^r} \otimes_{F'} (E/F', \sigma, b),$$

where $f_1', f_2', b \in F'$ have p-power order over F and $E = F(\mu_{p^l})$ for some l. The results from sections 4.5.1 and 4.5.2 describe how to compute $cor_{F'/F}(f_1', f_2'; \zeta)_{p^r}$ and $cor_{F'/F}(E/F', \sigma, b)$. Thus, we are able to compute $cor_{N/F}(t_1, t_2; \zeta)_{p^n}$ without any assumptions on the roots of unity present in F.

This generalization allows us to prove the following general result.

Theorem 4.7.4. *Suppose $F \subseteq N$ is a finite degree field extension. Suppose $\mu_n \subseteq N$ for some n. Let $s_1, s_2 \in N$ be elements such that s_1, s_2 each have finite order in N^*/F^*. Then we can compute $\mathrm{cor}_{N/F}(s_1, s_2; N)_n$ via Theorem 4.7.1 and Theorem 4.7.2.*

Proof. Suppose $s_1^{m_1}, s_2^{m_2} \in F$ for some $m_1, m_2 \in \mathbb{N}$. Let $m_1 = p_1^{a_1} \dots p_k^{a_k}, m_2 = p_1^{b_1} \dots p_k^{b_k}, n = p_1^{r_1} \dots p_k^{r_k}$, where we have $a_i, b_i, c_i \geq 0$ and p_i are all the primes which divide $m_1 m_2 n$. By primary decomposition, there exist $d_i \in \mathbb{Z}$ such that

$$(s_1, s_2; N)_n \cong (s_1, s_2; N)_{p_1^{r_1}}^{d_1} \otimes_N \dots \otimes_N (s_1, s_2; N)_{p_k^{r_k}}^{d_k}.$$

For $i = 1, \dots, k$, let $x_i = p_1^{a_1} \dots \widehat{p_i^{a_i}} \dots p_k^{a_k}$ and $y_i = p_1^{b_1} \dots \widehat{p_i^{b_i}} \dots p_k^{b_k}$. Then, there exist c_i such that $c_1 x_i y_i \equiv 1 \ mod \ {p_i}^{r_i}$. Let $T_i = (s_1^{x_i}, s_2^{y_i}; N)_{p_i^{r_i}}$, so $(s_1^{x_i})^{p_i^{a_i}}, (s_2^{y_i})^{p_i^{b_i}} \in F$, and

$$(s_1, s_2; N)_n \cong T_1^{c_1 d_1} \otimes_N \dots \otimes_N T_k^{c_k d_k}.$$

We may use Theorem 4.7.1 and Theorem 4.7.2 to compute $cor_{L/F}(T_i)$, hence we can compute $cor_{N/F}(s_1, s_2; N)_n$. $\square$

4.8 Application to Valuation Theory

We now apply Theorem 4.7.2 to a very specific situation. Let K, F, t_1, t_2 and all other constants be as defined in the development of Theorem 4.7.2. Let v be a valuation on F. We need two basic results first.

Lemma 4.8.1. *Fix $p \in \mathbb{N}$. Suppose A, B are subgroups of a p-torsion-free abelian group G. Let $\iota_1 : A/pA \to (A+B)/p(A+B)$ and $\iota_2 : (A \cap B)/p(A \cap B) \to B/pB$ be the obvious maps induced by inclusion. Then $\ker(\iota_1) \cong \ker(\iota_2)$. In particular, ι_1 is injective if and only if ι_2 is injective.*

Proof. We first have

$$\ker(\iota_1) = (A \cap p(A+B))\,/pA = (A \cap (pA + pB))\,/pA = ((A \cap pB) + pA)\,/pA.$$

By the second isomorphism theorem,

$$((A \cap pB) + pA)\,/pA \cong (A \cap pB)/(A \cap pB) \cap pA = (A \cap pB)/(pA \cap pB).$$

Suppose $pa = pb \in pA \cap pB$ for some $a \in A$ and $b \in B$. Then $p(b-a) = 0$ in G, whence $b = a$ as G is p torsion-free. So $pa = pb \in p(A \cap B)$, hence, $pA \cap pB = p(A \cap B)$ (the reverse inclusion being obvious). Thus,

$$(A \cap pB)/(pA \cap pB) = (A \cap pB)/p(A \cap B) = (A \cap B \cap pB)/p(A \cap B) = \ker(\iota_2).$$

So $\ker(\iota_1) \cong \ker(\iota_2)$. $\square$

Proposition 4.8.2. *Let F be a field with valuation v and let p be a prime with $p \neq \mathrm{char}(\overline{F})$. Let L be a totally ramified extension of F. Suppose $t_1, \ldots, t_n \in L^*$ are elements such that there exists an $N \in \mathbb{N}$ with $t_i^{p^N} \in F^*$ for all i. Let $K = F(t_1, \ldots, t_n)$. Then*

1. *$\Gamma_K = \Gamma_F + \langle v(t_1), \ldots, v(t_n) \rangle$. In particular, $o(t_i F^*) = o(v(t_i) + \Gamma_F)$.*
2. *$\Gamma_K / \Gamma_F \cong \langle t_1 F^*, \ldots, t_n F^* \rangle$.*

Remark 4.8.3. The proof of Prop. 4.8.2 is similar in nature to the methods used in [MW04, §2].

Proof. We first prove part 1. Suppose that part 1 of the proposition holds for $n = 1$. Set $K_j = F(t_1, \ldots, t_j)$ and suppose $k > 1$. Then, L is totally ramified over K_{k-1} and, by hypothesis, there exists an N such that $t_i^{p^N} \in F^* \subseteq K_{k-1}^*$. Thus, $\Gamma_{K_k} = \Gamma_{K_{k-1}} + \langle v(t_k)\rangle$, so, by induction, we can show that $\Gamma_{K_k} = \Gamma_F + \langle v(t_1), \ldots, v(t_k)\rangle$. Therefore, it is enough for part 1 just to consider the case $n = 1$.

Suppose $o(tF^*) = p^m$ in L^*/F^*. Set $K = F(t)$. Since L is totally ramified over F, the extension $F \subseteq K$ is totally ramified, whence p-pure. Then, by Proposition 4.6.3, $[K : F] = o(tF^*) = p^m$, so $|\Gamma_K : \Gamma_F| = [K : F] = p^m$. Suppose that $o(v(t)+\Gamma_F) = p^l$. Then there exists $f \in F^*$ such that $v(t^{p^l} f) = 0$ and $t^{p^l} f \in U_K$. Now $\overline{K} = \overline{F}$, so $\overline{t^{p^l} f} = \overline{y}$ for some $y \in U_F$. Let $u = t^{p^l} f y^{-1} \in K$; by construction $\overline{u} = \overline{1}$ and $o(uF^*) = o(t^{p^l} F^*) = p^{m-l}$.

Since $F(u)$ is an intermediate extension of $F \subseteq K$, we have $F \subseteq F(u)$ is p-pure. Then, by Proposition 4.6.3, $[F(u) : F] = o(uF^*) = p^{m-l}$. Let V_F be the valuation ring of F and let $V_F[x]$ denote the polynomial ring in one variable over V_F. Then, $V_F[u] \cong V_F[x]/(x^{p^{m-l}} - u)$, since the minimal polynomial of u over F is monic in $V_F[x]$. Let M_F be the (unique) maximal ideal of V_F and we have

$$V_F[u]/M_F V_F[u] \cong \overline{F}[x]/(x^{p^{m-l}} - \overline{u}) = \overline{F}[x]/(x^{p^{m-l}} - \overline{1}).$$

By assumption $p \neq char(\overline{F})$, so $x^{p^{m-l}} - \overline{1}$ is a separable polynomial. By the Chinese Remainder Theorem, $\overline{F}[x]/(x^{p^{m-l}} - \overline{1})$ is a direct sum of fields $\overline{F_1} \times \cdots \times \overline{F_k}$ with $\sum_{i=1}^{k} [\overline{F_i} : \overline{F}] = p^{m-l}$; note that k is the number of irreducible factors of $x^{p^{m-l}} - \overline{1}$ in $\overline{F}[x]$. Each field $\overline{F_i}$ corresponds to a maximal ideal M_i of $V_F[u]$ contracting to $M_F V_F[u]$ (note that these also correspond to the irreducible factors of $x^{p^{m-l}} - \overline{1}$ in $\overline{F}[x]$). Let D be the integral closure of V_F in $F[u]$. Since D is integral over $F[u]$, for each M_i, there is a maximal ideal N_i of D lying over M_i (i.e. $N_i \cap V_F[u] = M_i$). Each N_i corresponds to an extension v_i of v to $F(u)$ (cf. [End72, Theorem 13.4]). There are at least k extensions of v to $F(u)$, yet $F \subseteq F(u) \subseteq L$ and $F \subseteq L$ is totally ramified. By the fundamental inequality (cf. [End72, Theorem 17.5]), there is only one extension of v to L, so there is only one extension of v to $F(u)$, i.e. $k = 1$. Since k is the number of irreducible factors of $x^{p^{m-l}} - \overline{1}$, this forces $m = l$ (as $x - \overline{1}$ is always a factor).

Thus, $o(v(t) + \Gamma_F) = o(tF^*) = p^m$. So $|\Gamma_K : \Gamma_F| = [K : F] = p^m = |(\Gamma_F + \langle v(t)\rangle) : \Gamma_F|$, whence, $\Gamma_K = \Gamma_F + \langle v(t)\rangle$ (as $\Gamma_K \supseteq \Gamma_F + \langle v(t)\rangle$). This gives the first part of the proposition.

Let $C = \langle t_1 F^*, \ldots, t_n F^*\rangle$. Define $w : C \to \Gamma_K/\Gamma_F$ by $w(aF^*) = v(a) + \Gamma_F$. Since $\Gamma_K = \Gamma_F + \langle v(t_1), \ldots, v(t_n)\rangle$ by part 1., we have w is surjective. Now suppose $w(cF^*) = \Gamma_F$ for some $cF^* \in C$. Note that $F(c) \subseteq F(C) = K$ is a totally ramified extension and $c^{p^N} \in F^*$ for some $N \in \mathbb{N}$. Thus, by part 1., $\Gamma_{F(c)} = \Gamma_F + \langle v(c)\rangle = \Gamma_F$. Thus, $F(c) = F$, so $c \in F^*$. Thus, w is an isomorphism, proving 2. □

Theorem 4.8.4. *Suppose now that $K = F(t_1, t_2)$ is a totally ramified extension of F with respect to a valuation v, and suppose that $o(t_i F^*) = p^{m_i}$ for $m_i \in \mathbb{N}$. Suppose $T = (t_1, t_2; K)_{p^k}$ is TTR over K and let $T' = \mathrm{cor}_{K/F} T$. Then*

$$T' = \left((-1)^{\epsilon_1} t_1^{p^{l_1}} t_2^d, (-1)^{\epsilon_2} t_2^{p^{m_2}}; F\right)_{p^k},$$

with ϵ_1, ϵ_2, and d as defined in Theorem 4.7.2. Also, T' is TTR over F and

$$\Gamma_{T'} = \frac{1}{p^k}\left(\langle v(t_1), v(t_2)\rangle \cap \Gamma_F\right) + \Gamma_F \subseteq \Gamma_T.$$

Proof. Set $T' = \mathrm{cor}_{K/F} T$. By Theorem 4.7.2,

$$T' = \left((-1)^{\epsilon_1} t_1^{p^{l_1}} t_2^d, (-1)^{\epsilon_2} t_2^{p^{m_2}}; F\right)_{p^k},$$

where $\epsilon_1 = p^{l_1} - 1 + d(p-1)$, $\epsilon_2 = p^{m_2} - 1$, and

$$d = \begin{cases} 0 & \text{if } m_1 = l_1; \\ -c_3 p^{l_2} & \text{if } m_1 > l_1. \end{cases}$$

Note that K is totally ramified over F and $\mu_{p^k} \subseteq K$, so $\omega \in \mu_{p^k} \subseteq F$ and $n_1 = 0 = n_2$ in the notation of Theorem 4.7.2.

Let $C = \langle t_1F^*, t_2F^*\rangle \subseteq K^*/F^*$. Because K is totally ramified over F and $t_1^{p^{m_1}}, t_2^{p^{m_2}} \in F$, we may apply Proposition 4.8.2 and get $\Gamma_K = \langle v(t_1), v(t_2)\rangle + \Gamma_F$ and $C \cong \Gamma_K/\Gamma_F$. In particular, $o\,(v(t_2)+\Gamma_F) = o(t_2F^*) = [F(t_2) : F] = p^{m_2}$ and $\langle v(t_1) + \Gamma_F\rangle \cap \langle v(t_2) + \Gamma_F\rangle = \langle p^{l_i}v(t_i) + \Gamma_F\rangle$, where $p^{l_1} = [K : F(t_2)]$ and $p^{l_2} = [K : F(t_1)]$. By construction, we have $v(t_1^{p^{l_1}}t_2^d) = 0$. Let $h : \mathbb{Z}\times\mathbb{Z} \to \Gamma_K/\Gamma_F$ be the map defined by $h(a, b) = av(t_1) + bv(t_2) + \Gamma_F$. Let h_1 and h_2 be the restriction of h to the first and second components of $\mathbb{Z} \times \mathbb{Z}$. Then $ker(h_2) = \langle p^{m_2}\rangle$. Also, $h_1(p^{l_1}) = v(t_1^{p^{l_1}}) = -v(t_2^d) = h_2(-d)$ generates the intersection of $im(h_1)$ and $im(h_2)$. Since $p^{l_1} \mid p^{m_1}$ (as $l_1 \leq m_1$), Lemma 4.4.1 tells us that $ker(h)$ is generated by (p^{l_1}, d) and $(0, p^{m_2})$.

Let $A = \langle v(t_1), v(t_2)\rangle \subseteq \Gamma_K$ and let $B = \Gamma_F$. We saw above that $A + B = \Gamma_K$, which is a torsion-free group. Now $T = (t_1, t_2; K)_{p^k}$ is TTR over K, so $v(t_1), v(t_2)$ have independent images in $\Gamma_K/p\Gamma_K$. In other words, the map, $\iota_1 : A/pA \to (A+B)/p(A+B)$, induced by inclusion, is injective. Then, by Lemma 4.8.1, $\iota_2 : (A\cap B)/p(A\cap B) \to B/pB$ is injective. In other words, free generators of $A\cap\Gamma_F$ have independent images in $\Gamma_F/p\Gamma_F$.

Now $A = \langle v(t_1), v(t_2)\rangle$ is torsion-free of rank 2, so there is an isomorphism $g : A \to \mathbb{Z}\times\mathbb{Z}$ (given by $av(t_1)+bv(t_2) \mapsto (a, b)$). Then $ker(hg) = A\cap\Gamma_F$ is torsion-free with the same rank as A (as $A/(A\cap\Gamma_F)$ is torsion). Since $ker(hg)$ is freely generated by $v(t_1^{p^{l_1}}t_2^d)$ and $v(t_2^{p^{m_2}})$, we showed in the preceding paragraph that these elements have independent images in $\Gamma_F/p\Gamma_F$ and T' is TTR over F. Finally,

$$\Gamma_{T'} = \Gamma_F + \frac{1}{p^k}\langle v(t_1^{p^{l_1}}t_2^d), v(t_2^{p^{m_2}})\rangle = \frac{1}{p^k}(A\cap\Gamma_F) + \Gamma_F.$$

□

Remark 4.8.5. Using Theorem 4.8.4 and Theorem 4.7.1, we can compute $cor_{N/F}\,(t_1, t_2; N)_{p^n}$, where N is any field over F containing t_1, t_2 (where t_1, t_2 are as in Theorem 4.8.4). The resulting algebra is TTR over F, and has value group $\frac{u}{p^k}\,(\langle v(t_1), v(t_2)\rangle \cap \Gamma_F)$, where k are u are defined by $\mu_{p^n}\cap K = \mu_{p^k}$ and $u = [N : K(\mu_{p^n})]$ $(K = F(t_1, t_2))$.

Theorem 4.8.6. *Let L be any totally ramified field extension of a valued field F and let p be a prime with $\mathrm{char}(\overline{F}) \neq p$. Suppose $t_1, \dots, t_{2n} \in L^*$ and there exists an $N \in \mathbb{N}$ such that $t_i^{p^N} \in F^*$ for all i. Suppose further that $T = (t_1, t_2; L)_{p^{k_1}} \otimes_L \cdots \otimes_L (t_{2n-1}, t_{2n}; L)_{p^{k_n}}$ is a TTR division algebra over L and let $T' = \mathrm{cor}_{L/F} T$. Then the underlying division algebra T' is TTR over F, and furthermore, we may use Theorem 4.8.4 and Theorem 2.2.1 to compute T', $\Gamma_{T'}$, and the canonical pairing $C_{T'}$ on T'.*

Proof. Since L is totally ramified over F, we have $\mu_{p^\infty} \cap L = \mu_{p^\infty} \cap F$, so the extension $F \subseteq L$ is p-pure. By using the projection formula (cf. Theorem 4.2.3), we may assume that $L = F(t_1, \dots, t_{2n})$. Thus, $[L : F]$ is a power of p (via Proposition 4.6.3 applied repeatedly).

Now, T is TTR over L. Let

$$G = \langle (1/p^{k_1})v(t_1), (1/p^{k_1})v(t_2), \dots, (1/p^{k_n})v(t_{2n-1}), (1/p^{k_n})v(t_{2n}) \rangle.$$

Let $\mathcal{T}$ be any armature of T. By [TW87, Prop. 3.5], $\mathcal{T} \cong \Gamma_T/\Gamma_L = (G + \Gamma_L)/\Gamma_L$ via $\overline{v}$, the map induced by v. Thus, $(G + \Gamma_L)/\Gamma_L \cong \mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_n}} \times \mathbb{Z}_{p^{k_n}}$. In particular,

$$(\langle (1/p)v(t_1), (1/p)v(t_2), \dots, (1/p)v(t_{2n-1}), (1/p)v(t_{2n}) \rangle + \Gamma_L)/\Gamma_L \cong (\mathbb{Z}_p)^{2n},$$

whence $v(t_1), \dots, v(t_{2n})$ have $\mathbb{Z}/p\mathbb{Z}$-independent images in $\Gamma_L/p\Gamma_L$.

Let $C = \langle t_1, \dots, t_{2n} \rangle \subseteq L^*$ and let $w : C \to \Gamma_L/\Gamma_F$ be defined by $w(c) = v(c) + \Gamma_F$. By Proposition 4.8.2, we have $C/(C \cap F^*) \cong \Gamma_L/\Gamma_F$ via the map induced by v, thus $v(c) \in \Gamma_F$ if and only if $c \in F^*$. So $ker(w) = C \cap F^*$ and $v(C \cap F^*) = v(ker(w)) = v(C) \cap \Gamma_F$.

Since $v(t_1), \dots, v(t_{2n})$ have independent images in $\Gamma_L/p\Gamma_L$, we have $v : C \to \Gamma_L$ is injective and $v(C)/pv(C)$ maps injectively into $\Gamma_L/p\Gamma_L$. By Proposition 4.8.2, $\Gamma_L = v(C) + \Gamma_F$. Set $A = v(C)$ and $B = \Gamma_F$. Now $A, B \subseteq \Gamma_L$ and Γ_L is a torsion-free abelian group, and by the above A/pA maps injectively into $(A + B)/p(A + B)$, so by Lemma 4.8.1 $A \cap B/p(A \cap B)$ maps injectively into B/pB. Note that $A \cap B =$

$v(C) \cap \Gamma_F = v(C \cap F^*)$, and $v(C \cap F^*) \subseteq v(C)$, the latter group being isomorphic to C, which is a torsion-free, finitely generated $\mathbb{Z}$-module. Thus, $v(C \cap F^*)$ is a torsion-free, finitely generated (hence free) $\mathbb{Z}$-module and any base as a free $\mathbb{Z}$-module has images which are $\mathbb{Z}/p\mathbb{Z}$-independent in $\Gamma_F/p\Gamma_F$. Now $v : C \cap F^* \to v(C \cap F^*)$ is an isomorphism since v on C is injective, so any $\mathbb{Z}$-base of $C \cap F^*$ has images which are $\mathbb{Z}/p\mathbb{Z}$-independent in $\Gamma_F/p\Gamma_F$. For $i = 1, \dots n$, let $T_i = (t_{2i-1}, t_{2i}; L)_{p^{k_i}}$. Let $T'_i = cor_{L/F} T_i$.

Assume first that p is odd. By Theorem 4.2.3 and Theorem 4.8.4, we have $T'_i = (s_{2i-1}, s_{2i}; F)_{p^{k_i - r_i}}$, where $p^{r_i} = [L : F(t_{2i-1}, t_{2i})]$ and $s_{2i-1}, s_{2i} \in C \cap F^*$ are as in the formula given in Theorem 4.8.4. Thus, $T' \sim \bigotimes_{i=1}^n (s_{2i-1}, s_{2i}; F)_{p^{k_i - r_i}}$. Theorem 2.3.2 applies because all the s_i are in $C \cap F^*$, which we just proved has a generating set with $\mathbb{Z}_p$-independent images in $\Gamma_F/p\Gamma_F$. (Such a generating set would be the t_i of Theorem 2.3.2.) Therefore, we may apply Theorem 2.2.1 to obtain T', $\Gamma_{T'}$ and $C_{T'}$.

Suppose instead that $p = 2$. Then $T'_i = ((-1)^{\epsilon_{2i-1}} s_{2i-1}, (-1)^{\epsilon_{2i}} s_{2i}; F)_{2^{k_i - r_i}}$, where $2^{r_i} = [L : F(t_{2i-1}, t_{2i})]$ and $\epsilon_{2i-1}, \epsilon_{2i}$, and $s_i \in C \cap F^*$ are as defined in Theorem 4.7.2. Without loss of generality, we may suppose that $k_1 \geq k_2 \geq \cdots \geq k_n$, i.e. the symbols T_i are ordered in order of decreasing degree. Also, let $m \leq n$ be the largest index for which $k_m = k_1$. Suppose $r_j > 0$ for $j = 1, \dots, m$, then $deg(T'_i) = 2^{k_i - r_i} < 2^{k_1}$ for all $i = 1, \dots, n$. Let $s = \max\{2^{k_1 - r_1}, \dots, 2^{k_n - r_1}\} < 2^{k_1}$. Since L is totally ramified over F and $\mu_{2^{k_1}} \subseteq L$, we have $\mu_{2s} \subseteq \mu_{2^{k_1}} \subseteq F$. In addition, -1 is an s-th power (as $s \leq 2^{k_1 - 1}$), so we may remove the factors of -1 in T_i. In other words, $T' \sim \bigotimes_{i=1}^n (s_{2i-1}, s_{2i}; F)_{p^{k_i - r_i}}$ and $\mu_{2s} \subseteq F$. By Remark 2.3.3 following Theorem 2.3.2, we may apply Theorem 2.2.1 and obtain T', $\Gamma_{T'}$ and $C_{T'}$.

It remains to see what happens when $r_j = 0$ for some $j = 1, \dots, m$. Without loss of generality, we may suppose that $r_1 = 0$. In other words, $[L : F(t_1, t_2)] = 1$, so $L = F(t_1, t_2)$. Suppose first that either $F(t_2) = L$ or $F(t_1) = L$. By symmetry, we need only consider the case $F(t_1) = L$ so $\Gamma_L = \langle v(t_1) \rangle + \Gamma_F$. Then, for $i = 2, 3, \dots, 2n$, we have $v(t_i) = a_i v(t_1) + v(f_i)$, where $f_i \in F$. If we let $x_i = t_i t_1^{-a_i} \in L$, we have $v(x_i) \in \Gamma_F$ and $x_i^{2^N} \in F^*$ for some $N \in \mathbb{N}$ (since this is true of t_i and t_1). Set $K_i = F(x_i)$ and apply Proposition 4.8.2 to get $\Gamma_{K_i}/\Gamma_F \cong \langle x_i F^* \rangle$, whence $x_i \in F^*$. By assumption, $\{v(t_1), v(t_2), \ldots, v(t_{2n})\}$ maps to an independent set in $\Gamma_L/2\Gamma_L$. Since we are making a linear change of variables, we see that $v(t_1), v(x_2), v(x_3), \ldots, v(x_{2n})$ must have independent images in $\Gamma_L/2\Gamma_L$. Since $2\Gamma_F \subseteq 2\Gamma_L$ and $v(x_2), v(x_3), \ldots, v(x_{2n}) \in \Gamma_F$, the set $\{v(x_2), v(x_3), \ldots, v(x_{2n})\}$ is independent in $\Gamma_F/2\Gamma_F$. For $i = 2, 3, \ldots, n$, we compute in $Br(L)$ (using the symbol identities given in Prop. 1.2.4.8 and Prop. 1.2.4.1)

$$\begin{aligned}
T_i &= (t_{2i-1}, t_{2i}; L)_{2^{k_i}} \\
&= (t_1^{a_{2i-1}} x_{2i-1}, t_1^{a_{2i}} x_{2i}; L)_{2^{k_i}} \\
&= (t_1, t_1^{a_{2i-1}a_{2i}} x_{2i}^{a_{2i-1}}; L)_{2^{k_i}} \otimes_L (x_{2i-1}, t_1^{a_{2i}}; L)_{2^{k_i}} \otimes_L (x_{2i-1}, x_{2i}; L)_{2^{k_i}} \\
&= \left(t_1, (-1)^{a_{2i-1}a_{2i}} x_{2i}^{a_{2i-1}} x_{2i-1}^{-a_{2i}}; L\right)_{2^{k_i}} \otimes_L (x_{2i-1}, x_{2i}; L)_{2^{k_i}}.
\end{aligned}$$

Also, we have $T_1 = (t_1, t_2; L)_{2^{k_1}} = (t_1, t_1^{a_2} x_2; L)_{2^{k_1}} = (t_1, (-1)^{a_2} x_2; L)_{2^{k_1}}$. Let $\epsilon = a_2 + \sum_{i=2}^{n} (a_{2i-1} a_{2i} 2^{k_1 - k_i})$ and let $x_2' = (-1)^{\epsilon} x_2 \prod_{i=2}^{n} x_{2i}^{2^{k_1-k_i} a_{2i-1}} x_{2i-1}^{-2^{k_1-k_i} a_{2i}}$. Then, using $k_1 = \max\{k_1, \ldots, k_n\}$, we have

$$\begin{aligned}
T &= T_1 \otimes_L \cdots \otimes_L T_n \\
&= (t_1, (-1)^{a_2} x_2; L)_{2^{k_1}} \otimes_L \\
&\qquad \bigotimes_{i=2}^{n} \left(\left(t_1, (-1)^{a_{2i-1}a_{2i}} x_{2i}^{a_{2i-1}} x_{2i-1}^{-a_{2i}}; L\right)_{2^{k_i}} \otimes_L (x_{2i-1}, x_{2i}; L)_{2^{k_i}} \right) \\
&= \left(t_1, (-1)^{\epsilon} x_2 \prod_{i=2}^{n} x_{2i}^{2^{k_1-k_i} a_{2i-1}} x_{2i-1}^{-2^{k_1-k_i} a_{2i}}; L \right)_{2^{k_1}} \otimes_L \bigotimes_{i=2}^{n} (x_{2i-1}, x_{2i}; L)_{2^{k_i}} \\
&= (t_1, x_2'; L)_{2^{k_1}} \otimes_L \bigotimes_{i=2}^{n} (x_{2i-1}, x_{2i}; L)_{2^{k_i}}
\end{aligned}$$

Recall that $C = \langle t_1, \ldots t_{2n} \rangle = \langle t_1, x_2, x_3, \ldots, x_{2n} \rangle$. Since $t_1, x_2', x_3, \ldots, x_{2n}$ is obtained from $t_1, x_2, x_3, \ldots, x_{2n}$ by a linear change of variables, $C = \langle t_1, x_2', x_3, \ldots, x_{2n} \rangle$. Now $C/(C \cap F^*)$ is torsion, since the t_i all have p-power order over F and $x_i \in C = \langle \{t_i\}_{i=1}^{2n} \rangle$. Thus, $C \cap F^*$ is free a $\mathbb{Z}$-module with rank equal to the rank of C, namely, $2n$. Let $o(t_1 F^*) = 2^{m_1}$ and set $x_1 = t_1^{2^{m_1}}$. Then $x_1, x_2', x_3, \ldots, x_{2n}$ generate $C \cap F^*$; since $C \cap F^*$ has rank $2n$, these generators form a free $\mathbb{Z}$-module base for $C \cap F^*$. Consequently,

$x_1, x_2', x_3, \dots, x_{2n}$ have $\mathbb{Z}/2\mathbb{Z}$-independent images in $\Gamma_F/2\Gamma_F$ by Lemma 4.8.1 with $A = C$ and $B = F^*$ and the fact that $v : C \cap F^* \to v(C \cap F^*)$ is an isomorphism. Using either Proposition 4.8.4 or Theorem 4.2.3, we have

$$cor_{L/F}(T) = \Big((-1)^{2^{m-1}-1}x_1, x_2'; F\Big)_{2^{k_1}} \otimes_F \bigotimes_{i=2}^{n} (x_{2i-1}, x_{2i}; F)_{2^{k_i - m_1}} ,$$

which is TTR over F because the slots have independent images in $\Gamma_F/2\Gamma_F$.

Now suppose $L \neq F(t_1)$ and $L \neq F(t_2)$. Replace F by $F' = F(t_2)$, so $L = F'(t_1)$. The preceding calculation shows that $cor_{L/F'}(T)$ is TTR over F'. Note that $\pm x_1, x_2, \dots, x_{2n}$ all have some 2^N-power in F for some $N \in \mathbb{N}$, so the same argument applies for computing $T' = cor_{F'/F}(cor_{L/F'}(T))$. Thus, T' is TTR over F. □

Remark 4.8.7. Hwang proved the following result in [Hwa95b, Th. 13] which we will obtain as a corollary of Theorem 4.8.6.

Corollary 4.8.8. *Suppose that F is Henselian and let L be any finite-degree TRRT extension of F. Let T be a TTR division algebra over L and let $T' = cor_{L/F}T$. Then T' is TTR over F.*

Proof. We will first describe how to rewrite T as a tensor product of symbol algebras whose slots have finite order modulo F^*. Since L is TRRT over F, there exist $t_1, \dots, t_n$ radical over F such that $\Gamma_L = \Gamma_F + \langle v(t_1), \dots, v(t_n)\rangle$. Let $C = \langle t_1, \dots, t_n\rangle \subseteq L^*$.

If $a \in L$, then $v(a) = v(fc)$ for some $f \in F^*$ and $c \in C$. Then $af^{-1}c^{-1} \in U_L$. Because L is totally ramified over F, we have $\overline{F} = \overline{L}$. Thus, for some $u \in U_F$, we have $\overline{af^{-1}c^{-1}} = \overline{u}$. Let $x = u^{-1}af^{-1}c^{-1} \in L^*$. Since F is Henselian and x is a 1-unit, $x \in L^{*i}$ for all $i \in \mathbb{N}$ with i prime to $char(\overline{F})$. Note that $ax^{-1} = ufc$ and $ufc \in L^*$ has finite order modulo F^*.

Now suppose that T is TTR over L. By Theorem 1.4.5 $T \cong \bigotimes_{i=1}^{k} (\alpha_i, \beta_i; L)_{n_i}$, for some $\alpha_i, \beta_i \in L$ and n_i prime to $char(\overline{F})$. The previous paragraph showed that for each i, there exists 1-units $y_i, z_i \in L^*$ such that $\alpha_i y_i$ and $\beta_i z_i$ have finite order modulo F^*. Since $y_i, z_i \in L^{*n_i}$, by Prop. 1.2.4.4, we have $T \cong \bigotimes_{i=1}^{n} (\alpha_i y_i, \beta_i z_i; L)_{n_i}$. Let $p_1, \dots, p_m$ be all the primes dividing $deg(T)$ (so $p_i \neq char(\overline{F})$). By applying the primary decomposition in the same manner as in the proof of Theorem 4.7.4, we can write $T = T_1 \otimes_L \cdots \otimes_L T_m$, where each T_i is TTR over L and has degree a power of p_i. Furthermore, each T_i is similar to a tensor product of symbols whose slots have p_i^N-th powers in F. Thus, we may apply Theorem 4.8.6 to each T_i to see that $T_i' = cor_{L/F} T_i$ is TTR over F. Since T_i' are TTR algebras of relative prime degrees, we have $T' = cor_{L/F} T = T_1' \otimes_F \cdots \otimes_F T_m'$ is TTR over F. $\square$

4.9 Corestriction Over Generalized Local Fields

For the remainder of this section, let F be a GLF. Suppose $L \supseteq F$ is a tame finite degree field extension. We know that there is a field E such that $E \supseteq F$ is unramified and $L \supseteq E$ is tame totally ramified. Then, by [Sch50, p.64, Th. 3], $L \supseteq E$ is totally ramified of radical type (TRRT), i.e. there exist $n_1, \ldots, n_m$ with $n_1 \ldots n_m = n = [L : E]$ and $t_1, \ldots t_m \in E$ such that $L = E(\sqrt[n_1]{t_1}, \ldots, \sqrt[n_m]{t_m})$ and $nv(t_i)/n_i + n\Gamma_E$ are independent of order n_i in $\Gamma_E/n\Gamma_E$.

If $D \in \mathcal{D}(K)$, then, by Cor. 2.1.2 $D \sim N \otimes_L T$ with N NSR over F and T is TTR over F. It suffices to show how to compute $cor_{L/F}N$ and $cor_{L/F}T$ where L is either unramified or TRRT over F. We will let ${}^cD$ stand for the underlying division algebra of $cor_{L/F}D$.

4.9.1 $L \supseteq F$ Is Unramified

Proposition 4.9.1. *Suppose L is unramified over F and N is NSR over L. Then ${}^cN$ is NSR over F with $[N : L] = [{}^cN : F]$ and $\Gamma_{{}^cN} = \Gamma_N$.*

Remark 4.9.2. Proposition 4.9.1 verifies some of the information provided in [Hwa95a, Thm. 2.4]. Hwang proved that ${}^cN$ is NSR and has value group contained in Γ_N assuming only F Henselian and L/F unramified. In the GLF case, more is true; in fact the value group stays the same.

Proof. By Prop. 2.1.3, $N \cong (M/L, \tau, b)$, where M/L is unramified, τ generates $Gal(M/L)$ and $b \in L^*$. Since L is unramified over F, we have $\Gamma_F = \Gamma_L$, so $b = ua$, where $u \in U_L$ and $a \in F^*$. By Prop. 2.1.1, $(M/L, \tau, u)$ is split, so $N \cong (M/L, \tau, a)$. By Prop. 2.1.3, M is cyclic over F, whence we use Lemma 4.2.14 to obtain

$$ {}^cN = cor_{L/F}(M/L, \tau, a) = (E/F, \sigma|_E, a), $$

where σ is a generator of $Gal(M/F)$ satisfying $\sigma^{[L:F]} = \tau$ and E is determined by $F \subseteq E \subseteq M$ and $[E : F] = [M : L]$. Thus, ${}^cN$ is NSR, $\Gamma_{{}^cN} = \Gamma_N$ (both are generated by $v(b)/[M : L] = v(a)/[E : F]$ over $\Gamma_F = \Gamma_L$), and $[N : L] = [M : L]^2 = [E : F]^2 = [{}^cN : F]$. □

Proposition 4.9.3. *Suppose L is unramified over F. Let T be a TTR division algebra over L with $T \cong T_1 \otimes_L \cdots \otimes_L T_k$ where each T_i is a symbol of degree n_i. Then ${}^cT \sim N \otimes_F T'$ where N is NSR over F and T' is TTR over F. Suppose $N_{L/F}(\mu_{n_i}) = \mu_{d_i}$ for some $d_i \mid n_i$. Then, $\Gamma_{{}^cT} = \Gamma_N + \Gamma_{T'} \subseteq \Gamma_T$ and*

$$\Gamma_{T'} = \sum_{i=1}^{k} \tfrac{n_i}{d_i}[L : F(\mu_{n_i})]\Gamma_{T_i}.$$

Furthermore, $[\overline{{}^cT} : \overline{F}] = (ind\ N)/[(\Gamma_N \cap \Gamma_T) : \Gamma_F]$.

Proof. For each i, there exist $\alpha_i, \beta_i \in L$ such that $T_i = (\alpha_i, \beta_i; L)_{n_i}$. Now $\Gamma_L = \Gamma_F$ as $L \supseteq F$ is unramified. Thus, there exist $x_i, y_i \in U_L$ and $a_i, b_i \in F$ such that $T_i = (x_i a_i, y_i b_i; L)_{n_i}$. So, we may write $T \sim A \otimes_L B$, where

$$A = (a_1, b_1; L)_{n_1} \otimes_L \cdots \otimes_L (a_k, b_k; L)_{n_k},$$

and

$$B = \bigotimes_{i=1}^{k} \left((x_i, y_i b_i; L)_{n_i} \otimes_L (a_i, y_i; L)_{n_i} \right).$$

The underlying division algebra of B is NSR, and can be computed via Lemma 3.1.1, whence Prop. 4.9.1 gives us that $N = cor_{L/F}(B)$ is NSR and $\Gamma_N = \Gamma_B \subseteq \Gamma_T$. Also, A is TTR over L. Let $T_i' = cor_{L/F}(a_i, b_i; L)_{n_i}$. Since $a_i, b_i \in F^*$, we may apply Theorem 4.2.3 followed by Theorem 4.2.4 and Remark 4.2.5 to get

$$\begin{aligned} T_i' &= cor_{L/F}(a_i, b_i; L)_{n_i} \\ &= cor_{F(\mu_{n_i})/F}(a_i, b_i; L)_{d_i}^{[L:F(\mu_{n_i})]} \\ &= (a_i, b_i^{c_i}; L)_{d_i}^{[L:F(\mu_{n_i})]}, \end{aligned}$$

where $N_{L/F}(\mu_{n_i}) = \mu_{d_i}$ and $c_i \in \mathbb{Z}$ is prime to d_i (c_i is described in Remark 4.2.5). So

$$\begin{aligned} \Gamma_{T_i'} &= \frac{[L : F(\mu_{n_i})]}{d_i}\langle v(a_i), c_i v(b_i)\rangle + \Gamma_F \\ &= \frac{n_i}{d_i}[L : F(\mu_{n_i})]\left(\frac{1}{n_i}\langle v(a_i), v(b_i)\rangle\right) + \Gamma_F \\ &= \frac{n_i}{d_i}[L : F(\mu_{n_i})]\Gamma_{T_i} + \Gamma_F. \end{aligned}$$

Let $T' = T'_1 \otimes_F \cdots \otimes_F T'_k = \operatorname{cor}_{L/F} A$. Let $n = n_1 \dots n_k$. Note that $a_1^{n/n_1}, b_1^{n/n_1}, \dots, a_k^{n/n_k}, b_k^{n/n_k}$ have independent images in $\Gamma_L/n\Gamma_L$ of orders $n_1, n_1, \dots, n_k, n_k$. Thus, the same condition holds for $a_1^{d/d_1}, b_1^{c_1 d/d_1}, \dots, a_k^{d/d_k}, b_k^{c_k d/d_k}$ in $\Gamma_F/d\Gamma_F$, whence T' is TTR over F with value group

$$\Gamma_{T'} = \sum_{i=1}^{k} \tfrac{n_i}{d_i}[L : F(\mu_{n_i})]\Gamma_{T_i} + \Gamma_F.$$

Finally, the fact about $\overline{{}^cT}$ comes from Corollary 2.1.5 since $N \otimes_F T'$ gives a decomposition of ${}^cT$ into NSR and TTR parts. $\square$

Remark 4.9.4. Given $D \in \mathcal{D}(L)$, we can find N, T such that $D \sim N \otimes_L T$. Then, using Prop. 4.9.1 and Prop. 4.9.3, we can compute ${}^cD \sim {}^cN \otimes_F {}^cT \sim N' \otimes_F T'$, where N' is NSR over F and T' is TTR over F. Thus, by the remarks following Prop. 2.1.4, we can compute $[{}^cD : F]$, $[\overline{{}^cD} : \overline{F}]$, and $\Gamma_{{}^cD}$. Also, Theorem 2.4.1 gives ${}^cD$ explicitly.

Remark 4.9.5. Now suppose F is any Henselian valued field. For L unramified over F and T TTR over F, Hwang gave bounds for $\Gamma_{{}^cT}$ in [Hwa95a, Thm. 4.4]. The formula $\Gamma_{{}^cT} = \Gamma_N + \Gamma_{T'}$ in Prop. 4.9.3 is still valid (with $\Gamma_{T'}$ defined in Prop. 4.9.3), although we will not give a proof of this. In fact, we may still decompose $T \sim A \otimes_L B$ as in the proof and ${}^cT \sim N \otimes_F T'$ where $N = {}^cB$ is NSR and $T = {}^cA$ is TTR. However, there is no exact formula for Γ_N, so knowing $\Gamma_{{}^cT} = \Gamma_N + \Gamma_{T'}$ is, at best, a bound for $\Gamma_{{}^cT}$. The residue information given in Prop. 4.9.3 is only valid when $\overline{{}^cT}$ is a field, which is always the case when F is a GLF.

4.9.2 $L \supseteq F$ is TRRT

Suppose L is TRRT over F. Then, there are $n_1, \dots, n_m \in \mathbb{N}$ with $n_1 \dots n_m = n = [L : F]$ and $t_1, \dots, t_m \in F$ such that $L = F(\sqrt[n_1]{t_1}, \dots, \sqrt[n_m]{t_m})$ and $nv(t_i)/n_i$ are independent of order n_i in $\Gamma_F/n\Gamma_F$.

Proposition 4.9.6. *Suppose N is NSR over L. Let $N = (M/L, \sigma, b)_k$ where M is an unramified extension of L and $b \in L^*$ has value which has order k in $\Gamma_L/k\Gamma_L$. Let*

$l = o(v(b) + \Gamma_F)$. Then, ${}^cN$ is NSR over F with $ind({}^cN) = [\overline{{}^cN} : \overline{F}] = k/gcd(k, n/l)$ and $\Gamma_{{}^cN} = n\Gamma_N + \Gamma_F$.

Proof. Suppose $v(b^l) = v(a)$ for some $a \in F^*$. Then $b^l = au$ for some $u \in U_L$. By Prop. 2.1.3, there are fields E and M' with E cyclic unramified over F and M' cyclic unramified over L such that $[E : F] = kl$ and $[M' : M] = l$. Thus, by Prop. 1.2.6,

$$N = (M/L, \sigma, b)_k \sim (M'/L, \overline{\sigma}, b^l)_{kl} = (M'/L, \overline{\sigma}, au)_{kl},$$

where $\overline{\sigma}$ is any extension of σ to M' such that $\overline{\sigma}$ generates $Gal(M'/L)$. Then, as L is a GLF, by Prop. 2.1.1, $N \sim (M'/L, \overline{\sigma}, a)_{kl}$. Now, E is unramified over F and L is totally ramified over F, so E and L are linearly disjoint over F. Thus, $E \otimes_F L = EL$ is unramified over L and $[EL : L] = [E : F] = kl$, whence, by Prop. 2.1.3, $EL = M'$. Then, by Prop. 1.2.5,

$$res_{L/F}(E/F, \overline{\sigma}|_E, a)_{kl} = (EL/L, \overline{\sigma}, a)_{kl} = (M'/L, \overline{\sigma}, a)_{kl}.$$

So,

$${}^cN = cor_{L/F} res_{L/F}(E/F, \overline{\sigma}|_E, a)_{kl} = (E/F, \overline{\sigma}|_E, a)^n_{kl}.$$

Then, by a character calculation (cf. Lemma 3.1.1),

$$\Gamma_{{}^cN} = \langle (n/(kl)v(a)\rangle + \Gamma_F = \langle (n/k)v(b)\rangle + \Gamma_F = n\Gamma_N + \Gamma_F,$$

since $n\Gamma_L \subseteq \Gamma_F$ and $\Gamma_N = \langle v(b)/k\rangle + \Gamma_L$.

Now set $A = \langle v(b)\rangle$ and $B = \Gamma_F$. Then $A/kA \to (A + B)/k(A + B)$ is injective since $v(b)$ has order k in $\Gamma_L/k\Gamma_L$. By Lemma 4.8.1, the map $(A \cap B)/k(A \cap B) \to B/kB$ is injective. Now, $A \cap B = \langle v(a)\rangle$, so, $v(a)$ has order k in $\Gamma_F/k\Gamma_F$. Let $d = gcd(k, n/l)$ and let E' be the unique cyclic unramified extension of F of degree k/d. Then, ${}^cN \sim (E/F, \overline{\sigma}|_E, a)^n_{kl} \sim (E'/F, \overline{\sigma}|_{E'}, a)^{n/ld}_{k/d}$. The last algebra is an NSR division algebra, whence $ind({}^cN) = [\overline{{}^cN} : \overline{F}] = k/gcd(k, n/l)$. □

Proposition 4.9.7. *Suppose T is TTR over L. Then we can compute ${}^cT$, $\Gamma_{{}^cT}$, and $C_{{}^cT}$ using Theorem 4.8.6.*

Proof. The result follows immediately from Theorem 4.8.6 and Remark 4.8.8. □

Bibliography

[Alb03] T. Albu, *Cogalois theory*, Marcel Dekker Inc., New York, 2003. MR 1 989 999

[Ami72] S. A. Amitsur, *On central division algebras*, Israel J. Math. **12** (1972), 408–420. MR 47 #6763

[BHN32] R. Brauer, H. Hasse, and E. Noether, *Beweis eines Hauptsatzes in der Theorie der Algebren*, J. Reine Angew. Math. **167** (1932), 399–404.

[Bro94] K. S. Brown, *Cohomology of groups*, Springer-Verlag, New York, 1994. MR 96a:20072

[Bru95] E. S. Brussel, *Noncrossed products and nonabelian crossed products over* $\mathbf{Q}(t)$ *and* $\mathbf{Q}((t))$, Amer. J. Math. **117** (1995), no. 2, 377–393. MR 96a:16014

[Bru01] ———, *The division algebras and Brauer group of a strictly Henselian field*, J. Algebra **239** (2001), no. 1, 391–411. MR 2002b:16027

[Bru04] ———, *Twisted bilinear forms and the Brauer group (preprint)*, http://www.mathcs.emory.edu/∼brussel/Papers/twist.html, March 2004.

[CF67] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory*, Academic Press, London, 1967. MR 35 #6500

[dOV84] M. A. de Orozco and W. Y. Vélez, *The torsion group of a field defined by radicals*, J. Number Theory **19** (1984), no. 2, 283–294. MR 86g:12009

[Dra83] P. K. Draxl, *Skew fields*, Cambridge University Press, Cambridge, 1983. MR 85a:16022

[Dra84] ———, *Ostrowski's theorem for Henselian valued skew fields*, J. Reine Angew. Math. **354** (1984), 213–218. MR 86g:12008

[End72] O. Endler, *Valuation theory*, Springer-Verlag, New York, 1972. MR 50 #9847

[Ers82] Y. L. Ershov, *Valued division rings (Russian)*, Fifth All Union Symposium, Theory of Rings, Algebras, and Modules, Akad. Nauk SSSR Sibirsk. Otdel. Inst. Mat., Novosibirsk, 1982, pp. 53–55. MR 83m:16001

[FK00] I. Fesenko and M. Kurihara (eds.), *Invitation to higher local fields*, Geometry & Topology Publications, Coventry, 2000. MR 2001h:11005, http://www.emis.ams.org/journals/UW/gt/gtmcontents3.html

[GV81] D. Gay and W. Y. Vélez, *The torsion group of a radical extension*, Pacific J. Math. **92** (1981), no. 2, 317–327. MR 82h:12022

[HLW03] Y. S. Hwang, D. Leep, and A. Wadsworth, *Galois groups of order* $2n$ *containing a cyclic subgroup of order* n, Pacific J. Math. **212** (2003), no. 2, 297–319.

[Hwa95a] Y. S. Hwang, *The corestriction of valued division algebras over Henselian fields. I*, Pacific J. Math. **170** (1995), no. 1, 53–81. MR 96j:12005a

[Hwa95b] ______, *The corestriction of valued division algebras over Henselian fields. II*, Pacific J. Math. **170** (1995), no. 1, 83–103. MR 96j:12005b

[Jac75] N. Jacobson, PI-*algebras*, Springer-Verlag, Berlin, 1975. MR 51 #5654

[Jac96] ______, *Finite-dimensional division algebras over fields*, Springer-Verlag, Berlin, 1996. MR 98a:16024

[JW86] B. Jacob and A. R. Wadsworth, *A new construction of noncrossed product algebras*, Trans. Amer. Math. Soc. **293** (1986), no. 2, 693–721. MR 87g:16027

[JW90] ______, *Division algebras over Henselian fields*, J. Algebra **128** (1990), no. 1, 126–179. MR 91d:12006

[Kar89] G. Karpilovsky, *Topics in field theory*, North-Holland Publishing Co., Amsterdam, 1989. MR 90f:12003

[Mer85] A. S. Merkurjev, *Structure of the Brauer group of fields*, Izv. Akad. Nauk SSSR Ser. Mat. **49** (1985), no. 4, 828–846, 895. MR 87b:12005

[Mil71] J. Milnor, *Introduction to algebraic* K*-theory*, Princeton University Press, Princeton, N.J., 1971. MR 50 #2304

[Mor89] P. Morandi, *The Henselization of a valued division algebra*, J. Algebra **122** (1989), no. 1, 232–243. MR 90h:12007

[MW04] J. Mináč and A. Wadsworth, *Division algebras of prime degree and maximal galois p-extensions*, to appear in Canadian Journal of Math (2004).

[NSW00] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, Springer-Verlag, Berlin, 2000. MR 2000j:11168

[Pie82] R. S. Pierce, *Associative algebras*, Springer-Verlag, New York, 1982. MR 84c:16001

[Rei75] I. Reiner, *Maximal orders*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975. MR 52 #13910

[Rib85] P. Ribenboim, *Equivalent forms of Hensel's lemma*, Exposition. Math. **3** (1985), no. 1, 3–24. MR 87a:12014

[Rot79] J. J. Rotman, *An introduction to homological algebra*, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1979. MR 80k:18001

[Row80] L. H. Rowen, *Polynomial identities in ring theory*, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, 1980. MR 82a:16021

[RT83] S. Rosset and J. Tate, *A reciprocity law for K_2-traces*, Comment. Math. Helv. **58** (1983), no. 1, 38–47. MR 85b:11105

[Sch50] O. F. G. Schilling, *The Theory of Valuations*, American Mathematical Society, New York, N. Y., 1950. MR 13,315b

[Ser79] J.-P. Serre, *Local fields*, Springer-Verlag, New York, 1979. MR 82e:12016

[Tig87] J.-P. Tignol, *On the corestriction of central simple algebras*, Math. Z. **194** (1987), no. 2, 267–274. MR 88f:12005

[TW87] J.-P. Tignol and A. R. Wadsworth, *Totally ramified valuations on finite-dimensional division algebras*, Trans. Amer. Math. Soc. **302** (1987), no. 1, 223–250. MR 88j:16025

[Wad86] A. R. Wadsworth, *Extending valuations to finite-dimensional division algebras*, Proc. Amer. Math. Soc. **98** (1986), no. 1, 20–22. MR 87i:16025

[Wad02] A. R. Wadsworth, *Valuation theory on finite dimensional division algebras*, Valuation theory and its applications, Vol. I (Saskatoon, SK, 1999), Amer. Math. Soc., Providence, RI, 2002, pp. 385–449. MR 2003g:16023