

THE UNIVERSITY OF CHICAGO

TWISTED HEISENBERG REPRESENTATIONS AND LOCAL CONDUCTORS

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY
ROMYAR T. SHARIFI

CHICAGO, ILLINOIS

JUNE 1999

To my parents: Hassan and Carol Sharifi.

ACKNOWLEDGEMENTS

I thank my advisor Spencer Bloch for many helpful discussions. I thank Dick Gross for suggesting this problem to me and for his advice. I thank Rene Schoof for his suggestions on use of the Hochschild-Serre spectral sequence and Hendrik Lenstra for advice on the Galois module structure of the multiplicative group of a local field. I would also like to thank my roommate Andrew Przeworski for listening to me ramble on about my thesis and trying to help out when he could and my officemate Paul Li for giving me advice about group theory.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS	iii
INTRODUCTION	1
1 COHOMOLOGICAL RESULTS	7
1.1 The transgression	7
1.2 Galois embedding problems	11
1.3 Twisted Galois maps	17
2 TWISTED HEISENBERG REPRESENTATIONS	21
2.1 Definitions	21
2.2 Twisted Kummer representations	24
2.3 Cup product	26
2.4 Three-dimensional Heisenberg representations	27
2.5 Three-dimensional twisted Heisenberg representations	29
2.6 Twisted Heisenberg representations	31
3 LOCAL FIELDS	34
3.1 The Hochschild-Serre spectral sequence	34
3.2 The spectral sequence for local fields	39
3.3 Twisted Heisenberg representations	43
4 RAMIFICATION	46
4.1 Preliminaries	46
4.2 The multiplicative group as a module	49
4.3 Comparison of module structure with unit filtration	52
4.4 Conductors in the metabelian case	53
4.5 Ramification in a Heisenberg extension	58
REFERENCES	65

INTRODUCTION

In this thesis, we consider a special class of Galois representations which we call “twisted Heisenberg representations.” These are modular representations of the absolute Galois group of a field in dimension at least three, providing an interesting class of examples beyond the often studied two-dimensional representations. We study these from two perspectives. The first is the point of view of embedding problems, for which we investigate lifts to twisted Heisenberg representations for fields of good characteristic. The other is the point of view of number theory, for which we consider the representations over local fields and study their ramification.

An embedding problem is the attempt to realize a given Galois extension of the ground field inside a larger extension with predetermined Galois group. The study of embedding problems dates back to Brauer [1] and even before, with many results, some quite general, having been proven of the sort which profess existence of a solution to a given embedding problem [11]. One of the key aspects of our study of lifts to twisted Heisenberg representations, described in more detail below, is that we can not only determine conditions for a solution to exist but also give a concrete description of the fixed fields of the kernels of these representations. We expect this to be one of many examples of Galois groups for which we will be able to construct solutions to embedding problems explicitly.

Although obtained entirely independently, our construction generalizes work of Massy [17], [18], who obtained a constructive solution to the embedding problem for extra-special p -groups as central extensions of abelian p -groups over fields of characteristic not p containing p th roots of unity. This problem finds its origins in papers of Dedekind [6], who gave examples of quaternion extensions of \mathbf{Q} and Witt, who solved the embedding problem of the quaternion group of order 8 over the dihedral group of order 4 [23]. It was then studied in [5], [4], [7] and [19] before Massy gave his constructive solution. More recently, Swallow [21] has given a solution which is

in general more explicit than Massy's, and Brattström [2] has studied the case in which the field is not assumed to contain p th roots of unity (which can be viewed as a special case of the twisted Heisenberg representations we consider).

Another aspect of the theory of Galois representations is the relationship of Galois representations with modular forms. This is the subject of several conjectures, beginning with Serre's conjecture [16] on two-dimensional Galois representations of the absolute Galois group of \mathbf{Q} . More recently, Gross has made conjectures on the existence of modular representations associated to modular forms modulo p [9], [10]. In order to obtain results on the existence of modular representations, one can first attempt to determine some information about the representations involved. To do this, we can describe ramification in the extension given by the fixed of the kernel. We give an analysis of ramification in the fixed fields of the kernels of certain twisted Heisenberg representations of the absolute Galois group of \mathbf{Q}_p . From the point of view of local class field theory, this description provides interesting examples of ramification groups for two and three-step solvable extensions.

Before discussing this thesis in more detail, let us first define the representations that we will consider. For a field K , we let G_K denote its absolute Galois group. Let E be a field of characteristic not dividing a positive integer m , and let F denote the cyclotomic extension of E by m th roots of unity. Let B_d denote the subgroup of upper triangular matrices modulo scalars of $PGL_d(\mathbf{Z}/m\mathbf{Z})$.

Definition. A twisted Heisenberg representation is a homomorphism $\rho: G_E \rightarrow B_d$ with the following properties:

- (1) The image of G_F under ρ is the Heisenberg group H_d of elements of the form

$$\begin{pmatrix} 1 & * & * & \cdots & * & * \\ & 1 & 0 & \cdots & 0 & * \\ & & \ddots & \ddots & \vdots & \vdots \\ & & & 1 & 0 & * \\ & & & & 1 & * \\ & & & & & 1 \end{pmatrix}.$$

- (2) The image of G_E under ρ is contained in the product of H_d and the group D_d of diagonal matrices modulo scalars.

A twisted Heisenberg representation induces (as the fixed field of $\rho|_{G_F}$) a Galois extension of E consisting of an extension with Heisenberg Galois group over the cyclotomic extension F/E . One example of such an extension, when $\mu_m \subset E$, is given by adjoining to E the m th roots of x , $1-x$ and

$$c = \prod_{i=1}^m (1 - \zeta_m^i \sqrt[m]{x})^i$$

for $x \in E^\times$ such that $x, 1-x \notin E^{\times m}$, where ζ_m denotes a primitive m th root of unity. (Often this works without the assumption $\mu_m \subset E$.) This example was studied in an analogous form as a cover of $\mathbf{P}^1 - \{0, 1, \infty\}$ in an unpublished letter from Deligne to Grothendieck. In general, one can view the representations studied in this thesis as being associated to mixed Tate motives which arise as étale cohomology groups in a geometric setting. The description of these as representations of $G_{\mathbf{Q}_p}$ should help in better understanding the p -adic Galois representations associated to mixed Tate motives.

For simplicity of presentation, let us assume in the remainder of this discussion that $m = p^n$ for an odd prime p . Let Z_d denote the center of H_d . Assume that we are given a homomorphism $\bar{\rho}: G_E \rightarrow B_d/Z_d$ satisfying conditions compatible with the definition of a twisted Heisenberg representation (that is, $\bar{\rho}(G_F) = H_d/Z_d$ and $\bar{\rho}(G_E) \subseteq H_d D_d/Z_d$). Since F/E is a cyclic extension, we then have a fixed number r such that any lifting ρ of the “twisted Kummer representation” $\bar{\rho}$ will act via conjugation by the r th power of the cyclotomic character on Z_d . And for i with $2 \leq i \leq d-1$, we obtain twisted characters χ_i and χ'_i of G_E which are given roughly (i.e., up to certain powers of the cyclotomic character) by following $\bar{\rho}$ with projection to the $(1, i)$ and (i, d) th matrix entries, respectively. We have the following result concerning the solution of a particular embedding problem, which is proven using non-abelian Galois cohomology.

Proposition 0.1. *The map $\bar{\rho}$ lifts to a twisted Heisenberg representation ρ if and only if the sum of cup products $\sum_{i=2}^{d-1} [\chi_i \cup \chi'_i]$ is 0 in $H^2(E, \mu_{p^n}^{\otimes r})$.*

When $\bar{\rho}$ does lift, we wish to give a description of the possible liftings and construct as explicitly as possible the fixed fields of their kernels. When each cup product $[\chi_i \cup \chi'_i]$ is trivial, we do this by reduction to the case $d = 3$.

In general, let L/K be an arbitrary field extension with $\mu_{p^n} \subset L$ and assume we are given a surjection $\mathcal{G} \twoheadrightarrow G_{L/K}$ with kernel isomorphic to $\mu_{p^n}^{\otimes r}$ as a $G_{L/K}$ -module via conjugation, thereby defining a class $\varepsilon \in H^2(L/K, \mu_{p^n}^{\otimes r})$. We note that to solve the embedding problem for G_K and the surjection $\mathcal{G} \rightarrow G_{L/K}$ it suffices to show that ε is in the image of the transgression map

$$\text{Tra}: H^1(L, \mu_{p^n}^{\otimes r})^{L/K} \rightarrow H^2(L/K, \mu_{p^n}^{\otimes r}).$$

The first cohomology group can be described by Kummer theory

$$H^1(L, \mu_{p^n}^{\otimes r})^{L/K} \cong [L^\times / L^{\times p^n} (r-1)]^{L/K}.$$

Hence, a non- p th power $a \in L^\times$ fixed under the appropriate twisted Galois action yields a group extension in two manners, one through the transgression map and the other through the (appropriate class of the) extension $L(\sqrt[p^n]{a})/K$. These are equivalent extensions. So by describing the sequence of low degree terms in the Hochschild-Serre spectral sequence, we can in theory not only determine if there is a solution to the embedding problem, but count the number of solutions and describe the field extensions explicitly. We give an analysis of the terms in the spectral sequence, beginning with any field E as above and then focusing on local fields over \mathbf{Q}_p .

This can also be phrased so as to give results on the lifting of representations. By comparison with nonabelian cohomology, we describe a dictionary between group extensions as provided via the transgression map and liftings of Galois representations, as provided by triviality of the boundary “map” in degree 1. In particular, we see that in order for a lifting ρ of a representation $\bar{\rho}$ to a group obtained via extension by

$\mu_{p^n}^{\otimes r}$ to exist, it suffices that the class of this group extension be the image of some element $a \in L^\times$ under transgression, as we have just described. In this case, $\rho|_{G_L}$ will actually be the character of order dividing p^n associated to the element a . That is, we will have

$$\rho(\tau) = \tau(p^n\sqrt{a})/p^n\sqrt{a}$$

for $\tau \in G_L$ (after making an appropriate choice of isomorphism $\mathbf{Z}/p^n\mathbf{Z} \xrightarrow{\sim} \mu_{p^n}$).

Returning to the more specific situation of twisted Heisenberg representations, we have that in the three-dimensional case the off-diagonal characters χ and χ' correspond to elements a and b of F which are fixed under Tate twisted actions of $G_{F/E}$. We assume $[\chi \cup \chi'] = 0$ so that a lifting exists. Fix a generator τ of the Galois group of $F(p^n\sqrt{a})/F$, and let N be the norm for this extension. We have that $b = N\beta$ for some $\beta \in F(p^n\sqrt{a})$. Let $L = F(p^n\sqrt{a}, p^n\sqrt{b})$. We obtain several results of the following nature.

Theorem 0.2. *Let $d = 3$. Any element c such that $L(p^n\sqrt{c})$ is the fixed field of $\rho|_{G_F}$ for a lifting ρ of $\bar{\rho}$ is given by*

$$c = e \prod_{j=0}^{p^n-1} \tau^j(\beta)^j$$

for some $e \in F^\times$. Furthermore, the lifting ρ is the character of order p^n associated to c on the absolute Galois group of L .

In particular, we determine conditions under which we can choose $e = 1$. We also analyze a certain Hochschild-Serre spectral sequence which, in the case of local fields, allows us to give such conditions quite explicitly.

We also give an analysis of ramification in these three-step solvable extensions over \mathbf{Q}_p . In essence, this amounts to finding the conductors of the abelian Kummer subextensions, as one can determine the ramification groups and discriminants of the entire extensions from these.

The ‘‘middle step’’ of the extensions we consider is a compositum of Kummer extensions of $F = \mathbf{Q}_p(\zeta_{p^n})$ by p^n th roots of elements fixed under a twisted Galois

action. More specifically, these elements can be described as $x \in F^\times$ satisfying

$$\sigma_i(x)/x^{i^r} \in F^\times p^n \quad (1)$$

for some r and a generator $\sigma_i \in G_{F/\mathbf{Q}_p}$ such that $\sigma_i(\zeta_{p^n}) = \zeta_{p^n}^i$. We let $f_{n,K}(x)$ denote the conductor (considered additively) of $K(\sqrt[p^n]{x})/K$ for any field K containing p^n th roots of unity. In the “nice” cases, we determine:

Theorem 0.3. *Assume $r \not\equiv 0, 1 \pmod{p-1}$, and let $x \notin F^{\times p}$ satisfy (1). Then for $1 \leq m \leq n$ we have*

$$f_{m,F}(x) = p^{m-1}(t+1),$$

where t is the smallest positive integer such that $t \equiv 2 - r \pmod{p-1}$.

The method used here for determining the conductors involves a comparison of the Galois module structure of F^\times to the filtration of the unit group of F .

The “top step” of the extensions is a Kummer extension of degree p^n . We end with the computation of the conductor of this step for the fundamental example of adjoining a p^n th root of $c = \prod_{j=0}^{p^n-1} (1 - \zeta_{p^n}^j \sqrt[p^n]{p})^j$ to $L = \mathbf{Q}_p(\sqrt[p^n]{\mathbf{Q}_p^\times})$, obtaining the following result.

Theorem 0.4. *Let m be an integer with $1 \leq m \leq n$. Then*

$$f_{m,L}(c) = \begin{cases} 2p^{3m} - \frac{p^{3m} - 1}{p^2 + p + 1} + 1 & \text{if } 1 \leq m < n, \\ p^{3n-1} + p^{3n-3} - \frac{p^{3n-3} - 1}{p^2 + p + 1} + 1 & \text{if } m = n. \end{cases}$$

CHAPTER 1

COHOMOLOGICAL RESULTS

1.1 The transgression

We would like a suitable definition of the transgression map in the Hochschild-Serre spectral sequence in terms of group extensions. What we obtain is known, but the author is unaware of a good reference for it. Let G be a profinite group, N an open normal subgroup of G and A a discrete G -module upon which N acts trivially. From the Hochschild-Serre spectral sequence we obtain the transgression map

$$\text{Tra}: H^1(N, A)^{G/N} \rightarrow H^2(G/N, A).$$

Koch [12, §3.6] describes this map as follows. For a homomorphism $f \in H^1(N, A)^{G/N}$, extend f to a continuous map $h: G \rightarrow A$ satisfying $\sigma h(\sigma^{-1}\tau\sigma) = h(\tau)$ and $h(\tau\sigma) = h(\tau) + h(\sigma)$ for all $\tau \in N$ and $\sigma \in G$. Then dh induces a well-defined 2-cocycle on G/N , the class of which is $\text{Tra } f$.

In terms of group extensions, we can express this as follows. For $f \in H^1(N, A)^{G/N}$, define $g: N \rightarrow A \rtimes G$ by $g(\tau) = (f(\tau), \tau)$. Then $g(N)$ is normal in $A \rtimes G$, so define $\mathcal{E} = (A \rtimes G)/g(N)$. This yields the following commutative diagram, in which the upper exact sequence induces the lower exact sequence (*)

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & A \rtimes G & \longrightarrow & G & \longrightarrow & 1 \\ & & \parallel & & \downarrow \pi & & \downarrow & & \\ 0 & \longrightarrow & A & \longrightarrow & \mathcal{E} & \longrightarrow & G/N & \longrightarrow & 1 \end{array} \quad (*)$$

The maps in the lower sequence are well-defined and (*) is exact. To see this, note that for $a \in A$ and $\tau \in N$ we have

$$(a, \tau)(f(\tau), \tau)^{-1} = (a - f(\tau), 1)$$

so

$$\pi(a, \tau) = \pi(a - f(\tau), 1). \quad (1.1)$$

Alternatively, we can describe \mathcal{E} as the pushout in the following commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & N & \longrightarrow & G & \longrightarrow & G/N \longrightarrow 1 \\ & & \downarrow -f & & \downarrow & & \parallel \\ 0 & \longrightarrow & A & \longrightarrow & \mathcal{E} & \longrightarrow & G/N \longrightarrow 1 \end{array} \quad (*). \quad (1.2)$$

Lemma 1.1. *The equivalence class of $(*)$ as a group extension in $H^2(G/N, A)$ is $\text{Tra } f$.*

Proof. We choose an extension h of f as above. By definition of dh and the correspondence of factor sets and group extensions, we have that the class of dh corresponds to the class of a group extension \mathcal{E}' which is $A \times G/N$ as a set. Multiplication on \mathcal{E}' is given by the formula

$$(a_1, \bar{\sigma}_1) \cdot (a_2, \bar{\sigma}_2) = (a_1 + \sigma_1(a_2) + dh(\sigma_1, \sigma_2), \bar{\sigma}_1 \bar{\sigma}_2)$$

for $a_1, a_2 \in A$ and $\sigma_1, \sigma_2 \in G$ (where we have let overbars denote images in G/N). Note that

$$dh(\sigma_1, \sigma_2) = \sigma_1 h(\sigma_2) - h(\sigma_1 \sigma_2) + h(\sigma_1).$$

We define $F: \mathcal{E}' \rightarrow \mathcal{E}$ by

$$(a, \bar{\sigma}) \longmapsto \pi(a + h(\sigma), \sigma)$$

for $a \in A$ and $\sigma \in G$. This is well-defined since for any $\tau \in N$ we have

$$\pi(a + h(\tau\sigma), \tau\sigma) = \pi(a + h(\sigma) + h(\tau), \tau\sigma) = \pi(a + h(\sigma), \sigma),$$

where the last equality follows by equation (1.1). It is a homomorphism as

$$\begin{aligned} F(a_1, \bar{\sigma}_1)F(a_2, \bar{\sigma}_2) &= \pi(a_1 + \sigma_1(a_2) + h(\sigma_1) + \sigma_1 h(\sigma_2), \sigma_1 \sigma_2) \\ &= \pi(a_1 + \sigma_1(a_2) + dh(\sigma_1 \sigma_2) + h(\sigma_1 \sigma_2), \sigma_1 \sigma_2) = F((a_1, \bar{\sigma}_1) \cdot (a_2, \bar{\sigma}_2)) \end{aligned}$$

It is easily checked that F is an isomorphism and induces the identity map on A and G/N . \square

We make the following notational conventions for a given field K . We let G_K denote the Galois group of the separable closure of K over itself. For a Galois extension L/K , we let $G_{L/K}$ denote its Galois group. For a module A of G_K , we denote the Galois cohomology groups of G_K with coefficients in A by $H^*(K, A)$ and we let A^K denote the group of invariants of A under G_K . Similarly, if A is a $G_{L/K}$ -module, we denote the corresponding cohomology groups by $H^*(L/K, A)$ and invariants by $A^{L/K}$.

Fix a positive integer m . If K is a field of characteristic prime to m , we let μ_m denote the group of m th roots of unity in a separable closure of K . The cyclotomic character $\omega: G_K \rightarrow (\mathbf{Z}/m\mathbf{Z})^*$ is defined by $\sigma(\zeta_m) = \zeta_m^{\omega(\sigma)}$ for a primitive m th root of unity ζ_m and $\sigma \in G_{L/K}$. Let $F = K(\zeta_m)$ denote the fixed field of ω .

In the case that L is a Galois extension of F , a homomorphism $\psi: G_K \rightarrow (\mathbf{Z}/m\mathbf{Z})^*$ with kernel containing G_L provides $\mathbf{Z}/m\mathbf{Z}$ with a $G_{L/K}$ -module structure given by $\sigma(a) = \psi(\sigma|_L) \cdot a$ for $a \in \mathbf{Z}/m\mathbf{Z}$. We denote this module by $\mathbf{Z}/m\mathbf{Z}(\psi)$ and the various cohomology groups with coefficients in $\mathbf{Z}/m\mathbf{Z}(\psi)$ by $H^*(L/K, \psi)$ (and $H^*(K, \psi)$). Tensoring with a $G_{L/K}$ -module A yields a twisted module which we denote $A(\psi)$. We often use $A(r)$ to denote $A(\omega^r)$.

Fix a finite Galois extension L/K and a character ψ as above. We have

$$H^1(L, \psi) \cong (L^\times / L^{\times m})(\psi\omega^{-1})$$

as $G_{L/K}$ -modules via Kummer theory. Explicitly, this is induced by a homomorphism

$$\varphi: L^\times \rightarrow H^1(L, \mu_m) \tag{1.3}$$

defined by $\varphi(x) = f_x$ with $f_x(\tau) = \tau(\sqrt[m]{x})/\sqrt[m]{x}$ for $\tau \in G_L$.

At this point, there arises a certain non-canonical aspect to our approach because, for any character ψ , we would like to describe a homomorphism $\varphi: L^\times \rightarrow H^1(L, \psi)$ as in (1.3). To avoid having to make choices later, we fix for each field K once and

for all an isomorphism of groups $\mathbf{Z}/m\mathbf{Z} \rightarrow \mu_m$ compatible with containment of fields. That is, we identify 1 with ζ_m for a fixed primitive root of unity ζ_m in K . We denote the inverse of this map by $\text{Ind} = \text{Ind}_{\zeta_m}$. Furthermore, for varying m these isomorphisms should be compatible in the sense that if l divides m then $\zeta_m^{m/l} = \zeta_l$. In the case we have just described, this provides fixed (compatible) group isomorphisms $H^1(L, \mu_m) \xrightarrow{\sim} H^1(L, \psi)$ for each ψ , allowing us to define φ from the map described in 1.3. Again, we set $f_x = \varphi(x)$.

For $x \in L^\times$, let \bar{x} denote its homomorphic image in $L^\times/L^{\times m}$. We let

$$(L/K)^\psi = \{x \in L^\times \mid \sigma(\bar{x})^{\psi(\sigma)} = \bar{x}^{\omega(\sigma)} \text{ for all } \sigma \in G_K\}. \quad (1.4)$$

Note that $(L/K)^\psi$ maps onto $H^1(L, \psi)^{L/K}$ under φ . Take $x \in (L/K)^\psi$ and let $M = L(\sqrt[m]{x})$. Observe that $G_{M/L}$ is isomorphic as a $G_{L/K}$ -module (under conjugation) to $\mathbf{Z}/m'\mathbf{Z}(\psi)$ via f_x (and so via $-f_x$), where m' is the order of \bar{x} in $L^\times/L^{\times m}$. Furthermore, M/K is Galois. Hence we have a group extension of $G_{L/K}$ by $\mathbf{Z}/m'\mathbf{Z}(\psi)$ which we can push out as in the following diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & G_{M/L} & \longrightarrow & G_{M/K} & \longrightarrow & G_{L/K} \longrightarrow 1 \\ & & \downarrow -f_x & & \downarrow & & \parallel \\ 0 & \longrightarrow & \mathbf{Z}/m'\mathbf{Z}(\psi) & \longrightarrow & \mathcal{E}'' & \longrightarrow & G_{L/K} \longrightarrow 1 \end{array} \quad (**).$$

Remark. If x is not an l th power in L^\times for any l dividing m , then $\mathcal{E}'' \cong G_{M/K}$, since f_x is surjective in this case.

Proposition 1.2. *The exact sequence $(**)$ is the class of $\text{Tra } f_x$ in $H^2(L/K, \psi)$.*

Proof. We remark that the pushout \mathcal{E}'' is the semidirect product $\mathbf{Z}/m'\mathbf{Z}(\psi) \rtimes G_{M/K}$ via the action of G_K on $\mathbf{Z}/m'\mathbf{Z}(\psi)$ modulo the subgroup of elements of the form $(f_x(\tau), \tau)$ with $\tau \in G_{M/L}$. By Lemma 1.1, the class of $\text{Tra } f_x$ is defined by the group

$$\mathcal{E} = \frac{\mathbf{Z}/m'\mathbf{Z}(\psi) \rtimes G_K}{\langle (f_x(\tau), \tau) \mid \tau \in G_L \rangle}.$$

Finally, we note that the quotient map $G_K \rightarrow G_{M/K}$ induces an isomorphism of \mathcal{E} to \mathcal{E}'' which preserves the groups $\mathbf{Z}/m\mathbf{Z}(\psi)$ and $G_{L/K}$. \square

Proposition 1.2 tells that in our situation the image of the transgression is “given” by Kummer extensions. As will often occur, when the transgression is surjective, any group extension as above comes from a Kummer extension of L which is Galois over K . Because of the negative sign appearing in (1.2), the transgression is actually the negative of the map we will be need. We abuse notation and set

$$\mathrm{Tra} x = -\mathrm{Tra} f_x = \mathrm{Tra} f_{x-1}$$

for $x \in (L/K)^\psi$. When the ground field is clear, we denote $(L/K)^\psi$ more simply by L^ψ .

1.2 Galois embedding problems

We are not merely interested a Galois extension but in the actual homomorphism which yields it. In particular, we want to study (surjective) homomorphisms of the absolute Galois group of a field to a group H and their (surjective) lifts to a larger group G with H as a quotient. That is, we study in this section Galois embedding problems. Some and perhaps most all of what we obtain in this section is known. Much of it is presented in [11] (and parts in [14]), but at the same time our point of view is somewhat different than that of [11], in that we are interested only in solutions to the embedding problem which are fields. Furthermore, we are primarily interested in solutions in the strict sense, for which we specify (up to an equivalence) a particular homomorphism from the absolute Galois group to G yielding the desired lifting.

Fix a field K . We consider an exact sequence of finite groups of the form

$$0 \rightarrow A \xrightarrow{\iota} G \xrightarrow{\phi} H \rightarrow 1,$$

where A is abelian and view these groups as trivial G_K -modules. We obtain an sequence of sets

$$0 \rightarrow \text{Hom}(G_K, A) \xrightarrow{\iota} \text{Hom}(G_K, G) \xrightarrow{\phi} \text{Hom}(G_K, H), \quad (1.5)$$

which is exact in the sense that those elements in the image of one map are exactly those taken to the trivial homomorphism by the next. Passing to nonabelian cohomology [14], we have

$$0 \rightarrow H^1(K, A) \xrightarrow{\iota^*} H^1(K, G) \xrightarrow{\phi^*} H^1(K, H). \quad (1.6)$$

As A is not necessarily central in G , we cannot quite extend the sequence (1.6) to $H^2(K, A)$. Instead, given a homomorphism $\bar{\rho} \in \text{Hom}(G_K, H)$ we can twist A by $\bar{\rho}$ so that the action of $\sigma \in G_K$ on $a \in A$ is now given by

$$a^\sigma = f(\sigma)af(\sigma)^{-1}, \quad (1.7)$$

where f is any continuous function lifting $\bar{\rho}$ to G . We denote this new module structure by $A_{\bar{\rho}}$. We then obtain an element $\Delta(\bar{\rho}) \in H^2(K, A_{\bar{\rho}})$ by lifting $\bar{\rho}$ to some f as above and defining the desired 2-cocycle by

$$a(\sigma_1, \sigma_2) = f(\sigma_1)f(\sigma_2)f(\sigma_1\sigma_2)^{-1}. \quad (1.8)$$

The image of a in cohomology is $\Delta(\bar{\rho})$, and this class does not change for homomorphisms cohomologous to $\bar{\rho}$. In particular, $\bar{\rho}$ (resp., $[\bar{\rho}]$) will be in the image of ϕ (resp., ϕ^*) if and only if $\Delta(\bar{\rho})$ is trivial.

Remark. The class $\Delta(\bar{\rho})$ is the obstruction to lifting $\bar{\rho}$ in a very real sense. If $\Delta(\bar{\rho}) = 0$, then a is a coboundary, so we can choose $\kappa: G_K \rightarrow A$ with $d\kappa = -a$. Then, as one can easily check, $\kappa \cdot f$ is a homomorphism lifting $\bar{\rho}$.

We can give a description of $\Delta(\bar{\rho})$ in terms of group extensions. Consider the fiber product

$$G \times_H G_K = \{(g, \sigma) | \phi(g) = \bar{\rho}(\sigma), g \in G, \sigma \in G_K\},$$

which is the pullback in the following diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & A_{\bar{\rho}} & \longrightarrow & G \times_H G_K & \xrightarrow{p_2} & G_K \longrightarrow 1 \\
& & \parallel & & \downarrow p_1 & & \downarrow \bar{\rho} \\
0 & \longrightarrow & A & \longrightarrow & G & \xrightarrow{\phi} & H \longrightarrow 1.
\end{array} \quad (\dagger) \quad (1.9)$$

Lemma 1.3. *The class of (\dagger) in $H^2(G_K, A_{\bar{\rho}})$ is $\Delta(\bar{\rho})$.*

Proof. Let α be a continuous section of p_2 . A factor set corresponding to (\dagger) is given by

$$[\sigma, \tau] = \alpha(\sigma)\alpha(\tau)\alpha(\sigma\tau)^{-1}$$

for $\sigma, \tau \in G_K$. Let $g = p_1 \circ \alpha$. As $[\sigma, \tau] \in A$,

$$[\sigma, \tau] = h(\alpha(\sigma)\alpha(\tau)\alpha(\sigma\tau)^{-1}) = g(\sigma)g(\tau)g(\sigma\tau)^{-1}.$$

As g is a lifting of $\bar{\rho}$, we have that the class of the factor set is $\Delta(\bar{\rho})$ by (1.8). \square

Let L denote the fixed field of the kernel of $\bar{\rho}$. Clearly, we can also take the pullback

$$\begin{array}{ccccccc}
0 & \longrightarrow & A_{\bar{\rho}} & \longrightarrow & \phi^{-1}(G_{L/K}) & \longrightarrow & G_{L/K} \longrightarrow 1 \\
& & \parallel & & \downarrow & & \downarrow \bar{\rho} \\
0 & \longrightarrow & A & \longrightarrow & G & \xrightarrow{\phi} & H \longrightarrow 1.
\end{array} \quad (\dagger\dagger)$$

The group extension $(\dagger\dagger)$ yields a class $\delta(\bar{\rho}) \in H^1(L/K, A_{\bar{\rho}})$. However, this class is not necessarily invariant under conjugation of $\bar{\rho}$. Hence we do not define δ on the class $[\bar{\rho}]$. In particular, we have by Lemma 1.3 that $\Delta(\bar{\rho}) = \text{Inf}(\delta(\bar{\rho}))$, where Inf denotes the inflation from $G_{L/K}$ to G_K .

The rest of this section is devoted to the comparison of two different useful points of view for the solution of embedding problems: the study of lifts of Galois representations as described above and the study of group extensions and the transgression map as described in Section 1.1. We shall describe a relationship between the sequences (1.5) and (1.6) in nonabelian cohomology and the exact sequence of low degree terms in the Hochschild-Serre spectral sequence.

Given $\rho \in \text{Hom}(G_K, G)$ with image $\bar{\rho} \in \text{Hom}(G_K, H)$ we can define $\Lambda(\rho) \in H^1(L, A_{\bar{\rho}})^{L/K}$ by

$$\Lambda(\rho)(\tau) = -\rho(\tau)$$

for $\tau \in G_L$. To see that ρ is actually fixed under the action of $G_{L/K}$, we merely remark that for $\sigma \in G_K$ and $\tau \in G_L$ we have

$$\rho^\sigma(\tau) = \sigma\rho(\sigma^{-1}\tau\sigma) = \rho(\sigma)\rho(\sigma^{-1}\tau\sigma)\rho(\sigma)^{-1} = \rho(\tau).$$

Again, we do not define Λ on the class of ρ unless A is central in G .

Lemma 1.4. *We have $\text{Tra } \Lambda(\rho) = \delta(\phi \cdot (\rho))$.*

Proof. Observe the following diagram:

$$\begin{array}{ccccccc}
 1 & \longrightarrow & G_L & \longrightarrow & G_K & \longrightarrow & G_{L/K} \longrightarrow 1 \\
 & & \downarrow -\Lambda(\rho) & & \downarrow & & \parallel \\
 0 & \longrightarrow & A_{\bar{\rho}} & \longrightarrow & \mathcal{E} & \longrightarrow & G_{L/K} \longrightarrow 1 \\
 & & \parallel & & \downarrow \text{dotted} & & \parallel \\
 0 & \longrightarrow & A_{\bar{\rho}} & \longrightarrow & \phi^{-1}(G_{L/K}) & \longrightarrow & G_{L/K} \longrightarrow 1 \\
 & & \parallel & & \downarrow & & \downarrow \bar{\rho} \\
 0 & \longrightarrow & A & \longrightarrow & G & \xrightarrow{\phi} & H \longrightarrow 1.
 \end{array} \tag{1.10}$$

We will obtain a map $\mathcal{E} \rightarrow \phi^{-1}(G_{L/K})$ for which (1.10) commutes. By the Five Lemma, it will be an isomorphism, thus proving that the classes of the group extensions are the same.

Note that $\phi^{-1}(G_{L/K}) = G \times_H G_{L/K}$. We define $A_{\bar{\rho}} \rightarrow G \times_H G_{L/K}$ by $a \mapsto (a, 0)$ and $G_K \rightarrow G \times_H G_{L/K}$ by $\sigma \mapsto (\rho(\sigma), \bar{\sigma})$. For $\tau \in G_L$, these maps coincide because $-\Lambda(\rho)(\tau) = \rho(\tau)$. By the universal property of the pushout \mathcal{E} , we obtain the desired map. \square

Lemma 1.5. *Right multiplication by ρ induces a well-defined map from $Z^1(K, A_{\bar{\rho}})$ to $\text{Hom}(K, G)$ (and, in fact, from $H^1(K, A_{\bar{\rho}})$ to $H^1(K, G)$). Furthermore, for $k \in$*

$Z^1(K, A_{\bar{\rho}})$ we have

$$\text{Res}[k] \cdot \Lambda(\rho) = \Lambda(k \cdot \rho),$$

where Res denotes restriction from G_K to G_L . Any lift of $\bar{\rho}$ has the form $k \cdot \rho$ for some k .

Proof. For $\sigma, \tau \in G_K$, we have

$$k(\sigma\tau)\rho(\sigma\tau) = k(\sigma)k(\tau)^\sigma \rho(\sigma)\rho(\tau) = k(\sigma)\rho(\sigma)k(\tau)\rho(\tau),$$

where the last step follows by (1.7). Furthermore, for $a \in A_{\bar{\rho}}$ and $\sigma \in G_K$ we have

$$a^{-1}a^\sigma \rho(\sigma) = a^{-1}\rho(\sigma)a,$$

so coboundaries are mapped to coboundaries. This verifies the first statement.

As for the second statement, we merely note that for $\tau \in G_L$ the cocycles of both terms take on value $-k(\tau)\rho(\tau)$. For the last statement, let ρ' be another lifting of $\bar{\rho}$ and set $k = \rho\rho'^{-1}$. We claim that $k \in Z^1(K, A_{\bar{\rho}})$. For this, we compute

$$\kappa(\sigma\tau) = \rho(\sigma\tau)\rho'^{-1}(\sigma\tau) = \rho(\sigma)\rho(\tau)\rho'(\tau)^{-1}\rho'(\sigma)^{-1} = \rho(\sigma)\kappa(\tau)\rho'(\sigma)^{-1} = \kappa(\sigma)\kappa(\tau)^\sigma.$$

□

We now determine when two different lifts of $\bar{\rho}$ have the same restriction to L via Λ .

Lemma 1.6. *Two lifts ρ and ρ' of $\bar{\rho}$ satisfy $\Lambda(\rho) = \Lambda(\rho')$ if and only if $\rho' = t\rho$ for some $t \in Z^1(L/K, A_{\bar{\rho}})$.*

Proof. By Lemma 1.5, the two lifts satisfy $\bar{\rho} = t\bar{\rho}'$ for some $t \in Z^1(K, A_{\bar{\rho}})$. We must show that t is inflated from L/K . But this is clear as the fact that $\Lambda(t\rho) = \Lambda(\rho)$ says exactly that t is trivial on G_L . □

Putting everything together, we have the following “commutative diagram” in which certain of the maps must be taken only on certain elements (which map to or

come from $\bar{\rho}$ or a lift ρ of it) and in which exactness holds only in the appropriate sense and where appropriate. We include it merely to summarize what we have defined and proven above:

$$\begin{array}{ccccccccc}
Z^1(L/K, A_{\bar{\rho}}) & \hookrightarrow & Z^1(K, A_{\bar{\rho}}) & \xrightarrow{\iota} & \text{Hom}(G_K, G) & \xrightarrow{\phi} & \text{Hom}(G_K, H) & \xrightarrow{\Delta} & H^2(K, A_{\bar{\rho}}) \\
\downarrow & & \downarrow & & \downarrow \Lambda & & \downarrow \delta & & \parallel \\
H^1(L/K, A_{\bar{\rho}}) & \xrightarrow{\text{Inf}} & H^1(K, A_{\bar{\rho}}) & \xrightarrow{\text{Res}} & H^1(L, A_{\bar{\rho}})^{L/K} & \xrightarrow{\text{Tra}} & H^2(L/K, A_{\bar{\rho}}) & \xrightarrow{\text{Inf}} & H^2(K, A_{\bar{\rho}}).
\end{array} \tag{1.11}$$

In particular, we obtain the following proposition which relates liftings of Galois representations to group extensions.

Proposition 1.7. *Let $\bar{\rho}: G_K \rightarrow H$, and let L denote the fixed field of its kernel. Then $\bar{\rho}$ lifts to some $\rho: G_K \rightarrow G$ if and only if $\delta(\bar{\rho})$ is in the image of the transgression map. If $\delta(\bar{\rho}) = \text{Tra} \xi$ then ρ may be chosen so that $\Lambda(\rho) = \xi$. The choice of ρ is unique up to left multiplication by a cocycle in $Z^1(L/K, A_{\bar{\rho}})$. Furthermore, ρ will be surjective if and only if both $\bar{\rho}$ and ξ are surjective.*

Proof. If $\bar{\rho}$ lifts to ρ then $\delta(\bar{\rho}) = \text{Tra}(\Lambda(\rho))$ by Lemma 1.4. If, conversely, $\delta(\bar{\rho}) = \text{Tra} \xi$ with $\xi \in H^1(L, A_{\bar{\rho}})^{L/K}$ then

$$\Delta(\bar{\rho}) = \text{Inf} \circ \text{Tra} \xi = 0,$$

so $\bar{\rho}$ lifts. In this case, let ρ' be a lifting of $\bar{\rho}$. Since

$$\text{Tra} \Lambda(\rho') = \delta(\bar{\rho}) = \text{Tra} \xi,$$

we have that $\text{Res}[k] \cdot \Lambda(\rho') = \xi$ for some $k \in Z^1(K, A_{\bar{\rho}})$. Set $\rho = k\rho'$. From Lemma 1.5 we conclude that $\Lambda(\rho) = \xi$. The statement of uniqueness is just Lemma 1.6, and the last statement is clear. \square

Remark. In the case A is central in G , the module $A_{\bar{\rho}}$ is just A with trivial action, and all the maps we defined above pass to cohomology classes. Hence we obtain another

“commutative diagram,” similar to (1.11), in which all the maps in the top row are defined on all elements:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1(K, A) & \xrightarrow{L^*} & H^1(K, G) & \xrightarrow{\phi^*} & H^1(K, H) & \xrightarrow{\Delta} & H^2(K, A) \\
& & \parallel & & \downarrow \Lambda & & \downarrow \delta & & \parallel \\
0 & \longrightarrow & H^1(L/K, A) & \xrightarrow{\text{Inf}} & H^1(K, A) & \xrightarrow{\text{Res}} & H^1(L, A)^{L/K} & \xrightarrow{\text{Tra}} & H^2(L/K, A) & \xrightarrow{\text{Inf}} & H^2(K, A).
\end{array}$$

1.3 Twisted Galois maps

Let m be a fixed positive integer and E a field of characteristic not dividing m . Set $F = E(\zeta_m)$. Let \mathcal{N} be a finite nilpotent group with a minimal generating set S consisting of elements of exponent dividing m . We fix, if possible, an action of $(\mathbf{Z}/m\mathbf{Z})^*$ on \mathcal{N} such that all of the cyclic subgroups generated by the elements of S are closed under this action. With this action, we define $\mathcal{G} = \mathcal{N} \rtimes (\mathbf{Z}/m\mathbf{Z})^*$. We define a twisted Galois map with group \mathcal{N} to be a homomorphism $\rho: G_E \rightarrow \mathcal{G}$ (for some such \mathcal{G}) satisfying $\rho(G_F) = \mathcal{N}$ and such that the projection of ρ to $(\mathbf{Z}/m\mathbf{Z})^*$ is the cyclotomic character ω . The image of a twisted Galois map with group \mathcal{N} and a fixed action is therefore dependent only on the field E , and we denote it by \mathcal{G}_E . Note that $\mathcal{G}_E \cong \mathcal{N} \rtimes G_{F/E}$.

Let $c \in S$ and assume c is central in \mathcal{N} , generating a cyclic subgroup C of order l dividing m . Note that $\mathcal{G}/C = \mathcal{N}/C \rtimes (\mathbf{Z}/m\mathbf{Z})^*$. Assume we are given a twisted Galois representation $\bar{\rho}$ with group \mathcal{N}/C . This defines an action of G_E on C given by a twist of the cyclotomic character. That is, C is isomorphic to $\mathbf{Z}/l\mathbf{Z}(\psi)$ for some twist $\psi: G_{F/E} \rightarrow (\mathbf{Z}/l\mathbf{Z})^*$ and we fix an isomorphism identifying C with this module, taking c to 1. To see when $\bar{\rho}$ lifts to a twisted Galois representation with group \mathcal{N} , we apply the discussions of Sections 1.1 and 1.2.

Let L denote the fixed field of the kernel $\bar{\rho}$, so that $\bar{\rho}: G_{L/E} \xrightarrow{\sim} \mathcal{G}_E/C$. Then we have a group extension

$$0 \rightarrow \mathbf{Z}/l\mathbf{Z}(\psi) \rightarrow \mathcal{G}_E \rightarrow G_{L/E} \rightarrow 1,$$

and we let $[\mathcal{G}_E]$ denote its class in $H^2(L/E, \psi)$.

For $z \in L^\psi$, we can define $\text{Tra} z \in H^2(L/E, \psi)$ as in Section 1.1. That is, if $f_z \in H^1(L, \psi)$ denotes the fixed twist of the character associated to z by Kummer theory, as described in Section 1.1, and if $M = L(\sqrt[l]{z})$, then by Proposition 1.2 the transgression $\text{Tra} z$ is the class of the group extension defined by the lower exact sequence in the following commutative diagram, in which the vertical arrows are all isomorphisms:

$$\begin{array}{ccccccc} 1 & \longrightarrow & G_{M/L} & \longrightarrow & G_{M/E} & \longrightarrow & G_{L/E} \longrightarrow 1 \\ & & f_z \downarrow \wr & & \downarrow \wr & & \parallel \\ 0 & \longrightarrow & \mathbf{Z}/l\mathbf{Z}(\psi) & \longrightarrow & \mathcal{E} & \longrightarrow & G_{L/E} \longrightarrow 1. \end{array}$$

Proposition 1.8. *Let $\bar{\rho}$ be a twisted Galois map with group \mathcal{N}/C as above. Then $\bar{\rho}$ lifts to a twisted Galois map with group \mathcal{N} if and only if there is an $z \in L^\times$, not a k th power for any k dividing l , such that $z \in L^\psi$ and $\text{Tra} z = [\mathcal{G}_E] \in H^2(L/E, \psi)$. In this case, ρ may be chosen so that*

$$\rho(\tau) = \text{Ind} \frac{\tau(\sqrt[l]{z})}{\sqrt[l]{z}}$$

for all $\tau \in G_L$.

Proof. The first statement is immediate by Proposition 1.7 and the preceding discussion. The other follows from Proposition 1.7 and the definitions in Section 1.1. \square

We now analyze the situation in Proposition 1.8 more closely. Note that we have a commutative diagram

$$\begin{array}{ccc} H^1(L, \psi)^{L/E} & \xrightarrow{\text{Tra}_E} & H^2(L/E, \psi) \\ & \searrow \text{Tra}_F & \downarrow \text{Res} \\ & & H^2(L/F, \psi)^{F/E}. \end{array}$$

If $\text{Tra}_F z$ has class $[\mathcal{N}]$, it comes from a class $\text{Tra}_E z$ in $H^2(L/E, \psi)$. However, we need more information to guarantee that that the latter class is $[\mathcal{G}_E]$.

Note that as $G_{F/E}$ sits (non-canonically) as a subgroup of \mathcal{G}_E . Under $\bar{\rho}$, it can be identified with a subgroup of $G_{L/E}$ with a fixed field E' . We then have a restriction homomorphism

$$\text{Res}_F: H^2(L/E, \psi) \rightarrow H^2(L/E', \psi) \cong H^2(F/E, \psi).$$

Though as a map to $H^2(F/E, \psi)$ this may not be canonical, it always has the same kernel. Note that $[\mathcal{G}_E]$ will be taken to zero under this homomorphism.

Proposition 1.9. *Let $\bar{\rho}$ be a twisted Galois map with group \mathcal{N}/C as above. Then $\bar{\rho}$ lifts to a twisted Galois map with group \mathcal{N} if and only if there is a $z \in L^\times$, not a k th power for any k dividing l , satisfying $z \in L^\psi$ and such that $\text{Tra}_F z = [\mathcal{N}] \in H^2(L/F, \psi)$ and $\text{Res}_F \circ \text{Tra}_E z = 0$.*

Proof. Clearly, if there is a lift, then such a z exists, corresponding as described in Section 1.1 to $\Lambda(\rho)$ as defined in Section 1.2. Conversely, let z satisfy the properties listed and set $M = L(\sqrt[l]{z})$. We illustrate the situation with the following commutative diagram, which should help to clarify our argument below:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathbf{Z}/l\mathbf{Z}(\psi) & \longrightarrow & G_{M/E'} & \xrightarrow{\quad} & G_{F/E} \longrightarrow 1 \\ & & \parallel & & \downarrow & \nearrow & \downarrow \\ 1 & \longrightarrow & \mathbf{Z}/l\mathbf{Z}(\psi) & \longrightarrow & G_{M/E} & \longrightarrow & G_{L/E} \longrightarrow 1 \\ & & \parallel & & \uparrow & & \uparrow \\ 1 & \longrightarrow & \mathbf{Z}/l\mathbf{Z}(\psi) & \longrightarrow & \mathcal{N} & \longrightarrow & G_{L/F} \longrightarrow 1. \end{array}$$

Since $\text{Res}_F \circ \text{Tra}_E z = 0$, we have a splitting map $G_{F/E} \rightarrow G_{M/E'}$. By composition, we obtain a splitting map $G_{F/E} \rightarrow G_{M/E}$ and hence an isomorphism $G_{M/E} \cong G_{M/F} \rtimes G_{F/E}$. Since $\text{Tra}_E z = [\mathcal{N}]$, we have an isomorphism $\alpha: G_{M/F} \xrightarrow{\sim} \mathcal{N}$. On $G_{M/L}$, this is the map f_z , identifying it with $\mathbf{Z}/l\mathbf{Z}(\psi)$ as a G_E -module. Projecting to $G_{L/F}$, this is given by $\bar{\rho}|_{G_{L/F}}: G_{L/F} \xrightarrow{\sim} \mathcal{N}/C$.

We claim that α and the identity of $G_{F/E}$ are compatible maps, providing an isomorphism $\rho: G_{M/E} \xrightarrow{\sim} \mathcal{G}_E$. That is, we require for $\sigma \in G_{F/E}$ and $\tau \in G_{M/F}$ that

$\alpha(\sigma\tau\sigma^{-1}) = \sigma\alpha(\tau)\sigma^{-1}$. This follows from the identification of $G_{M/L}$ with $\mathbf{Z}/l\mathbf{Z}(\psi)$ and the fact that $\bar{\rho}$ is a homomorphism on $G_{L/E}$. At the same time, this argument insures that the isomorphism ρ provides an equality of classes in $H^2(L/E, \psi)$. \square

Given the group $PGL_d(\mathbf{Z}/m\mathbf{Z})$ of d -dimensional invertible matrices over integers modulo m , we let B_d denote its upper triangular Borel subgroup modulo scalars, N_d the subgroup of upper-triangular unipotent elements and D_d the group of diagonal matrices modulo scalars. Assume we are given a map $\iota: \mathcal{G} \rightarrow B_d$ satisfying that ι maps \mathcal{N} injectively into N_d and the image of ι is contained in $D_d \cdot \iota(\mathcal{N})$. In this case, we may consider the representation $\iota \circ \rho$, and so we refer to ρ as a twisted Galois representation. Note that ι may be lifted to a map to the Borel subgroup of $GL_d(\mathbf{Z}/m\mathbf{Z})$ by placing a 1 in the lower right hand corner.

CHAPTER 2

TWISTED HEISENBERG REPRESENTATIONS

2.1 Definitions

In this chapter, we consider a special type of twisted Galois representation. Let $d \geq 2$. We define H_d as follows. First, it is a central extension

$$0 \rightarrow \mathbf{Z}/m\mathbf{Z} \rightarrow H_d \rightarrow (\mathbf{Z}/m\mathbf{Z})^{\oplus 2(d-2)} \rightarrow 0 \quad (2.1)$$

where the leftmost term is generated by z and the rightmost term is generated by elements \bar{x}_i and \bar{y}_i with $2 \leq i \leq d-1$ lifting to elements x_i and y_i of order m in H_d . We then require that these elements commute except that $[x_i, y_i] = z$ for $2 \leq i \leq d-1$. The group H_d is a Heisenberg group, nilpotent of exponent m if m is odd and $2m$ if m is even. We define $Z_d \cong \mathbf{Z}/m\mathbf{Z}$ as the subgroup generated by z .

We observe that H_d is isomorphic to the subgroup of the unipotent matrices N_d consisting of matrices of the form

$$\begin{pmatrix} 1 & * & * & \cdots & * & * \\ & 1 & 0 & \cdots & 0 & * \\ & & \ddots & \ddots & \vdots & \vdots \\ & & & 1 & 0 & * \\ & & & & 1 & * \\ & & & & & 1 \end{pmatrix}$$

under the map which takes x_i to the elementary unipotent matrix E_{i1} , y_i to E_{di} and z to E_{d1} . We identify H_d with this group of matrices.

Let E be a field of characteristic not dividing m and set $F = E(\zeta_m)$. For $d \geq 3$, we define a twisted Heisenberg representation of G_E to be a homomorphism $\rho: G_E \rightarrow PGL_d(\mathbf{Z}/m\mathbf{Z})$ such that $\rho(G_F) = H_d$ and $\rho(G_E) \subset D_d \cdot H_d$, where D_d is the group

of diagonal matrices modulo scalars. When $d = 2$, we call such a homomorphism a twisted Kummer representation. When $F = E$, we leave the word “twisted” out. Given a twisted Heisenberg representation, we may view it as a representation to GL_d by always choosing the lift in which the lower right hand entry is 1.

We let ω_i denote the composite of ρ with projection to the (i, i) -entry:

$$\omega_i(\sigma) = \rho(\sigma)_{ii}.$$

Note that by our choice of lift, $\omega_d = 1$. Each ω_i factors through ω , and we let $\theta_i: (\mathbf{Z}/m\mathbf{Z})^* \rightarrow (\mathbf{Z}/m\mathbf{Z})^*$ be defined by $\omega_i = \theta_i \circ \omega$.

Before we analyze these representations, let us show how the definition of a twisted Heisenberg representation matches up with the definition of a twisted Galois representation with group H_d . Let \mathcal{G} be a group of the form $\mathcal{G} = H_d \rtimes (\mathbf{Z}/m\mathbf{Z})^*$ with the requirement that the cyclic subgroups of H_d generated by any x_i or y_i (and hence by z) are closed under the action of $(\mathbf{Z}/m\mathbf{Z})^*$ by conjugation. We call \mathcal{G} a twisted Heisenberg group. We have the following lemma.

Lemma 2.1. *Let \mathcal{G} be a twisted Heisenberg group. Then there is a homomorphism $\iota: \mathcal{G} = H_d \rtimes (\mathbf{Z}/m\mathbf{Z})^* \rightarrow H_d \cdot D_d$ which is the identity on H_d . Any twisted Heisenberg representation factors through a twisted Heisenberg group via this map: $\rho = \iota \circ \rho'$. Furthermore, the projection of ρ' to $(\mathbf{Z}/m\mathbf{Z})^*$ may be taken to be ω .*

Proof. We define $\theta'_i: (\mathbf{Z}/m\mathbf{Z})^* \rightarrow (\mathbf{Z}/m\mathbf{Z})^*$ for $2 \leq i \leq d-1$ by the equations $ay_i a^{-1} = y_i^{\theta'_i(a)}$ for $a \in (\mathbf{Z}/m\mathbf{Z})^*$. We define θ'_1 similarly by $aza^{-1} = z^{\theta'_1(a)}$ and set $\theta'_d = 1$. The θ'_i determine \mathcal{G} . To see this, for i with $2 \leq i \leq d-1$, let $\beta_i(a)$ be defined by $ax_i a^{-1} = x_i^{\beta_i(a)}$. Since $[x_i, y_i] = z$, we have

$$z^{\theta'_1(a)} = aza^{-1} = [ax_i a^{-1}, ay_i a^{-1}] = [x_i^{\beta_i(a)}, y_i^{\theta'_i(a)}] = z^{\beta_i(a)\theta'_i(a)}.$$

Hence we have $\beta_i(a) = \theta'_1(a)\theta'_i(a)^{-1}$.

The map ι is defined as the identity on H_d and on $(\mathbf{Z}/m\mathbf{Z})^*$ by taking a to the diagonal matrix $\theta'(a)$ with $\theta'_i(a)$ as its i th entry. Note that $D_d \cdot H_d = H_d \rtimes D_d$. To

check that ι is a homomorphism, it suffices to check that it respects the action of conjugation on H_d by $(\mathbf{Z}/m\mathbf{Z})^*$ and D_d . Clearly

$$\theta'(a)E_{id}\theta'(a)^{-1} = E_{id}^{\theta'(a)}$$

for each i , and since $[x, y] = z$ (or $[E_{1i}, E_{id}] = E_{dd}$) it follows that ι respects this action on all matrices in H_d . Hence ι is a homomorphism.

Given ρ , we choose \mathcal{G} by letting $\theta'_i = \theta_i$. We decompose any matrix in the image of ρ as a product of matrices $\rho(\sigma) = \alpha(\sigma)\beta(\sigma)$ with $\alpha(\sigma) \in H_d$ and $\beta(\sigma) \in D_d$. By definition, $\beta = \theta' \circ \omega$, so $\beta(\sigma)_{ii} = \omega_i(\sigma)$. Then ρ' defined by

$$\rho'(\sigma) = (\alpha(\sigma), \omega(\sigma)) = (\alpha(\sigma), 1)(1, \omega(\sigma))$$

is a homomorphism to \mathcal{G} satisfying $\rho = \iota \circ \rho'$. □

By Lemma 2.1, a twisted Heisenberg representation can be viewed as a twisted Galois representation with group H_d . We use the two ways of viewing twisted Heisenberg representations almost interchangeably. However, when we speak of the fixed field of the kernel of ρ , we mean in the form which agrees with that of Section 1.3, which is actually the fixed field of the kernel of $\rho|_{G_F}$, so that the field contains μ_m .

We now consider the non-diagonal entries of the image of ρ . Let $\chi_i: G_E \rightarrow \mathbf{Z}/m\mathbf{Z}$ (resp. χ'_i) be the composition of a twisted Heisenberg representation ρ with the projection of \mathcal{G} onto its \bar{x}_i -coordinate (resp. \bar{y}_i -coordinate) for $2 \leq i \leq d-1$. The multiplication law for semidirect products yields that

$$\chi_i(\sigma_1\sigma_2) = \chi_i(\sigma_1) + \omega_1\omega_i^{-1}(\sigma_1)\chi_i(\sigma_2)$$

for $\sigma_1, \sigma_2 \in G_E$. Similarly, we have

$$\chi'_i(\sigma_1\sigma_2) = \chi'_i(\sigma_1) + \omega_i(\sigma_1)\chi'_i(\sigma_2).$$

Therefore χ_i and χ'_i are cocycles in $Z^1(E, \omega_1\omega_i^{-1})$ and $Z^1(E, \omega_i)$, respectively.

As a matrix representation, we may view ρ as a homomorphism satisfying

$$\rho(\sigma) = \begin{pmatrix} \omega_1(\sigma) & \omega_2\chi_2(\sigma) & \cdots & \omega_{d-1}\chi_{d-1}(\sigma) & \kappa(\sigma) \\ & \omega_2(\sigma) & \cdots & 0 & \chi'_2(\sigma) \\ & & \ddots & \vdots & \vdots \\ & & & \omega_{d-1}(\sigma) & \chi'_{d-1}(\sigma) \\ & & & & 1 \end{pmatrix}$$

for $\sigma \in G_E$ and some map $\kappa: G_E \rightarrow \mathbf{Z}/m\mathbf{Z}$. We observe that

$$\kappa(\sigma_1\sigma_2) = \omega_1(\sigma_1)\kappa(\sigma_2) + \kappa(\sigma_1) + \sum_{i=2}^{d-1} \chi_i(\sigma_1)\omega_i(\sigma_1)\chi'_i(\sigma_2). \quad (2.2)$$

This will be useful in Section 2.3.

2.2 Twisted Kummer representations

Before we begin an analysis of the twisted Heisenberg representations we should at least briefly consider their quotients. In this section, we study twisted Galois representations for which the fixed fields of their kernels are nonabelian Kummer extensions. In general, we take a twisted Kummer representation to be a twisted Galois map ρ on G_E with abelian group $K_d = (\mathbf{Z}/m\mathbf{Z})^{\oplus(d-1)}$. We fix a generating set $\{x_i \mid 1 \leq i \leq d-1\}$ such that $(\mathbf{Z}/m\mathbf{Z})^*$ acts on each cyclic group $\langle x_i \rangle$.

This may be realized as a d -dimensional twisted Galois representation. For instance, K_d is isomorphic to the subgroup of N_d of matrices of the form

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & * \\ & 1 & \ddots & \vdots & \vdots \\ & & \ddots & 0 & * \\ & & & 1 & * \\ & & & & 1 \end{pmatrix}.$$

Define $\theta_i: (\mathbf{Z}/m\mathbf{Z})^* \rightarrow (\mathbf{Z}/m\mathbf{Z})^*$ for $1 \leq i \leq d-1$ by the equation $ax_ia^{-1} = x_i^{\theta_i(a)}$

for $a \in (\mathbf{Z}/m\mathbf{Z})^*$ and set $\theta_d = 1$. Then the map

$$\iota: K_d \rtimes (\mathbf{Z}/m\mathbf{Z})^* \rightarrow PGL_d(\mathbf{Z}/m\mathbf{Z})$$

which takes $(x_i, 0)$ to the elementary unipotent matrix E_{id} for $1 \leq i \leq d-1$ and $(1, a)$ to the diagonal matrix with $\theta_j(a)$ as its j th entry realizes ρ as a twisted Galois representation, as defined in Section 1.3. (This is not quite the form in which we are interested in considering them with regard to twisted Heisenberg representations.)

Assume we are given a $(d-1)$ -dimensional twisted Kummer representation $\bar{\rho}$ with group $K_d/\langle x_d \rangle$, and fix a character $\psi: G_E \rightarrow (\mathbf{Z}/m\mathbf{Z})^*$ yielding the action of G_E on $\langle x_d \rangle$ in K_d . Let L denote the fixed field of the kernel of $\bar{\rho}|_{G_F}$.

Lemma 2.2. *An element $a \in L^\psi$ which is not an l th power for any l dividing m provides a lifting of $\bar{\rho}$ to a twisted Kummer representation with group K_d if and only if the projection of a to $[L^\times/L^{\times m}(\psi)]^{L/E}$ is in the image of the restriction map from $H^1(E, \psi)$.*

Proof. Note that

$$K_d \cong K_d/\langle x_d \rangle \oplus \langle x_d \rangle \cong G_{L/F} \oplus \langle x_d \rangle.$$

Hence the map $\bar{\rho}$ will lift to a d -dimensional twisted Kummer representation as above if and only if $a \in L^\psi$ is such that both $\text{Tra}_F a = 0$ and $\text{Res}_F \text{Tra}_E a = 0$ by Lemma 1.9. That $\text{Tra}_F a = 0$ means exactly that a is in the image of restriction and so comes from an element of F^ψ . Given this, that $\text{Res}_F \text{Tra}_E a = 0$ means exactly that $\text{Tra}_E a = 0$, so a comes from an element of $H^1(E, \psi)$. \square

Remark. In order for an element $a \in F^\psi$ to provide a lifting, it must satisfy that a is not an l th power in L^\times . That is, a should be linearly independent from the elements b_1, \dots, b_{d-2} for which $L = K(\sqrt[m]{b_1}, \dots, \sqrt[m]{b_{d-2}})$. (The elements b_1 through b_{d-2} can themselves be chosen as in Lemma 2.2 with the appropriate twists.) The results of Section 3.1 will provide conditions under which Lemma 2.2 holds.

2.3 Cup product

Assume we are given a twisted Galois map $\bar{\rho}: G_E \rightarrow \mathcal{G}/Z_d$ with group H_d/Z_d . This is a twisted Kummer representation, as defined in Section 2.2. We consider the question of when $\bar{\rho}$ lifts to a twisted Heisenberg representation. The action of \mathcal{G}/Z_d on Z_d by conjugation induces an action of G_E on Z_d factoring through $G_{F/E}$. Hence $Z_d \cong \mathbf{Z}/m\mathbf{Z}(\omega_1)$ under this action. For $2 \leq i \leq d-1$, we have as in Section 2.1 cocycles χ_i (resp. χ'_i) coming from projection of $\bar{\rho}$ to the x_i -coordinate (resp. y_i) of \mathcal{G} .

Consider the classes of the cup products $[\chi_i \cup \chi'_i] \in H^2(E, \omega_1)$. The following proposition tells us that the sum of these classes is the obstruction to lifting $\bar{\rho}$, as described in Section 1.2.

Proposition 2.3. *Let Δ be the “map” associated to the group G_E and the sequence*

$$0 \rightarrow Z_d \rightarrow \mathcal{G} \rightarrow \mathcal{G}/Z_d \rightarrow 1$$

as in Section 1.2. Then we have

$$\Delta(\bar{\rho}) = \sum_{i=2}^{d-1} [\chi_i \cup \chi'_i] \in H^2(E, \omega_1).$$

Proof. We can view $\bar{\rho}$ as a homomorphism into B_d/Z_d chosen such that every matrix (modulo its upper right hand corner) in its image has a 1 in its lower right hand corner. We lift $\bar{\rho}$ to a map $g: G_E \rightarrow B_d$ via the map taking a matrix modulo its upper right hand corner to a matrix with a zero in its upper right hand corner. Then by the definition given in (1.8) we have that $\Delta(\bar{\rho})$ is the class of the cocycle taking a pair (σ_1, σ_2) to $g(\sigma_1)g(\sigma_2)g(\sigma_1\sigma_2)^{-1}$ in $\mathbf{Z}/m\mathbf{Z}(\psi)$.

We compute this cocycle. First, letting $\sigma = \sigma_1\sigma_2$, we see that

$$g(\sigma_1)g(\sigma_2) = \begin{pmatrix} \omega_1(\sigma) & \omega_2\chi_2(\sigma) & \cdots & \omega_{d-1}\chi_{d-1}(\sigma) & \sum_{i=2}^{d-1} \omega_i\chi_i(\sigma_1)\chi'_i(\sigma_2) \\ & \omega_2(\sigma) & \cdots & 0 & \chi'_2(\sigma) \\ & & \ddots & \vdots & \vdots \\ & & & \omega_{d-1}(\sigma) & \chi'_{d-1}(\sigma) \\ & & & & 1 \end{pmatrix}.$$

Now $g(\sigma_1\sigma_2)$ is the same matrix but with a zero in its upper right hand corner and multiplication of it by $z \in Z_d$ just changes its upper right hand corner to (that of) z . Hence, our cocycle is defined by

$$(\sigma_1, \sigma_2) \mapsto \sum_{i=2}^{d-1} \chi_i(\sigma_1)\omega_i(\sigma_1)\chi'_i(\sigma_2).$$

On the other hand, we have by definition of the cup product [12, p. 117] that

$$\chi_i \cup \chi'_i(\sigma_1, \sigma_2) = \chi_i(\sigma_1)\omega_i(\sigma_1)\chi'_i(\sigma_2)$$

as well. □

2.4 Three-dimensional Heisenberg representations

In this section we let $d = 3$ and assume that $E = F$ contains μ_m . In this case, we have just the two cocycles $\chi = \chi_2$ and $\chi' = \chi'_2$, which are in fact characters. The obstruction to lifting the two-dimensional Kummer representation $\bar{\rho}$ as in Section 2.3 is given by the cup product $[\chi \cup \chi']$. Via our fixed choice of isomorphism in Section 1.1, any character χ has an associated element $a \in F^\times$, well-defined up to m th powers in F^\times , such that

$$\chi(\tau) = \text{Ind} \frac{\tau(\sqrt[m]{a})}{\sqrt[m]{a}}$$

for all $\tau \in G_F$. The cup product can then be viewed as a homomorphism

$$(\cdot, \cdot): F^\times \times F^\times \rightarrow H^2(F, \mathbf{Z}/m\mathbf{Z}),$$

which is the norm residue symbol. This means that if χ and χ' have representative elements a and b in F^\times then $[\chi \cup \chi'] = (a, b)$.

By Kummer theory, the fixed field of the kernel of the representation $\bar{\rho}$ is $L = F(\sqrt[m]{a}, \sqrt[m]{b})$. Let $K = F(\sqrt[m]{a})$ and $K' = F(\sqrt[m]{b})$. Let $\tau \in G_{L/K'} \cong G_{K/F}$ be the generator satisfying $\tau(\sqrt[m]{a}) = \zeta_m \sqrt[m]{a}$ (i.e., $\chi(\tau) = 1$). Similarly, let $\tau' \in G_{L/K} \cong G_{K'/F}$ be such that $\tau'(\sqrt[m]{b}) = \zeta_m \sqrt[m]{b}$. The norm residue symbol (a, b) is trivial if and only if $b \in N_{K/F} K^\times$ [15, XIV.2]. So $\bar{\rho}$ will lift if and only if $b = N_{K/F} \beta$ for some $\beta \in K^\times$.

Lemma 2.4. *Let $\beta \in K^\times$ be such that $N_{K/F}(\beta) \in K'^{\times m}$. Set*

$$c = \prod_{j=0}^{m-1} \tau^j(\beta)^j. \quad (2.3)$$

Then we have $\nu(c) \equiv c \pmod{L^{\times m}}$ for all $\nu \in G_{L/F}$.

Proof. As $c \in K$, it suffices to show that c is fixed by τ up to m th powers in L^\times . Note that

$$\tau(c) = \prod_{j=0}^{m-1} \tau^{j+1}(\beta)^j = N_{K/F}(\beta)^{-1} \prod_{j=0}^{m-1} \tau^{j+1}(\beta)^{j+1} = c \frac{\beta^m}{N_{K/F}(\beta)}. \quad (2.4)$$

Hence $\tau(c) \equiv c \pmod{L^{\times m}}$. □

We now explicitly describe the solution to the embedding problem given by the field K , homomorphism $\bar{\rho}$ and surjection $H_3 \twoheadrightarrow \mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}$.

Theorem 2.5. *Let $\beta \in K^\times$ be such that $b = N_{K/F}(\beta)$ and define c as in (2.3). Then we have that $\bar{\rho}$ lifts to a Heisenberg representation ρ with*

$$\rho(\nu) = \text{Ind} \frac{\nu(\sqrt[m]{c})}{\sqrt[m]{c}}$$

for $\nu \in G_L$. Furthermore, c is unique up to multiplication by an element of $F^\times L^{\times m}$.

Proof. Note that $\tau(c) = cb^{-1}\beta^m$ by (2.4). As $\tau'(c) = c$, we have for any extension of τ' to $K(\sqrt[m]{c})$ that $\tau'^m(\sqrt[m]{c}) = \sqrt[m]{c}$. Then same holds for τ , as

$$\tau^m(\sqrt[m]{c}) = \sqrt[m]{c}N_{K/F}(\beta)b^{-1} = \sqrt[m]{c}.$$

To see that $\text{Tr} c$ has order m , we observe that

$$[\tau, \tau'](\sqrt[m]{c}) = \zeta_m \sqrt[m]{c} \quad (2.5)$$

as $\tau'(\sqrt[m]{b}) = \zeta_m(\sqrt[m]{b})$ and τ' fixes K . The class of Heisenberg extension $L(\sqrt[m]{c})/L$ given by $\text{Tr} c$ is now seen to be equal to $\delta(\bar{\rho})$, as defined in Section 1.2, as (2.5) implies that $\rho([\tau, \tau']) = z$ and we are given $\bar{\rho}(\tau) = \bar{x}_1$ and $\bar{\rho}(\tau') = \bar{y}_1$. The rest follows immediately from Proposition 1.8. \square

2.5 Three-dimensional twisted Heisenberg representations

In this section we remove the assumption that E contains the m th roots of unity. We start with $\bar{\rho}$ as in Section 2.3 in the case $d = 3$ and assume a lifting exists, which means by Proposition 2.3 exactly that $[\chi \cup \chi'] = 0$ for the two off-diagonal cocycles. The two cocycles χ and χ' restricted to the Galois group of $F = E(\zeta_m)$ now have elements $a \in F^{\omega_1\omega_2^{-1}}$ and $b \in F^{\omega_2}$ associated to them. We let K, K' and L be as before. Furthermore, since the restriction from E to F satisfies

$$\text{Res}[\chi \cup \chi'] = \text{Res}[\chi] \cup \text{Res}[\chi'] = (a, b),$$

we have that $(a, b) = 0$.

Theorem 2.5 yields the following proposition for the “twisted” case.

Proposition 2.6. *Let $\beta \in K^\times$ be such that $N_{K/F}\beta = b$. Then there exists an element $e \in F^\times$ such that, setting*

$$c = e \prod_{j=0}^{m-1} \tau^j(\beta)^j,$$

the map $\bar{\rho}$ lifts to a twisted Heisenberg representation ρ for which $\rho|_{G_L}$ is the character of order m associated to c .

Proof. Let $c' = \prod_{i=1}^m \tau^i(\beta)^i$. By Theorem 2.5, we have that $\text{Tra } c'$ provides a lifting of $\bar{\rho}|_{G_F}$ to a Heisenberg representation and is unique up to an element of $F^\times L^{\times m}$ doing so. As $\bar{\rho}$ lifts by assumption, we conclude by Proposition 1.8 that there is some $e \in F^\times$ for which $c = c'e$ satisfies $\text{Tra } c = \delta\bar{\rho}$ and providing the desired lifting. \square

Remark. Unfortunately, Proposition 2.6 does not tell us exactly what the element e , and therefore c , can be. In general, e will be determined up to multiplication by any element coming from image of the restriction

$$\text{Res}: H^1(E, \psi) \rightarrow H^1(L, \psi)^{L/E}.$$

We shall describe this image in more detail in Chapter 3.

One question that arises is that of the existence of a good choice of β such that e is allowed to be 1. In the following proposition, we give sufficient conditions for this to be true.

Proposition 2.7. *Let E' be an extension of F with $G_{K/E'} \cong G_{F/E}$ by restriction. Assume there exists $\beta \in (K/E')^{\omega_2}$ with $N_{K/F}(\beta) = b$. Then*

$$c = \prod_{j=0}^{m-1} \tau^j(\beta)^j$$

satisfies $c \in L^{\omega_1}$. If $\text{Res}_F \circ \text{Tra}_E c = 0$, then $\bar{\rho}$ lifts to a twisted Heisenberg representation which restricts to the character of order m associated to c on G_L .

Proof. Let c be as in the statement of the proposition. For $\sigma \in G_{F/E}$, which we extend to an element of $G_{K/E'}$, we have

$$\sigma(c) = \prod_{j=0}^{m-1} \sigma \tau^j(\beta)^j = \prod_{j=0}^{m-1} \tau^{j\omega_1(\sigma)\omega_2(\sigma)^{-1}} \sigma(\beta)^j. \quad (2.6)$$

Working in $L^\times/L^{\times m}$, we see that (2.6) becomes

$$\sigma(\bar{c}) = \prod_{j=0}^{m-1} \tau^{j\omega_1(\sigma)\omega_2(\sigma)^{-1}}(\bar{\beta})^{j\omega_2(\sigma)^{-1}\omega(\sigma)} = \prod_{j=0}^{m-1} \tau^j(\bar{\beta})^{j\omega(\sigma)\omega_1(\sigma)^{-1}} = \bar{c}^{\omega(\sigma)\omega_1(\sigma)^{-1}}.$$

Hence $c \in L^{\omega_1}$.

By Proposition 2.5 we have $\text{Tra}_F c = \delta(\bar{\rho}|_{G_F})$. The last statement now follows immediately from Proposition 1.9. \square

In Chapter 3, we shall see that an element β as in Proposition 2.7 can often be found in the case of local fields.

2.6 Twisted Heisenberg representations

We now let $d \geq 3$ be arbitrary. Again we assume we are given a twisted Kummer representation $\bar{\rho}: G_E \rightarrow \mathcal{G}/Z_d$. To each character χ_i (resp. χ'_i) with $2 \leq i \leq d-1$, we have an associated element a_i (resp. b_i). As we saw in Proposition 2.3, the condition for a lifting to exist is that the sum of cup products $\sum_{i=2}^{d-1} [\chi_i \cup \chi'_i]$ be zero. Via restriction, this forces the corresponding fact on norm residue symbols over F that

$$\sum_{i=2}^{d-1} (a_i, b_i) = 0.$$

Let $K_i = F(\sqrt[m]{a_i})$ and $K'_i = F(\sqrt[m]{b_i})$ for each i . We let L denote the fixed field of $\bar{\rho}$, which is the compositum of the fields $L_i = K_i K'_i$.

We begin with some interesting observations.

Remark. As H_d is a metabelian group satisfying the exact sequence (2.1), we have by [22, p. 29] an exact sequence

$$\begin{aligned} 0 \rightarrow \text{Ext}\left(\bigoplus_{i=2}^{2d-2} \mathbf{Z}/m\mathbf{Z}, \mathbf{Z}/m\mathbf{Z}\right) &\rightarrow H^2(L/F, \mathbf{Z}/m\mathbf{Z}) \\ &\rightarrow \text{Hom}\left(\bigoplus_{i=2}^{2d-2} \mathbf{Z}/m\mathbf{Z} \wedge \bigoplus_{i=2}^{2d-2} \mathbf{Z}/m\mathbf{Z}, \mathbf{Z}/m\mathbf{Z}\right) \rightarrow 0. \end{aligned}$$

The first term represents the extensions with trivial commutators but relations $x_i^m = z^{d_i}$ and $y_i^m = z^{e_i}$. The last term is the group of possible commutator pairings and represents the possible relations $[x_i, x_j] = z^{f_{ij}}$ ($i \neq j$), $[y_i, y_j] = z^{g_{ij}}$ ($i \neq j$) and $[x_i, y_j] = z^{h_{ij}}$. We then have that

$$H^2(L/F, \mathbf{Z}/m\mathbf{Z}) \cong \mathbf{Z}/m\mathbf{Z}^{\oplus(d-2)(2d-3)}$$

with each summand representing one of the invariants d_i, e_i, f_{ij}, g_{ij} and h_{ij} and adding appropriately.

The group G_E acts on each of above summands by multiplication by the twist determined by the twists on x_i and y_i for each i . Thus, it is quite easy to compute the group $H^2(L/F, \psi)^{F/E}$ explicitly. One could then use the corresponding Hochschild-Serre spectral sequence to compare this to the group $H^2(L/E, \psi)$.

In the case that each of the individual cup products $[\chi_i \cup \chi'_i]$ is trivial, we can give a nice description of the lifting ρ by describing the element $c \in L^\times$ such that ρ is the character of order m associated to c on G_L .

Proposition 2.8. *Assume $[\chi_i \cup \chi'_i] = 0$ for each $2 \leq i \leq d-1$. Let $\beta_i \in K_i$ be such that $N_{K_i/F}(\beta_i) = b_i$ and set*

$$c_i = \prod_{j=0}^{m-1} \tau_i^j(\beta_i)^j.$$

Then there exists $e \in F^\times$ for which

$$c = e \prod_{i=2}^{d-1} c_i$$

satisfies $c \in L^{\omega_1}$ and such that $\bar{\rho}$ lifts to ρ with restriction to G_L equal the character of order m associated to c .

Proof. We have by functoriality of the transgression a commutative diagram

$$\begin{array}{ccc}
 \bigoplus_{i=2}^{d-1} (L_i^\times / L_i^{\times p^n})^{L_i/F} & \xrightarrow{\text{Tra}} & \bigoplus_{i=2}^{d-1} H^2(L_i/F, \mathbf{Z}/m\mathbf{Z}) \\
 \downarrow \text{Res} & & \downarrow \text{Inf} \\
 (L^\times / L^{\times p^n})^{L/F} & \xrightarrow{\text{Tra}} & H^2(L/F, \mathbf{Z}/m\mathbf{Z}).
 \end{array} \tag{2.7}$$

If we let ρ_i denote the projection of $\rho|_{G_F}$ onto the subgroup of H_d generated by x_i and y_i and isomorphic to H_3 , then ρ_i is a Heisenberg representation of dimension 3. We have by Proposition 2.5 an equality of classes

$$\text{Tra}_F c_i = \delta(\rho_i) \in H^2(L_i/F, \omega_1).$$

This tells us that $\text{Inf Tra}_F c_i$ is the class of the extension satisfying $[x_i, y_i] = z$ and with all other commutators and all m th powers of the generators trivial.

Furthermore, we have by (2.7) that

$$\text{Tra}_F c = \sum_{i=2}^{d-1} \text{Inf} (\text{Tra}_F c_i)$$

That $\text{Tra}_F c = \delta(\rho|_{G_F})$ is now just the fact that the sum of factor sets yields exactly the commutator relations for the given Heisenberg extension. Finally, the existence of e follows from the existence of a lifting as in Proposition 2.6. \square

Remark. The obvious generalization of Proposition 2.7 to $d \geq 3$ holds as well: that is, with the requirement that $\beta_i \in (K_i/E'_i)^{\omega_i}$ for a proper choice of field E'_i .

CHAPTER 3

LOCAL FIELDS

3.1 The Hochschild-Serre spectral sequence

We will maintain the following notation throughout this chapter. Let p be an odd prime and n a positive integer. Let E be a field with characteristic not equal p and $F = E(\zeta_{p^n})$. We assume that $G_{F/E}$ is cyclic (for instance, if p is odd). In this case, any twist is some power r of the cyclotomic character ω . For any field L containing F , we set $L^{1-r} = (L/E)\omega^r$.

In this section, we begin an analysis of the sequence of low degree terms in the Hochschild-Serre spectral sequence

$$E_2^{s,t}(r) = H^s(F/E, H^t(F, \mu_{p^n}^{\otimes r})) \Rightarrow H^{s+t}(r) = H^{s+t}(E, \mu_{p^n}^{\otimes r}) \quad (3.1)$$

for any integer r . In Section 3.2, we shall finish our analysis in case of local fields. We shall usually omit the r in $E_2^{s,t}(r)$, $H^{s+t}(r)$ and certain other notations defined below, as r is generally fixed. Let $\hat{E}_2^{s,t}$ denote the Tate cohomology group $\hat{H}^s(F/E, H^t(F, \mu_{p^n}^{\otimes r}))$.

We define numbers i and q by $|G_{F/E}| = p^{n-1-i}q$, where q divides $p-1$. Furthermore, we define $j(r)$ as follows. We let $j = 0$ if $r \not\equiv 0 \pmod{q}$. Otherwise, we let j be maximal less than or equal $n-1-i$ such that $r \equiv 0 \pmod{p^j}$.

We begin by computing the invariants $H^0 \cong E_2^{0,0}$.

Lemma 3.1. *We have that*

$$(\mu_{p^n}^{\otimes r})^E \cong \begin{cases} 0 & \text{if } r \not\equiv 0 \pmod{q} \\ \mathbf{Z}/p^{i+j+1}\mathbf{Z} & \text{if } r \equiv 0 \pmod{q}. \end{cases}$$

Proof. Let a be an integer with image \bar{a} in $\mathbf{Z}/p^n\mathbf{Z}$ generating $(\mathbf{Z}/p^n\mathbf{Z})^*$. Then for some generator σ of $G_{F/E}$ we have that $\omega(\sigma) = \bar{a}^{p^i(p-1)q^{-1}}$. Therefore the action of $G_{F/E}$ on $\mu_{p^n}^{\otimes r}$ viewed additively is given by multiplication by $\bar{a}^{p^i(p-1)q^{-1}r}$. This number is 1 modulo p if and only if $r \equiv 0 \pmod{q}$, in which case it is congruent to 1 in $(\mathbf{Z}/p^n\mathbf{Z})^*$ modulo exactly p^{i+j+1} . The result follows. \square

Lemma 3.2. *For all $s \in \mathbf{Z}$ we have $\hat{E}_2^{s,0} = \mathbf{Z}/p^j\mathbf{Z}$.*

Proof. By (3.1) we may assume $r \equiv 0 \pmod{q}$. Let a be as in Lemma 3.1. Note that the norm $N_{F/E}$ viewed additively is multiplication by

$$\sum_{k=0}^{p^{n-i-1}q-1} a^{p^i(p-1)q^{-1}rk} = \frac{a^{p^{n-1}(p-1)r} - 1}{a^{p^i(p-1)q^{-1}r} - 1}.$$

But both the power in the numerator and in the denominator are divisible by $p-1$, so this number is 0 modulo exactly p^{n-1-i} . Hence $N_{F/E}(\mu_{p^n}^{\otimes r}) \cong \mathbf{Z}/p^{i+1}\mathbf{Z}$ when $r \equiv 0 \pmod{q}$. Therefore $\hat{E}_2^{0,0}$ is as stated.

Furthermore, note that $\hat{E}_2^{-1,0} = \hat{H}^{-1}(F/E, \mu_{p^n}^{\otimes r})$ is cyclic. Since our module is finite, we have that this group has the same order as $\hat{E}_2^{0,0}$ and hence is isomorphic to it. Furthermore, each of the Tate cohomology groups is isomorphic to one of these, proving the lemma. \square

Let M denote a field of characteristic not equal p . Consider the long exact sequence in the Galois cohomology of G_M associated to

$$1 \rightarrow \mu_{p^n}^{\otimes r} \rightarrow \mathbf{Q}_p/\mathbf{Z}_p(r) \xrightarrow{p^n} \mathbf{Q}_p/\mathbf{Z}_p(r) \rightarrow 0,$$

i.e., given by multiplication by p^n on $\mathbf{Q}_p/\mathbf{Z}_p(r)$. We let $A_M \subset H^1(M, \mu_{p^n}^{\otimes r})$ denote the cokernel of multiplication by p^n on $H^0(E, \mathbf{Q}_p/\mathbf{Z}_p(r))$.

Lemma 3.3. *Assume that r is such that the action of G_M on $\mathbf{Q}_p/\mathbf{Z}_p(r)$ is non-trivial. Then A_M is a cyclic direct summand of $H^1(M, \mu_{p^n}^{\otimes r})$ isomorphic to $H^0(M, \mu_{p^n}^{\otimes r})$.*

Proof. We remark that if we let n increase past a sufficiently large number, with M and r fixed, the order of $H^0(M, \mu_{p^n}^{\otimes r})$ as given in Lemma 3.1 stabilizes (since the action of G_M is non-trivial). If this order is p^l , we see immediately that $H^0(M, \mathbf{Q}_p/\mathbf{Z}_p(r)) \cong \mathbf{Z}/p^l\mathbf{Z}$. So the first three terms of our exact sequence yield

$$0 \rightarrow H^0(M, \mu_{p^n}^{\otimes r}) \rightarrow \mathbf{Z}/p^l\mathbf{Z} \rightarrow \mathbf{Z}/p^l\mathbf{Z}. \quad (3.2)$$

Hence $A_M \xrightarrow{\sim} H^0(M, \mu_{p^n}^{\otimes r})$ and we have an injective map $A_M \hookrightarrow H^1(M, \mu_{p^n}^{\otimes r})$.

We are done if the image of any generator of $H^0(M, \mathbf{Q}_p/\mathbf{Z}_p(r))$ under the boundary map $H^0(M, \mathbf{Q}_p/\mathbf{Z}_p(r)) \xrightarrow{d} H^1$ is not in the image of multiplication by p on $H^1(M, \mu_{p^n}^{\otimes r})$. Let a generate $[\mathbf{Q}_p/\mathbf{Z}_p(r)]^M$ and let $p^n b = a$. Then we have $d(a) = f$ where f is the cochain defined by $f(\sigma) = \sigma(b) - b$ for $\sigma \in G_M$.

Assume that $[f]$ is a multiple of p , which means that $fg = ph$ for some coboundary $g \in B^1(M, \mu_{p^n}^{\otimes r})$ and cocycle $h \in Z^1(M, \mu_{p^n}^{\otimes r})$. But $fg = \sigma(b') - b'$ for some $b' \in \mathbf{Q}_p/\mathbf{Z}_p(r)$, and we can choose $c \in \mathbf{Q}_p/\mathbf{Z}_p(r)$ with $pc = b'$. Letting $h' = \sigma(c) - c$, we have $ph' = fg = ph$. As h takes values in $\mu_{p^n}^{\otimes r}$, so does h' : that is, $h' \in Z^1(M, \mu_{p^n}^{\otimes r})$. By definition, $h' \in B^1(M, \mathbf{Q}_p/\mathbf{Z}_p(r))$, so the class $[h']$ is in the image of the boundary map d . However, $p[h'] = [f]$, and $[f]$ generates the image, which is a contradiction. \square

Now assume that G_F acts non-trivially on $\mathbf{Q}_p/\mathbf{Z}_p(r)$. In this case, let $A = A_E$ and $B = A_F^{F/E}$. Since F contains the p^n th roots of unity, we can explicitly describe A_F and hence B . That is, if the action of G_F on $\mathbf{Q}_p/\mathbf{Z}_p(r)$ is nontrivial and F contains p^m of the p -power roots of unity, then

$$B = (\mu_{p^m}^{\otimes r} / \mu_{p^{m-n}}^{\otimes r})^{F/E} \cong (\mu_{p^n}^{\otimes r})^{F/E} \cong H^0. \quad (3.3)$$

We may now prove the following proposition.

Proposition 3.4. *Assume that r is such that the action of G_F on $\mathbf{Q}_p/\mathbf{Z}_p(r)$ is non-trivial. The transgression map in the Hochschild-Serre spectral sequence (3.1) is surjective. Furthermore, the short exact sequence of low degree terms induces an exact sequence*

$$0 \rightarrow E_2^{1,0} \rightarrow A \rightarrow B \rightarrow E_2^{2,0} \rightarrow 0 \quad (3.4)$$

where A and B are defined as above and are cyclic direct summands of the respective groups H^1 and $E_2^{0,1}$.

Proof. We may assume $r \cong 0 \pmod{q}$. Using Lemma 3.2, we know that $E_2^{0,1}$ fits into the exact sequence of low degree terms

$$0 \rightarrow \mathbf{Z}/p^j\mathbf{Z} \rightarrow H^1 \rightarrow E_2^{0,1} \rightarrow \mathbf{Z}/p^j\mathbf{Z}. \quad (3.5)$$

By Lemma 3.3, the group H^1 has a summand $A \cong \mathbf{Z}/p^k\mathbf{Z}$ which is the kernel of the map $H^1 \rightarrow H^1(E, \mathbf{Q}_p/\mathbf{Z}_p(r))$. Any cocycle f with class in H^1 coming from $E_2^{1,0}$ by inflation is uniquely described by its value on $\sigma \in G_E$ with $\sigma|_F$ generating $G_{F/E}$. Since the action of G_E on $\mathbf{Q}_p/\mathbf{Z}_p(r)$ is non-trivial, we have necessarily $f(\sigma) = \sigma(a) - a$ for some $a \in \mathbf{Q}_p/\mathbf{Z}_p(r)$, which means that f is in A . Hence $E_2^{1,0}$ maps to A inside H^1 . Furthermore, as restriction commutes with boundary maps, A maps into B under restriction.

By equation (3.3) and Lemma 3.1, B and A are isomorphic. We therefore have that the exact sequence (3.5) has the form of the sequence (3.4) of the Proposition. Let A' denote a complement of A in H^1 and set $B' = \text{Res}(A')$. Since the kernel of Res is contained in A , we have $B \cap B' = 0$. And since the cokernel of Res is the cokernel of Res on B , we have $E_2^{0,1} \cong B \oplus B'$. \square

Remark. The transgression map need not be surjective when the action of G_F on $\mathbf{Q}_p/\mathbf{Z}_p(r)$ is trivial. For instance, in the case $p^n = 4$, $E = \mathbf{R}$, $F = \mathbf{C}$ and $r = 1$ we have that $H^1(\mathbf{C}, \mu_4) = 0$ while $H^2(\mathbf{C}/\mathbf{R}, \mu_4) \cong \mathbf{Z}/2\mathbf{Z}$.

Let \tilde{F} denote the maximal cyclotomic extension of F by p -power roots of 1 (and therefore also of E). Note that if the action of G_F on $\mathbf{Q}_p/\mathbf{Z}_p(r)$ is trivial, then either $F = \tilde{F}$ or $r = 0$. Under the assumption that $r = 0$ and \tilde{F}/F is infinite, we set $A = H^1(\tilde{F}/E, \mathbf{Z}/p^n\mathbf{Z})$ and $B = H^1(\tilde{F}/F, \mathbf{Z}/p^n\mathbf{Z})$.

Proposition 3.5. *Assume that $r = 0$ and \tilde{F}/F is infinite. The transgression map in the Hochschild-Serre spectral sequence (3.1) is surjective. Furthermore, the short*

exact sequence of low degree terms induces an exact sequence of summands

$$0 \rightarrow E_2^{1,0} \rightarrow A \rightarrow B \rightarrow E_2^{2,0} \rightarrow 0. \quad (3.6)$$

Furthermore, A and B are both isomorphic to $\mathbf{Z}/p^n\mathbf{Z}$.

Proof. With $F_1 = E(\zeta_p)$, note that $G_{F_1/E}$ has order prime to p . Hence, A is isomorphic to $H^1(\tilde{F}/F_1, \mathbf{Z}/p^n\mathbf{Z})$. Both $G_{\tilde{F}/F_1}$ and $G_{\tilde{F}/F}$ are infinite groups injecting into the procyclic group \mathbf{Z}_p , and are thereby isomorphic to it. The last statement follows.

The exact sequence (3.6) is just the sequence of low degree terms in the corresponding Hochschild-Serre spectral sequence. The surjectivity of the transgression is forced by the equality of the orders of A and B . Since H^1 and $E_2^{0,1}$ are killed by p^n , the groups A and B are summands. \square

Remark. We now comment on the application of Propositions 3.4 and 3.5 to the results of Chapter 2. In these propositions, we describe, in their respective situations, exact sequences of the form (3.6) which are split off as summands of the exact sequence (3.5). In these cases, there exist complements A' and B' to the subgroups A and B of H^1 and $E_2^{0,1}$, respectively, which are mapped isomorphically to each other via the restriction map.

Recall that in Lemma 2.2 we give a characterization of the elements of F^\times which provide a lifting of a $(d-1)$ -dimensional twisted Kummer representation $\bar{\rho}$ to a d -dimensional twisted Kummer representation with G_E acting by ω^r on $\langle x_d \rangle$. The set X of such elements can be written

$$X = \{x \in F^{1-r} \mid x \notin \langle x_2, \dots, x_{d-1} \rangle F^{\times p}, \bar{x} \notin \text{im Res}\},$$

where \bar{x} denotes the image of x in $F^\times/F^{\times p^n}$ and Res is the restriction from E to F . In the case $j \geq 1$, the set X can be described as

$$X = \{x \in F^{1-r} \mid x = yz, \bar{y} \in B', \bar{z} \in B, \bar{z}^{p^{i+1}} = 1\}.$$

(Note that the group of p -power roots of unity in F^{1-r} projects onto B .) In the case that $j = 0$, all non- p th powers of L^\times in F^{1-r} will yield a lifting.

Furthermore, in Proposition 2.6 and Proposition 2.8 we have that the elements e providing the freedom in the choice of the element c which yields the lifting via transgression are those elements of F^{1-r} which, modulo $F^{1-r} \cap L^{\times p^n}$, are contained in the image of the restriction Res_F from E to F . Note that multiplication by elements of $F^{1-r} \cap L^{\times p^n}$ (i.e., with trivial image in $[L^{\times}/L^{\times p^n}(r-1)]^{L/E}$) will not change the lifting. These are the elements with projections to $[F^{\times}/F^{\times p^n}(r-1)]^{F/E}$ contained in the group of order $p^{2n(d-2)}$ generated by the images of the a_i and b_i with $2 \leq i \leq d-1$. The elements in the image of Res_F are given as the product of any element in B' and any elements of order dividing p^{i+1} in B .

3.2 The spectral sequence for local fields

We maintain the notation of the Section 3.1, restricting in this and future sections to the case that E is a local field over \mathbf{Q}_p . In addition, we define $j'(r)$ to be 0 if $r \not\equiv 1 \pmod{q}$ and the maximal integer such that $r \equiv 1 \pmod{p^{j'}}$ otherwise. We remark that at least one of j and j' is zero.

We begin with the following easy corollary of Lemma 3.1.

Lemma 3.6. *We have that*

$$H^2 \cong \begin{cases} 0 & \text{if } r \not\equiv 1 \pmod{q} \\ \mathbf{Z}/p^{i+j'+1}\mathbf{Z} & \text{if } r \equiv 1 \pmod{q}. \end{cases}$$

Proof. Via the duality induced by the cup product [12, p. 170], we have that $H^2(r) \cong H^0(1-r)$, so we apply Lemma 3.1. \square

From this we can obtain the Tate cohomology groups.

Lemma 3.7. *For all $s \in \mathbf{Z}$ we have $\hat{E}_2^{s,2} = \mathbf{Z}/p^{j'}\mathbf{Z}$.*

Proof. We first take $r = 1$. Note that $H^2(F, \mu_{p^n})$ is the kernel of multiplication by p^n on the Brauer group $\text{Br}(F)$ of F . By Hochschild-Serre, we have the exact sequence

$$0 \rightarrow H^2(F/E, F^{\times}) \rightarrow \text{Br}(E) \rightarrow \text{Br}(F)^{F/E} \rightarrow 0,$$

as

$$H^3(F/E, F^\times) \cong H^1(F/E, F^\times) = 0.$$

As $H^2(F/E, F^\times)$ is finite and $\text{Br}(E) \cong \mathbf{Q}/\mathbf{Z}$ by local class field theory, we conclude that $\text{Br}(F)^{F/E} \cong \mathbf{Q}/\mathbf{Z}$ as well. Since $\text{Br}(F) \cong \mathbf{Q}/\mathbf{Z}$ and any injection from \mathbf{Q}/\mathbf{Z} to itself is an isomorphism, we have $\text{Br}(F)$ is invariant under the action of $G_{F/E}$. Hence $H^2(F, \mu_{p^n}) \cong \mathbf{Z}/p^n\mathbf{Z}$ as a $G_{F/E}$ -module. For arbitrary r , we therefore have that $H^2(F, \mu_{p^n}^{\otimes r}) \cong \mu_{p^n}^{\otimes(r-1)}$. We need only apply Lemma 3.2 to get the result. \square

Note that the cohomological dimensions of G_E and G_F are both 2. Hence $E_2^{s,t}$ and H^t are 0 for $t \geq 3$.

Lemma 3.8. *Let m be the maximum of j and j' (of which at least one is 0). Then $\hat{E}_2^{s,1} \cong \mathbf{Z}/p^m\mathbf{Z}$.*

Proof. By the periodicity of Tate cohomology it suffices to prove this for s sufficiently large. First assume $r \not\equiv 1 \pmod{p}$ so that $j' = 0$. Then $\hat{E}_2^{s,2} = 0$ for all s . Thus, for $s \geq 3$ we have $\ker d_2^{s,1} = E_\infty^{s,1}$ and so is a subquotient of $H^{s+1} = 0$, which implies $d_2^{s,1}$ is injective. At the same time,

$$E_\infty^{s+2,0} = E_2^{s+2,0} / \text{im } d_2^{s,1}$$

is a graded piece of $H^{s+2} = 0$, so $d_2^{s,1}$ is surjective. Hence

$$E_2^{s,1} \cong E_2^{s+2,0} \cong \mathbf{Z}/p^j\mathbf{Z},$$

which implies the claim in this case.

If $r \equiv 1 \pmod{p}$, then $j = 0$ and also $\hat{E}_2^{s,0} = 0$ for all s . Similarly to the above, for $s \geq 3$ we have

$$E_2^{s,1} / \text{im } d_2^{s-2,2} = E_\infty^{s,1} = 0 \quad \text{and} \quad \ker d_2^{s-2,2} = E_\infty^{s-2,2} = 0.$$

Hence $E_2^{s,1} \cong E_2^{s-2,2} \cong \mathbf{Z}/p^{j'}\mathbf{Z}$. \square

Let us define numbers $k(r)$ and $k'(r)$ by $\#H^0 = p^k$ and $\#H^2 = p^{k'}$. These numbers are explicitly given in Lemmas 3.1 and 3.9. We now determine H^1 .

Proposition 3.9. *We have that*

$$H^1 = \mathbf{Z}/p^k\mathbf{Z} \oplus \mathbf{Z}/p^{k'}\mathbf{Z} \oplus (\mathbf{Z}/p^n\mathbf{Z})^{\oplus[E:\mathbf{Q}_p]}.$$

Proof. Since E is a finite extension of \mathbf{Q}_p , if the action of G_E on $\mathbf{Q}_p/\mathbf{Z}_p(r)$ is trivial, then $r = 0$. In this case, we may use the duality induced by the cup product and Kummer theory to say that

$$H^1(E, \mathbf{Z}/p^n\mathbf{Z}) \cong H^1(E, \mu_{p^n}) \cong E^\times/E^{\times p^n}.$$

The proposition then follows in this case, and in the case $r = 1$, from the structure theory of the multiplicative group of a local field. That is, the multiplicative group is isomorphic to a direct sum

$$E^\times \cong \mu \oplus \mathbf{Z} \oplus \mathbf{Z}_p^{\oplus[E:\mathbf{Q}_p]}.$$

where μ denotes the group of roots of unity in E and note that $\mu \cong H^0(E, \mu_{p^n})$.

We may now assume $r \neq 0, 1$, in which case the orders of H^0 and H^2 both stabilize as n increases. As in Lemma 3.3, we use the long exact sequence associated to

$$1 \rightarrow \mu_{p^n}^{\otimes r} \rightarrow \mathbf{Q}_p/\mathbf{Z}_p(r) \rightarrow \mathbf{Q}_p/\mathbf{Z}_p(r) \rightarrow 0$$

and we have that $A = A_E \cong \mathbf{Z}/p^k\mathbf{Z}$ is a direct summand of H^1 .

Since the cohomological dimension of G_E is 2, the long exact sequence ends with

$$H^2 \rightarrow H^2(E, \mathbf{Q}_p/\mathbf{Z}_p(r)) \xrightarrow{p^n} H^2(E, \mathbf{Q}_p/\mathbf{Z}_p(r)) \rightarrow 0. \quad (3.7)$$

The p -torsion group $H^2(E, \mathbf{Q}_p/\mathbf{Z}_p(r))$ is therefore p -divisible. As the order of H^2 stabilizes for n sufficiently large, the leftmost arrow must be zero for such n . But this means multiplication by p is an isomorphism on $H^2(E, \mathbf{Q}_p/\mathbf{Z}_p(r))$, which forces $H^2(E, \mathbf{Q}_p/\mathbf{Z}_p(r))$ to be zero.

Using equation (3.2), we therefore have an exact sequence

$$0 \rightarrow \mathbf{Z}/p^k\mathbf{Z} \rightarrow H^1 \rightarrow H^1(E, \mathbf{Q}_p/\mathbf{Z}_p(r)) \xrightarrow{p^n} H^1(E, \mathbf{Q}_p/\mathbf{Z}_p(r)) \rightarrow \mathbf{Z}/p^{k'}\mathbf{Z} \rightarrow 0. \quad (3.8)$$

Since the order of H^2 stabilizes, we conclude from (3.8) that $H^1(E, \mathbf{Q}_p/\mathbf{Z}_p(r))$ is a direct sum of a cyclic summand $\mathbf{Z}/p^{l'}\mathbf{Z}$ and a divisible p -torsion group. Hence our exact sequence (3.8) reduces to

$$0 \rightarrow \mathbf{Z}/p^k\mathbf{Z} \rightarrow H^1 \rightarrow (\mathbf{Z}/p^n\mathbf{Z})^{\oplus i} \oplus \mathbf{Z}/p^{k'}\mathbf{Z} \rightarrow 0 \quad (3.9)$$

for some number i . The Euler-Poincaré characteristic of $\mu_{p^n}^{\otimes r}$ as a G_E -module is $|\#\mu_{p^n}^{\otimes r}|_E = p^{-n[E:\mathbf{Q}_p]}$, where $|\cdot|_E$ is the absolute value on E [12, p. 171]. Hence the order of $H^1(E, \mu_{p^n}^{\otimes r})$ is $p^{k+k'+n[E:\mathbf{Q}_p]}$. That is, $i = [E:\mathbf{Q}_p]$. \square

Finally, we determine the remaining term in the spectral sequence.

Proposition 3.10. *Let k be such that the order of H^0 is p^k and k' be such that the order of H^2 is $p^{k'}$. Then*

$$E_2^{0,1} = \mathbf{Z}/p^k\mathbf{Z} \oplus \mathbf{Z}/p^{k'}\mathbf{Z} \oplus (\mathbf{Z}/p^n\mathbf{Z})^{\oplus [E:\mathbf{Q}_p]}.$$

Proof. For $r \neq 0$ we refer to Proposition 3.4. In the case $r = 0$, we are in the situation of Lemma 3.5. In either case, we have by Proposition 3.9 that since the groups A and B of Section 3.1 are direct summands, restriction induces an isomorphism between complements of these groups. The complement of A is isomorphic to $\mathbf{Z}/p^{k'}\mathbf{Z} \oplus \mathbf{Z}/p^n\mathbf{Z}^{[E:\mathbf{Q}_p]}$ and $B \cong \mathbf{Z}/p^k\mathbf{Z}$, so the result follows. \square

Remark. The groups A' and B' in the remarks of Section 3.1 are both isomorphic to $\mathbf{Z}/p^{k'}\mathbf{Z} \oplus \mathbf{Z}/p^n\mathbf{Z}^{[E:\mathbf{Q}_p]}$. This allows for an exact count of the number of elements (modulo p^n th powers) providing liftings of twisted Kummer representations to higher-dimensional twisted Kummer representations or to twisted Heisenberg representations.

3.3 Twisted Heisenberg representations

Let Δ be the subgroup of $G_{F/E}$ of order q . Let $\widehat{F^\times}$ denote the \mathbf{Z}_p -completion of F^\times . The action of Δ on $\widehat{F^\times}$ is semisimple, hence $\widehat{F^\times}$ decomposes into a direct sum of eigenspaces for the powers of the cyclotomic character on Δ . We let D_r denote the eigenspace consisting of $x \in \widehat{F^\times}$ such that

$$\sigma(x) = x^{\delta^r(\sigma)},$$

where $\delta: \Delta \rightarrow \mathbf{Z}_p^*$ is the character which reduces to $\omega|_\Delta$ under composition with the surjection $\mathbf{Z}_p^* \rightarrow (\mathbf{Z}/p\mathbf{Z})^*$.

Lemma 3.11. *The pairing*

$$D_s \times D_t \rightarrow \mu_{p^n}$$

induced by the Hilbert norm residue symbol is trivial unless $t \equiv 1 - s \pmod{q}$ and nondegenerate otherwise.

Proof. Let us evaluate (a_s, a_t) with $a_s \in D_s$ and $a_t \in D_t$. Let $i = \delta(\sigma)$ for a generator σ of Δ . Then we have

$$(a_s, a_t) = \sigma(a_s, a_t)^{i^{-1}}.$$

By Galois equivariance of the norm residue symbol, the last term equals

$$(\sigma(a_s), \sigma(a_t))^{i^{-1}} = (a_s^{i^s}, a_t^{i^t})^{i^{-1}} = (a_s, a_t)^{i^{s+t-1}}.$$

Hence either $i^{s+t-1} \equiv 1 \pmod{p}$ or $(a_s, a_t) = 1$. However, as i has order dividing $p-1$, the former condition is exactly that $i^{s+t-1} \equiv 1 \pmod{p^n}$. This proves the first statement and the second follows by nondegeneracy of the norm residue symbol. \square

Remark. Although we have not done it here, Lemma 3.11 could be used, along with the results of Section 3.2, to gain more information on the cup product pairing $H^1(s) \times H^1(t) \rightarrow \mathbf{Z}/m\mathbf{Z}$ or on the pairing induced by the Hilbert norm residue symbol $F^s \times F^t \rightarrow \mu_{p^n}$.

We now return to the situation of Section 2.5 and consider a three-dimensional Kummer representation $\bar{\rho}$ of G_E with twists given by the characters ω^{r-s} and ω^s on the cyclic groups generated by x and y , respectively. We let $K = F(\sqrt[p^n]{a})$ and $K' = F(\sqrt[p^n]{b})$ and $L = KK'$ for a and b given as in Section 2.5. Under certain assumptions, we can give conditions for Proposition 2.7 to hold. As in Proposition 2.7, let E' denote a field such that $G_{K/E'} \cong G_{F/E}$ via restriction.

Theorem 3.12. *Assume that $r \not\equiv 1 \pmod{q}$ and $j(s) = j'(s) = 0$. There exists $\beta \in (K/E')^{1-s}$ with $N_{K/F}(\beta) = b$. We have that*

$$c = \prod_{i=0}^{p^n-1} \tau^i(\beta)^i$$

satisfies $c \in L^{1-r}$ and $\bar{\rho}$ lifts to a twisted Heisenberg representation which restricts to the character of order p^n associated to c on G_L . Furthermore, if $j(r) = 0$ then the element $c \in L^{1-r}$ providing a lifting is unique up to multiplication by any element of $F^{1-r} L^{\times p^n}$.

Proof. For an integer t , we define

$$N_t: F^\times / F^{\times p^n}(t-1) \rightarrow [F^\times / F^{\times p^n}(t-1)]^{F/E}$$

by

$$N_t(X) = \prod_{\sigma \in G_{F/E}} \sigma(X)^{\omega^t(\sigma)}$$

for $X \in F^\times / F^{\times p^n}$. We also let N_t denote any lifting of N_t to a homomorphism $N_t: F^\times \rightarrow F^{1-t}$.

As $j(s) = j'(s) = 0$, we see that $\hat{E}_2^{0,1}(s) = 0$ by Lemma 3.8. As $b \in F^{1-s}$, we have therefore that $b = \delta p^n N_s(\gamma)$ for some $\delta, \gamma \in F^\times$. Note also that $N_s D_i \subset \widehat{F^\times} \cap F^{\times p^n}$ if $i \not\equiv 1-s \pmod{q}$. Hence, we may assume $\gamma \in D_{1-s}$.

Since $r \not\equiv 1 \pmod{q}$ we conclude by Lemma 3.11 that $(a, \gamma) = 1$. Hence, there exists $\alpha \in K$ such that $\gamma = N_{K/F}(\alpha)$. Set $\beta = \delta N_s(\alpha) \in K^{1-s}$ after extending N_s

to a map on K^\times defined in the same manner (via the identification of $G_{F/E}$ with $G_{K/E'}$ as in Proposition 2.7). Note that N_s commutes with $N_{K/F}$. We see that

$$N_{K/F}(\beta) = \delta^{p^n} N_s N_{K/F}(\alpha) = \delta^{p^n} N_s(\gamma) = b.$$

As $r \not\equiv 1 \pmod{q}$, we have that $H^2(r) = 0$. Hence, $\text{Res}_F \circ \text{Tra}_E$ is the trivial map. That $\bar{\rho}$ lifts to a twisted Heisenberg representation follows from Proposition 2.7.

The last statement follows from the remarks at the end of Section 3.1. That is, the kernel of Tra_E is the image of the restriction

$$\text{Res}: H^1(r) \rightarrow H^1(L, \mu_{p^n}^{\otimes r})^{L/E}.$$

If $j(r) = 0$ then $E_2^{2,0}(r) = 0$, and therefore Res factors through $E_2^{0,1}(r)$. Hence the product of c and any element of F^{1-r} also yields a lifting. \square

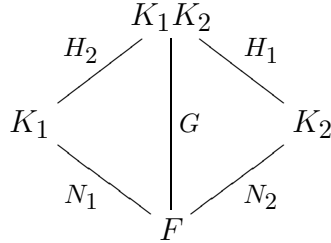
Remark. Alternatively to assuming $j(s) = j'(s) = 0$, one may merely assume that $b \in F^{\times p^n} N_s F^\times$. This should often not be necessary: i.e., that b be a twisted norm rather than just invariant under a twisted action. Furthermore, the restriction $r \equiv 1 \pmod{q}$ is clearly not always necessary, for instance when $F = E$.

CHAPTER 4 RAMIFICATION

4.1 Preliminaries

In this section, we prove some general lemmas on ramification numbers of local fields which will be useful to us later. These are well-known or easy, but for convenience we prove them here. For a Galois extension with group G , let ϕ_G and ψ_G be the functions which allow one to pass between the lower and upper numberings of the ramification groups [15, IV.3]. In particular, for a real number $w \geq -1$ we have $G^w = G_{\psi_G(w)}$ and $G_w = G^{\phi_G(w)}$.

We consider Galois extensions of local fields K_1/F and K_2/F with $K_1 \cap K_2 = F$. We define Galois groups via the following diagram.



Note that $G/H_1 = N_2$, $G/H_2 = N_1$ and $H_i \cong N_i$ for both i . We may identify subgroups of H_i and N_i through the latter isomorphism.

Given the ramification filtration for two adjacent sides of the diagram, we can obtain the ramification filtration for the other two.

Lemma 4.1. *For any real number $w \geq -1$ we have*

$$H_1^w \cong N_1^{\phi_{N_2}(w)}$$

via the natural isomorphism between N_1 and H_1 .

Proof. This follows from the usual properties of the ramification numberings [15, IV.3], as we demonstrate below. We have

$$H_1^w = (H_1)_{\psi_{H_1}(w)} = G_{\psi_{H_1}(w)} \cap H_1 = G^{\phi_{N_2}(w)} \cap H_1.$$

Using the isomorphism between H_1 and $N_1 = G/H_2$, this becomes

$$G^{\phi_{N_2}(w)} H_2/H_2 = N_1^{\phi_{N_2}(w)}.$$

□

We also have the following trivial corollary.

Corollary 4.2. *For any real number $w \geq -1$, we have*

$$N_1^w \cong H_1^{\psi_{N_2}(w)}.$$

Hence, a jump in the ramification filtration of K_1/F occurs at a number l in the upper numbering of if and only if a jump in the filtration of $K_1 K_2/K_2$ occurs at $\psi_{N_2}(l)$.

In this chapter, p will denote an odd prime. For a local field K/\mathbf{Q}_p containing the p^n th roots of unity and $a \in K^\times$ we denote by $f_{n,K}(a)$ the conductor of $K(p^n\sqrt{a})/K$ (considered as an integer) [15, XV.2], and we let $(\cdot, \cdot)_{n,K}$ denote the p^n th norm residue symbol of K . Let U_i denote the i th unit group of K for $i \geq 1$, and set $U_0 = U$. Then $f = f_{n,K}(a)$ is the smallest nonnegative integer for which $(a, u)_{n,K} = 1$ for all $u \in U_f$.

Let e denote the ramification index of K . We have the following lemma.

Lemma 4.3. *If $f_{n,K}(a^p) > e/(p-1) + 1$ then $f_{n,K}(a) = f_{n,K}(a^p) + e$.*

Proof. Let $b \in U_{e/(p-1)+1}$, so that the valuation of $b^p - 1$ is e more than that of $b - 1$. Since $(a^p, b)_{n,K} = (a, b^p)_{n,K}$, we conclude that $f_{n,K}(a) = f_{n,K}(a^p) + e$. □

Let $F_m = \mathbf{Q}_p(\zeta_{p^m})$ for each m . We consider now a diagram of the following form.

$$\begin{array}{ccccc}
 & & F_{n+1}(p^n\sqrt[n]{a}) & & \\
 & H_2 \swarrow & | & \searrow H_1 & \\
 F_n(p^n\sqrt[n]{a}) & & G & & F_{n+1} \\
 & N_1 \searrow & | & \swarrow N_2 & \\
 & & F_n & &
 \end{array}$$

For $a \in F_n^\times$, let $f_n(a) = f_{n,F_n}(a)$. The extension F_{n+1}/F_n has conductor p^n [15, IV.4]. Note that conductors are one more than the numbers where the jumps actually occur.

We have the following simple lemma.

Lemma 4.4. *Let $a \in F_n^\times$.*

(a) *We have*

$$f_{n+1}(a^p) = \begin{cases} f_n(a) & \text{if } f_n(a) < p^n \\ pf_n(a) - p^n(p-1) & \text{if } f_n(a) \geq p^n. \end{cases}$$

(b) *If $f_n(a) > p^n$ then $f_{n+1}(a) = pf_n(a)$.*

Proof. Part (a) follows immediately from Corollary 4.2, since the function ψ for the extension F_{n+1}/F_n is given by

$$\psi(r) = \begin{cases} r & \text{if } -1 \leq r \leq p^n - 1 \\ p^n - 1 + p(r - (p^n - 1)) & \text{if } r > p^n - 1. \end{cases}$$

As for part (b), we remark that, as $f_n(a) > p^n$ we have by part (a) that $f_{n+1}(a^p) > p^n + 1$. Hence, by Lemma 4.3, we have that $f_{n+1}(a) = f_{n+1}(a^p) + p^n(p-1)$. By part (a), this equals $pf_n(a)$. \square

4.2 The multiplicative group as a module

Let $F = \mathbf{Q}_p(\zeta_{p^n})$. We may decompose G_{F/\mathbf{Q}_p} with p odd into a direct product of cyclic groups $\Delta \times \Gamma$ where Δ has order $p-1$ and Γ has order p^{n-1} . We let F_1 denote the fixed field $\mathbf{Q}_p(\zeta_p)$ of Γ . We also define $\widehat{F^\times}$, D_r and δ as in Section 3.3. It is the goal of this section to gain an understanding of the $\mathbf{Z}_p[\Gamma]$ -module structure of D_r . We begin with the following lemma regarding the structure of D_r .

Lemma 4.5. *The eigenspace D_r has rank $p^{n-1} + 1$ as a \mathbf{Z}_p -module if $r \equiv 0 \pmod{p-1}$ and p^{n-1} otherwise. If $r \equiv 1 \pmod{p-1}$, then D_r has non-zero cyclic torsion and otherwise D_r has no torsion. Furthermore, D_r has a minimal set of generators*

$$\{x_t \in U_t - U_{t+1} \mid t \equiv r \pmod{p-1}, p \nmid t, t < p^n\}$$

with one extra generator x_0 of non-zero valuation when $r \equiv 0 \pmod{p-1}$ and one extra generator $x_{p^n} \in U_{p^n} - U_{p^{n+1}}$ when $r \equiv 1 \pmod{p-1}$.

Proof. Note first that the only torsion is μ_{p^n} , which is contained in D_1 . Consider $x \in D_r$ for some r . If x has non-zero valuation, then since $\sigma(x)$ has the same valuation as x , we must have $r \equiv 0 \pmod{p-1}$. As $\widehat{F^\times}$ is the direct sum of the D_r , there exists $x_0 \in D_0$ with valuation 1. So assume that x is a unit, $x \in U_t - U_{t+1}$. Let $\lambda_n = 1 - \zeta_{p^n}$. Then we have

$$\sigma(\lambda_n) \equiv \delta(\sigma)\lambda_n \pmod{(\lambda_n^2)}.$$

So we see that

$$\sigma(x) \equiv 1 + \delta(\sigma)^t(x-1) \equiv x^{\delta(\sigma)^t} \pmod{(\lambda_n^{t+1})}.$$

Hence, as $x \in D_r$, we must have $t \equiv r \pmod{p-1}$. Furthermore, for each such t , there is an element $x_t \in U_t \cap D_r$ such that $x_t \notin U_{t+1}$, for instance,

$$x_t = \prod_{\sigma \in \Delta} (1 - \sigma(\lambda_n^t))^{\delta(\sigma)^{-t}}.$$

To see $x_t \notin U_{t+1}$, note that we have

$$x_t \equiv \prod_{\sigma \in \Delta} (1 - \delta(\sigma)^t \lambda_n^t)^{\delta(\sigma)^{-t}} \equiv (1 - \lambda_n^t)^{p-1} \equiv 1 + \lambda_n^t \pmod{(\lambda_n^{t+1})}.$$

Note that none of the elements of

$$X = \{x_t \mid p \nmid t, t < p^n \text{ or } t = 0, p^n\}$$

can be p th powers. Furthermore, the elements of X are linearly independent in the $p^{n-1}(p-1) + 2$ -dimensional $\mathbf{Z}/p\mathbf{Z}$ -vector space $F^\times/F^{\times p^n}$. Therefore, X is a minimal generating set of $\widehat{F^\times}$ as a \mathbf{Z}_p -module. \square

Recall that $f_n(x)$ denotes the conductor of $F(p\sqrt[n]{x})/F$. We have the following easy corollary of Lemmas 3.11 and 4.5.

Corollary 4.6. *Let $x \in D_r \cap F^\times$. Then either $f_n(x) \equiv 2 - r \pmod{p-1}$ or $f_n(x) = 1$.*

Proof. If for some s we have a unit $y \in U_1 \cap D_s$ with $(x, y) \neq 1$, then $s \equiv 1 - r \pmod{p-1}$ by Lemma 3.11. By Lemma 4.5 we have that $v(y-1) \equiv 1 - r \pmod{p-1}$, where v denotes the additive valuation on F . \square

Each eigenspace D_r is a $\mathbf{Z}_p[\Gamma]$ -module. By Iwasawa Theory [13, §7.2], we know that in fact D_r is a free $\mathbf{Z}_p[\Gamma]$ -module of rank 1 when $r \not\equiv 0, 1 \pmod{p-1}$. We give a nice proof of this result, suggested by Hendrik Lenstra.

Proposition 4.7. *If $r \not\equiv 0, 1 \pmod{p-1}$ then D_r is a free $\mathbf{Z}_p[\Gamma]$ -module of rank 1. Otherwise D_r can be generated by two elements as a $\mathbf{Z}_p[\Gamma]$ -module.*

Proof. By Lemma 4.5, D_r has the correct minimal number of \mathbf{Z}_p -generators to be a free of rank one $\mathbf{Z}_p[\Gamma]$ -module when $r \not\equiv 0, 1 \pmod{p-1}$, but one too many for this when $r \equiv 0, 1 \pmod{p-1}$. Hence it takes at least one element to generate D_r as a $\mathbf{Z}_p[\Gamma]$ -module when $r \not\equiv 0, 1 \pmod{p-1}$ and at least two otherwise. In total, we must have at least $p+1$ generators.

Consider the abelian extension L of F with norm group $F^{\times p} I_\Gamma F^\times$, where I_Γ is the augmentation ideal of $\mathbf{Z}[\Gamma]$. Let $H = N_{F/F_1} F^\times$. By local class field theory we

have a Γ -module isomorphism $G_{L/F} \cong F^\times / F^{\times p} I_\Gamma F^\times$. Hence Γ acts trivially on this $G_{L/F}$ by conjugation. That is, L/F_1 is abelian. Furthermore,

$$N_{L/F_1} L^\times = N_{F/F_1} (F^{\times p} I_\Gamma F^\times) = N_{F/F_1} F^{\times p} = H^p.$$

Therefore the order of $F^\times / F^{\times p} I_\Gamma F^\times$, which is p to the minimal number of generators of $\widehat{F^\times}$ as a $\mathbf{Z}_p[\Gamma]$ -module, is equal to the index $[H : H^p]$.

But H is a subgroup of F_1^\times , the completion of which is a \mathbf{Z}_p -module generated by $p + 1$ elements. Hence $[H : H^p] \leq p^{p+1}$. As we know that we must have at least $p + 1$ generators, we have equality and the proposition is proven. \square

Greither [8] has worked out explicitly the Galois module structure of F^\times (and in fact for any finite unramified extension of F). Though we shall not actually use it, Greither's result is useful in dealing with the "bad" cases $r \equiv 0, 1 \pmod{p-1}$ in the determination of conductors as in Section 4.4. Therefore, we state the result below in our case, attempting to maintain a degree of notational consistency with [8].

Let Q be the $\mathbf{Z}[G_{F/\mathbf{Q}_p}]$ -module with generators Π and V and the relation Δ fixes V . Let Q_0 denote the submodule generated by U and V with $U = \sigma(\Pi) - \Pi$ for some generator σ of Δ . Let $Q_{0,p}$ denote the \mathbf{Z}_p -completion of Q_0 . Let Q_p denote the pushout $Q_{0,p} \amalg_{Q_0} Q$. Finally, let $Q' = Q_p \times \mu$ where μ is the module isomorphic to all roots of 1 in F .

Theorem 4.8 (Greither). *There is an isomorphism $Q' \rightarrow F^\times$ of $\mathbf{Z}[G_{F/\mathbf{Q}_p}]$ -modules taking Π to a prime element, V to $1 - p$, and the roots of unity to themselves.*

Remark. Theorem 4.8 is obtained via specifying Theorem 3.1 of [8] to the case of a totally ramified extension. The statement follows since \tilde{Q} as defined in [8] satisfies $\tilde{Q} \times \mu_p^n \cong Q'$ and since his map $\tilde{\beta}$ induces a split exact sequence by Step 2 of Theorem 2.9 of [8].

By taking \mathbf{Z}_p -completions, we obtain the following result.

Corollary 4.9. *There exists a prime element π of F^\times such that the $\mathbf{Z}_p[G_F/\mathbf{Q}_p]$ -submodule M of $\widehat{F^\times}$ generated by π is free and yielding a decomposition*

$$\widehat{F^\times} = M \times \mu_{p^n} \times \langle 1 - p \rangle^{\mathbf{Z}_p}.$$

4.3 Comparison of module structure with unit filtration

Let π and M be as in Corollary 4.9, and set $M_r = D_r \cap M$ for all r . Then M_r is a free $\mathbf{Z}_p[\Gamma]$ -module of rank 1, and for $r \not\equiv 0, 1 \pmod{p-1}$ we have $M_r = D_r$. We choose a generator y_r of M_r as a $\mathbf{Z}_p[\Gamma]$ -module. We identify M_r with $\mathbf{Z}_p[\Gamma]$ via the isomorphism

$$\mathbf{Z}_p[\Gamma] \xrightarrow{\sim} M_r, \quad \alpha \mapsto y_r^\alpha \tag{4.1}$$

of $\mathbf{Z}_p[\Gamma]$ -modules. Each subgroup arising from a unit group $V_t = U_t \cap M_r$ with $t > 0$ becomes identified with an ideal of $\mathbf{Z}_p[\Gamma]$ (independent of y_r) and by abuse of notation we treat them as equal. (Therefore, we may use either additive or multiplicative notation, depending on what is most notationally convenient for the situation.) Note that Lemma 4.5 implies that $V_t = V_{t+1}$ for $t \not\equiv r \pmod{p-1}$. Therefore we need only consider $t \equiv r \pmod{p-1}$.

Let γ denote a generator of Γ . We wish to determine V_t as an ideal. Note that $[V_t : V_{t+p-1}]$ is either 1 or p , and if $t \not\equiv 0, 1 \pmod{p-1}$ then $[V_t : V_{t+p-1}] = p$. We set $V'_t = V_t - V_{t+p-1}$. If $2 \leq u \leq p-2$, then $V_u = \mathbf{Z}_p[\Gamma]$ and, as $\mathbf{Z}_p[\Gamma]$ is a local ring, V_{u+p-1} is the maximal ideal $(p, \gamma - 1)$.

Lemma 4.10. *Let $x_t \in V'_t$ for $t \equiv r \pmod{p-1}$. If $p \nmid t$, then $\gamma(x_t)/x_t \in V'_{t+p-1}$. Otherwise, $\gamma(x_t)/x_t \in V_{t+2(p-1)}$.*

Proof. From the ramification groups of F/\mathbf{Q}_p in the lower numbering [15, IV.4], we see that $v(\gamma(\pi)/\pi - 1) = p - 1$, where v is the valuation on F and π is any prime element of F . Hence, for any $x \in U_t$ with $p \nmid v(x - 1)$, we have $v(\gamma(x) - x) = t + p - 1$. On the other hand, if $p \mid v(x - 1)$ then $v(\gamma(x) - x) > t + p - 1$. Since $\gamma(x_t)/x_t \in M_r$, the result follows. \square

Lemma 4.11. *Let $x_t \in V'_t$ for $t \equiv r \pmod{p-1}$. For $j \geq 1$, we have*

$$x_t^{(\gamma-1)^j} \in V_{jp}.$$

Proof. We will show the stronger result that

$$x_t^{(\gamma-1)^j} \in V_{t+(j+\lceil \frac{j-q}{p-1} \rceil)(p-1)}, \quad (4.2)$$

where $\lceil \cdot \rceil$ denotes the ceiling function and q denotes the smallest nonnegative integer with $q \equiv t \pmod{p-1}$. This implies the lemma since

$$t + (j + \lceil \frac{j-q}{p-1} \rceil)(p-1) \geq t + j(p-1) + j - q \geq jp.$$

Lemma 4.10 implies that $V_u^{(\gamma-1)} \subseteq V_{u+p-1}$ for all $u \equiv t \pmod{p-1}$. Hence

$$x_t^{(\gamma-1)^j} \in V_{u+j(p-1)}. \quad (4.3)$$

Furthermore, Lemma 4.10 implies that $x_t^{(\gamma-1)^q} \in V'_{p+(p-1)q}$ and that $a^{(\gamma-1)^{p-1}} \in V_{u+p(p-1)}$ for $a \in V'_u$ with $u \equiv t \pmod{p-1}$. Together these show that for every $p-1$ applications of $\gamma-1$ after the q th and starting with the $(q+1)$ st, we can add an additional $p-1$ to the subscript of V in (4.3), which yields equation (4.2). \square

4.4 Conductors in the metabelian case

We keep the notation of the previous section, but we now choose γ so that $\gamma(\zeta_{p^n}) = \zeta_{p^n}^{1+p}$. By (1.4), we have that $x \in F^{1-r}$ implies

$$\gamma(x) \equiv x^{(1+p)^{1-r}} \pmod{F^{\times p^n}}. \quad (4.4)$$

Furthermore, we assume in this section that $r \not\equiv 0, 1 \pmod{p-1}$. We then have as before $y_r \in D_r$ generating D_r as a free $\mathbf{Z}_p[\Gamma]$ -module, and hence its image generates $D_r / (D_r \cap \widehat{F^{\times p^n}})$ as a free $\mathbf{Z}/p^n\mathbf{Z}[\Gamma]$ -module.

Let $x \in F^{1-r}$. Our goal in this section is the determination of the conductor of the extension $F(\sqrt[p^n]{x})/F$. This is exactly the conductor of the norm residue symbol (x, \cdot) , where (\cdot, \cdot) denotes the p^n th norm residue symbol over F .

Lemma 4.12. *If $x \in F^{1-r}$ and $x \notin F^{\times p}$, then the symbol (x, y_r) is a primitive p^n th root of unity.*

Proof. The nondegeneracy of the norm residue symbol as proven in Lemma 3.11 implies that (x, y) is a primitive p^n th root of unity for some $y \in D_r$. But as D_r is a free $\mathbf{Z}_p[\Gamma]$ -module generated by y_r , and since we have that

$$\gamma(x, y_r) = (x, \gamma(y_r))^{(1+p)^{1-r}}$$

by (4.4), this cannot happen unless (x, y_r) is a primitive p^n th root of unity as well. \square

For $\alpha \in D_r$, we let $[x, \alpha] \in \mathbf{Z}/p^n\mathbf{Z}$ denote the power of (x, y_r) which (x, α) equals.

Lemma 4.13. *Let*

$$\alpha = y_r^{f(\gamma)}$$

with $f \in \mathbf{Z}_p[X]$. Then

$$[x, \alpha] \equiv f((1+p)^r) \pmod{p^n}.$$

Proof. We need only show that $[x, \gamma^j(y_r)] = (1+p)^{jr}$. We have

$$(x, \gamma^j(y_r)) = \gamma^j(\gamma^{-j}(x), y_r) = (x^{(1+p)^{-j(1-r)}}, y_r)^{(1+p)^j} = (x, y_r)^{(1+p)^{jr}}.$$

\square

Corollary 4.14. *We have*

$$(x, y_r^{p^k(\gamma-1)^{n-k}}) = 1$$

for $0 \leq k \leq n$.

Proof. We calculate:

$$[x, y_r^{p^k(\gamma-1)^{n-k}}] = p^k(1+p-1)^{n-k} \equiv 0 \pmod{p^n}.$$

□

Note that

$$\mathbf{Z}_p[\Gamma] \cong \mathbf{Z}_p[X]/(X^{p^{n-1}} - 1).$$

We shall require the following result.

Lemma 4.15. *In $\mathbf{Z}_p[X]$, the polynomial $X^{p^{n-1}} - 1$ is contained in the ideal*

$$(p^{n-1}(X-1), p^{n-2}(X-1)^p, \dots, (X-1)^{p^{n-1}}).$$

Proof. Let $Y = X - 1$. We need only show that

$$(Y+1)^{p^{n-1}} - 1 \in (p^{n-1}Y, p^{n-2}Y^p, \dots, Y^{p^{n-1}}).$$

It suffices therefore to verify that if $p^m \leq k < p^{m+1}$ with $0 \leq m < n-1$ then $v_p\left(\binom{p^{n-1}}{k}\right) \geq n-1-m$, where v_p denotes the p -adic valuation. We note that, in fact,

$$v_p\left(\binom{p^{n-1}}{k}\right) = n-1-v_p(k)$$

for $1 \leq k \leq p^{n-1}$, which implies the claim. □

To determine the conductor of (x, \cdot) , it suffices to look at two ideals of $\mathbf{Z}_p[\Gamma]$. Let t denote the smallest nonnegative integer such that $t \equiv r \pmod{p-1}$.

Lemma 4.16. *The ideal $V_{p^{n-1}(t+1)-1}$ of D_r contains an element a of the form*

$$a = p^{n-1} + \sum_{k=1}^{n-1} d_k p^{n-1-k} (\gamma-1)^{p^{k-1}(t+1)-1}$$

with $d_k \in \mathbf{Z}_p$. The ideal $V_{p^{n-1}(t+1)+p-2}$ of $\mathbf{Z}_p[\Gamma]$ is generated by p^n , $p^{n-1}(\gamma-1)$ and $p^{n-1-k}(\gamma-1)^{p^{k-1}(t+1)}$ for $1 \leq k \leq n-1$.

Proof. We begin with the second statement. We abuse notation via the identification (4.1) so that we can consider the unit groups additively. By Lemma 4.15, we have

that the ideal I of $\mathbf{Z}_p[X]$ generated by $p^{n-1}(X-1)$ and $p^{n-1-k}(X-1)^{p^{k-1}(t+1)}$ for $1 \leq k \leq n-1$ contains $X^{p^{n-1}} - 1$. Hence the image of I in $\mathbf{Z}_p[\Gamma]$ has index equal to the index of I in $\mathbf{Z}_p[X]$. This is equal to p to the power of

$$n+t(n-1)+(p-1)(t+1)(n-2)+\dots+p^{n-3}(p-1)(t+1) = (p^{n-2}+\dots+p+1)(t+1)+1.$$

This is equal to $[\mathbf{Z}_p[\Gamma] : V_{p^{n-1}(t+1)+p-2}]$.

To prove the second statement, we are left only to verify the claim that $I \subseteq V_{p^{n-1}(t+1)+p-2}$. By Lemma 4.10, we see that

$$p^{n-1}(\gamma-1) \in p^{n-1}V_{t+p-1} \subseteq p^{n-1}V_p \subseteq V_{p^n} \subseteq V_{p^{n-1}(t+1)+p-2}$$

as $2 \leq t \leq p-2$. Similarly, Lemma 4.11 yields

$$p^{n-k-1}(\gamma-1)^{p^{k-1}(t+1)} \in p^{n-k-1}V_{p^k(t+1)+p-2} \subseteq V_{p^{n-1}(t+1)+p^{n-k-1}(p-2)} \subseteq V_{p^{n-1}(t+1)+p-2}.$$

Hence we have the claim.

For the first statement, we proceed by constructing a finite sequence of elements which are not contained in I , the last of which is the desired element. Note that for an element $b \in V'_u$ for some $u \equiv t \pmod{p}$ such that $pb \notin I$, we have $pb \in V'_{pu}$ since $V_{p^{n+1}} \subseteq I$.

In V'_{pt} we have two distinct elements: p and a_1 for some element $a_1 \in \mathbf{Z}_p[\Gamma]$ which is nonzero modulo p . The latter element exists by Lemma 4.10, as $(\gamma-1)g \in V'_{pt}$ for any $g \in V'_{p(t+1)-1}$. Multiplying a_1 by a constant which is nonzero modulo p if necessary, we can insure that

$$p + a_1 \in V_{pt+p-1}.$$

Then we have $p^2 + pa_1 \in V_{p^2(t+1)-p}$. In fact, the latter element is in V'_{pu} for some $u \equiv t \pmod{p-1}$. Therefore, we can find as above $a_2 \not\equiv 0 \pmod{p}$ in V'_{pu} such that

$$p^2 + pa_1 + a_2 \in V_{p^2(t+1)-1}.$$

Multiplying this by p , we have an element in $V_{p^3(t+1)-p}$. Continuing on in this fashion, we obtain an element

$$a = p^{n-1} + p^{n-2}a_1 + \dots + a_{n-1} \in V_{p^{n-1}(t+1)-1}.$$

As a is not an element of I (by the second statement), we have in fact that $a \in V'_{p^{n-1}(t+1)-1}$. As

$$(\gamma - 1)V_{p^{n-1}(t+1)-1} \subseteq V_{p^{n-1}(t+1)+p-2},$$

we have by the second statement that $V_{p^{n-1}(t+1)-1}$ is contained in the ideal generated by p^{n-1} and $p^{n-1-k}(\gamma - 1)^{p^{k-1}(t+1)-1}$ for $1 \leq k \leq n-1$. Using this and the second statement, it is clear that a_k may be chosen to have the form $d_k(\gamma - 1)^{p^{k-1}(t+1)-1}$. \square

We now determine the desired conductors.

Theorem 4.17. *Let $r \not\equiv 0, 1 \pmod{p-1}$ and let t denote the smallest nonnegative integer with $t \equiv r \pmod{p-1}$. Let $x \in F^{1-r}$ with $x \notin F^{\times p}$. Then we have that $f_{m,F}(x) = (t+1)p^{m-1}$ for any positive integer m with $m \leq n$.*

Proof. By Corollary 4.14, $(x, y) = 1$ for each generator y of $V_{p^{n-1}(t+1)+p-2}$ listed in Lemma 4.16. On the other hand, for the element $a \in \mathbf{Z}_p[\Gamma]$ of Lemma 4.16, we have

$$[x, y_r^a] = [x, y_r^{p^{n-1}}] = p^{n-1}.$$

Noting Corollary 4.6, we see that the conductor of x is therefore $((1 - \zeta_{p^n})^{p^{n-1}(t+1)})$.

Setting $F_m = \mathbf{Q}_p(\zeta_{p^m})$ and $f_m = f_{m, F_m}$ as in Section 4.1, we now have that $f_m(x) = p^{m-1}(t+1)$. Since $t+1 < p$, Lemma 4.4a yields that

$$f_{m,F}(x) = f_n(x^{p^{n-m}}) = f_m(x),$$

which is as desired. \square

Remark. Although we have not written it out here, to compute the conductors for elements fixed under a twisted action of G_F/\mathbf{Q}_p in the “bad” cases $r \equiv 0, 1 \pmod{p-1}$, one can use Theorem 4.8 and proceed as in this section. In fact, one can in all cases actually determine explicit generators for each V_t as an ideal of $\mathbf{Z}_p[\gamma]$, as we have done in some specific cases in Lemma 4.16.

4.5 Ramification in a Heisenberg extension

We consider the twisted Heisenberg extension $\mathbf{Q}_p(\zeta_{p^n}, p^n\sqrt{p}, p^n\sqrt{1-p}, p^n\sqrt{c_n})/\mathbf{Q}_p$, where

$$c_n = \prod_{i=1}^{p^n} (1 - \zeta_{p^n}^i p^n\sqrt{p})^i.$$

This example is fundamental as, up to multiplying c_n by an element of F^\times , it is the only Heisenberg extension with lower steps coming from adjoining \mathbf{Q}_p all of its p^n th roots. (In fact, our computations will show that the conductor of the top step does not depend in this case on the choice of c_n .)

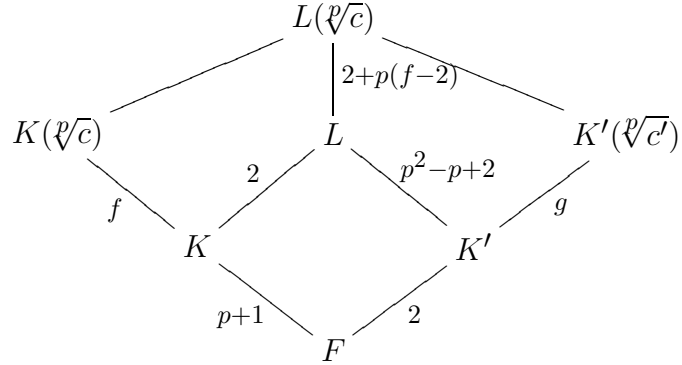
Let $F_n = \mathbf{Q}_p(\zeta_{p^n})$, $K_n = F_n(p^n\sqrt{p})$, $K'_n = F_n(p^n\sqrt{p^p(1-p)})$ and $L_n = K_n K'_n$. The conductors of K_n/F_n and K'_n/F_n were computed for all $n \geq 1$ in [3] (see also [20]). By induction on n , we shall determine the conductors of $K'_n(p^m\sqrt{c'_n})/K'_n$ for all $m \leq n$, where $c'_n \in K'_n$ differs from c_n by a p^n th power in K_n . We shall then use these conductors to compute the conductors of $L_n(p^n\sqrt{c_n})/L_n$.

We begin with the case $n = 1$.

Proposition 4.18. *We have $f_{1, K'_1}(c') = p^2 - p + 3$.*

Proof. For notational simplicity, we drop all subscript 1’s from the notation in this proof. We have the following diagram of field extensions, in which the numbers denote the conductors of the indicated extension. (The conductors of K/F and K'/F are

easily seen using Corollary 4.6 to be $p + 1$ and 2 , respectively. See also [3].)



By Corollary 4.2, the conductors of L/K and L/K' are as in the diagram. We wish to find $g = f_{K'}(c')$. We know that

$$f = f_K(c) \equiv 3 \pmod{p-1} \quad (4.5)$$

by Corollary 4.6. Since $f > 2$, we have by Corollary 4.2 that $f_L(c) = 2 + p(f - 2)$.

We claim that $f > 3$. If $f = 3$, then note that by Theorem 4.17 there is an element $a \in F^2$ with $f_F(a) = 3$, which implies by Corollary 4.2 that $f_K(a) = 3$ as well. If this is so, then for some integer k we have that $f_K(ca^k) < 3$, which by Corollary 4.6 implies that $f_K(ca^k) = 1$. This means that ca^k is a p th power in K^\times (or, possibly, in the case $p = 3$ that $K(\sqrt[p]{ca^k})/K$ is unramified, in which case we change a to make ca^k a p th power). But this would imply via Kummer theory that $G_{K(\sqrt[p]{c})/F}$ is abelian. Hence we have $f > 3$, or $f \geq p + 2$.

Now we note that

$$f_L(c') = f_L(c) = 2 + p(f - 2) \geq p^2 + 2 > p^2 - p + 2 = f_{K'}(p),$$

so by Lemma 4.1 we have

$$g = p^2 - p + 2 + p^{-1}(2 + p(f - 2) - (p^2 - p + 2)) = p^2 - 2p + 1 + f.$$

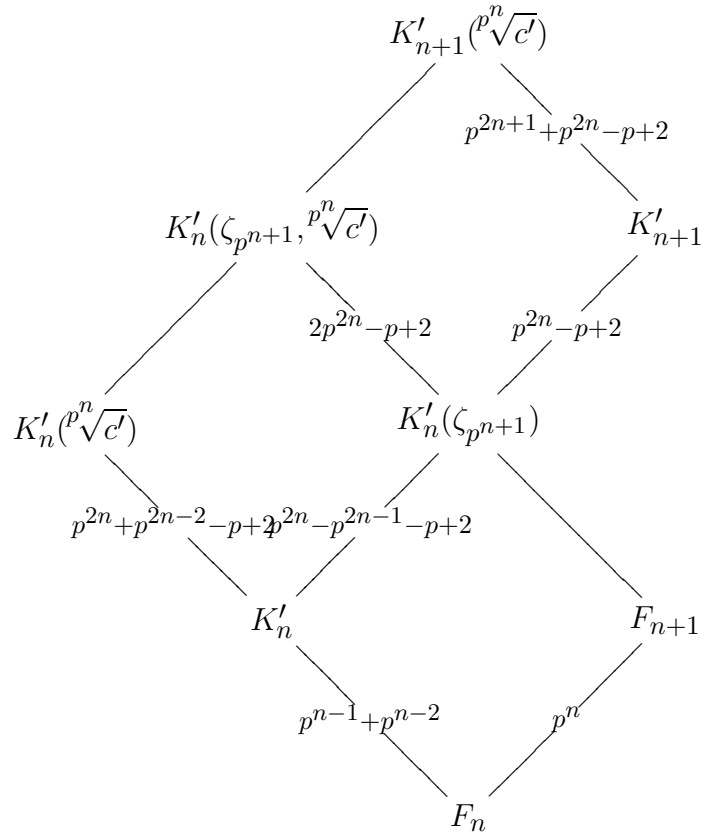
As $g \leq p^2$ and equation (4.5) holds, this forces $f = p + 2$. Hence $g = p^2 - p + 3$. \square

We can now obtain the conductors over K'_n by induction.

Proposition 4.19. *Let $n, m \geq 1$ with $n \geq m$. Then*

$$f_{m, K'_n}(c') = \begin{cases} p^{2m+1} + p^{2m} - p + 2 & \text{if } 1 \leq m < n, \\ p^{2n} + p^{2n-2} - p + 2 & \text{if } m = n. \end{cases}$$

Proof. The case $n = 1$ is proven by Proposition 4.18. By induction, let us assume we have proven the result for n . We use the following diagram of field extensions. (We indicate the conductors of some of the extensions in the diagram, which we shall determine later.)



The conductor of F_{n+1}/F_n is p^n and the conductors of the cyclic subextensions of K'_n/F_n are given in [3] as $2, p + 1, p^2 + p, \dots, p^{n-1} + p^{n-2}$. By Corollary 4.2, we

have that the conductor of $K'_n(\zeta_{p^{n+1}})/K'_n$ is equal

$$\begin{aligned} 2 + p(p-1) + p^2(p^2-1) + \cdots + p^{n-1}(p^{n-1} - p^{n-3}) + p^n(p^n - p^{n-1} - p^{n-2}) \\ = p^{2n} - p^{2n-1} - p + 2. \end{aligned}$$

By induction, we have that the conductors for $K'_n(p^n\sqrt{c'})/K'_n$ are as in the statement of the proposition. All but the largest of these is greater than $p^{2n} - p^{2n-1} - p + 2$. Therefore, by Corollary 4.2, the conductors for $K'_n(\zeta_{p^{n+1}}, p^n\sqrt{c'})/K'_n(\zeta_{p^{n+1}})$ are the same as those for $K'_n(p^n\sqrt{c'})/K'_n$ except for the largest, which is

$$p^{2n} - p^{2n-1} - p + 2 + p(p^{2n-1} + p^{2n-2}) = 2p^{2n} - p + 2.$$

To find the conductor of $K'_{n+1}/K'_n(\zeta_{p^{n+1}})$, we need only convert the upper numbering of K'_{n+1}/F_{n+1} to the lower numbering and find the largest jump in the filtration (plus one). This yields

$$2 + p(p-1) + p^2(p^2-1) + \cdots + p^n(p^n - p^{n-2}) = p^{2n} - p + 2.$$

We next apply Corollary 4.2 again to find the conductors for $K'_{n+1}(p^n\sqrt{c'})/K'_{n+1}$. Again, this changes only the final conductor, which becomes

$$p^{2n} - p + 2 + p(2p^{2n} - p + 2 - (p^{2n} - p + 2)) = p^{2n+1} + p^{2n} - p + 2.$$

Thus we have determined the conductors $f_{m, K'_{n+1}}(c')$ for $m \leq n$, and they match those in the statement of the proposition.

Finally, noting that the ramification index of K'_{n+1} is $p^{2n+1}(p-1)$ and that $p^{2n+1} + p^{2n} - p + 2 > p^{2n+1} + 1$, we conclude by Lemma 4.3 that

$$f_{n+1, K'_{n+1}}(c') = p^{2n+2} + p^{2n} - p + 2,$$

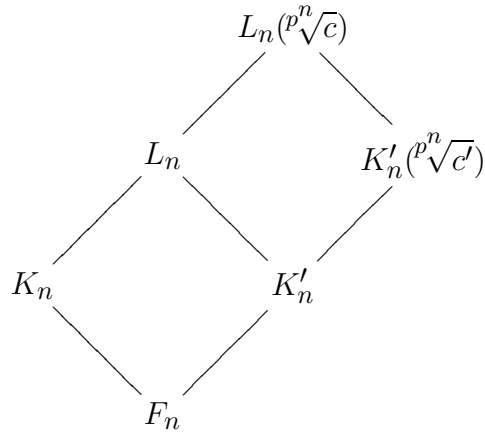
which finishes the induction. □

We now obtain the desired conductors.

Theorem 4.20. *Let $n, m \geq 1$ with $n \geq m$. Then*

$$f_{m,L_n}(c) = \begin{cases} 2p^{3m} - \frac{p^{3m} - 1}{p^2 + p + 1} + 1 & \text{if } 1 \leq m < n, \\ p^{3n-1} + p^{3n-3} - \frac{p^{3n-3} - 1}{p^2 + p + 1} + 1 & \text{if } m = n. \end{cases}$$

Proof. We have the following diagram of cyclic field extensions of degree p^n .



Again, the conductors of K'_n/F_n are $2, p+1, p^2+p, \dots, p^{n-1}+p^{n-2}$. The jumps in the lower numbering plus one are therefore given by

$$\begin{aligned}
 2 &= 2 \\
 p(p-1)+2 &= p^2-p+2 \\
 p^2(p^2-1)+p^2-p+2 &= p^4-p+2 \\
 &\vdots \\
 p^{n-1}(p^{n-1}-p^{n-3})+p^{2n-4}-p+2 &= p^{2n-2}-p+2.
 \end{aligned}$$

The conductors of K_n/F_n are shown in [3] to be $2p, 2p^2, \dots, 2p^{n-1}, p^n+p^{n-1}$, so

we have by Corollary 4.2 that the conductors of L_n/K'_n are

$$\begin{aligned} p^2(p-1) + p^2 - p + 2 &= p^3 - p + 2 \\ p^3(p^2 - p) + p^4 - p + 2 &= p^5 - p + 2 \\ &\vdots \\ p^n(p^{n-1} - p^{n-2}) + p^{2n-2} - p + 2 &= p^{2n-1} - p + 2 \\ p^n(p^n - p^{n-2}) + p^{2n-2} - p + 2 &= p^{2n} - p + 2. \end{aligned}$$

The conductors of $K'_n(p^n\sqrt{c})/K'_n$ are given by Proposition 4.19. Furthermore, we have that the jumps in the filtration of K'_n/F_n in the lower numbering (plus one) are given by

$$\begin{aligned} p^3 - p + 2 &= p^3 - p + 2 \\ p(p^5 - p^3) + p^3 - p + 2 &= p^6 - \frac{p^6 - 1}{p^2 + p + 1} + 1 \\ &\vdots \\ p^{n-2}(p^{2n-1} - p^{2n-3}) + p^{3n-6} - \frac{p^{3n-6} - 1}{p^2 + p + 1} + 1 &= p^{3n-3} - \frac{p^{3n-3} - 1}{p^2 + p + 1} + 1 \\ p^{n-1}(p^{2n} - p^{2n-1}) + p^{3n-3} - \frac{p^{3n-3} - 1}{p^2 + p + 1} + 1 &= p^{3n-1} - \frac{p^{3n} - 1}{p^2 + p + 1} + 1. \end{aligned}$$

Finally, we apply Corollary 4.2 to obtain the conductors of $L_n(p^n\sqrt{c})/L_n$. We obtain the following, as desired:

$$\begin{aligned} p(p^2) + p^3 - p + 2 &= 2p^3 - p + 2 \\ p^2(p^4) + p^6 - \frac{p^6 - 1}{p^2 + p + 1} + 1 &= 2p^6 - \frac{p^6 - 1}{p^2 + p + 1} + 1 \\ &\vdots \\ p^{n-1}(p^{2n-2}) + p^{3n-3} - \frac{p^{3n-3} - 1}{p^2 + p + 1} + 1 &= 2p^{3n-3} - \frac{p^{3n-3} - 1}{p^2 + p + 1} + 1 \\ p^n(p^{2n-2}) + p^{3n-1} - \frac{p^{3n} - 1}{p^2 + p + 1} + 1 &= p^{3n-1} + p^{3n-3} - \frac{p^{3n-3} - 1}{p^2 + p + 1} + 1. \end{aligned}$$

□

Remark. From the conductors of the various subextensions of $L(p^n\sqrt{c})/\mathbf{Q}_p$, one can di-

rectly compute the discriminant of entire extension. This could lead to a computation of the discriminant for the corresponding extension of \mathbf{Q} . With slightly more work, one can compute the ramification groups of the entire extension over \mathbf{Q}_p . This would provide an interesting example of the ramification groups of a three-step solvable extension: in particular, one could learn something about the jumps in the filtration in the upper numbering of such an extension.

REFERENCES

- [1] Brauer, Richard, “Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind,” *J. Reine Angew. Math.* **168** (1932), no. 1, 44–64.
- [2] Brattström, Gudrun, “On p -groups as Galois groups,” *Math. Scand.* **65** (1989), 165–174.
- [3] Coleman, R. F., McCallum, W., “Stable reduction of Fermat curves and Jacobi sum Hecke characters,” *J. Reine Angew. Math.* **385** (1988), 41–101.
- [4] Damey, P., Martinet, J., “Plongement d’une extension quadratique dans une extension quaternionienne,” *J. Reine Angew. Math.* **262/263** (1973), 323–338.
- [5] Damey, P., Payan, J.-J., “Existence et construction des extensions Galoisennes et non-abéliennes de degré 8 d’un corps de caractéristique différente de 2,” *J. Reine Angew. Math.* **244** (1970), 37–54.
- [6] Dedekind, Richard, “Konstruktion von Quaternionkörpern, Gesammelte mathematische Werke,” Band 2 (1931), Viewig, Braunschweig, 376–384.
- [7] Gillard, Roland, “Plongement d’une extension d’ordre p ou p^2 dans une surextension non abélienne d’ordre p^3 ,” *J. Reine Angew. Math.* **268/269** (1974), 418–426.
- [8] Greither, Cornelius, “On Chinburg’s second conjecture for abelian fields,” *J. Reine Angew. Math.* **479** (1996), 1–37.
- [9] Gross, Benedict, “Modular Forms (mod p) and Galois representations,” *Internat. Math. Res. Notices* **16** (1998), 865–875.
- [10] Gross, Benedict, “Algebraic Modular Forms,” *Israel J. Math.*, to appear.
- [11] Ishkhanov, V. V., Lur’e, B. B., Faddeev, D. D., “The Embedding Problem in Galois Theory,” *Translations of Mathematical Monographs* **165**, Amer. Math. Soc., 1997.
- [12] Koch, Helmut, “Algebraic Number Theory,” Springer-Verlag, 1997.
- [13] Lang, Serge, “Cyclotomic Fields I and II (Combined Second Edition),” Springer-Verlag, 1990.
- [14] Serre, Jean-Pierre, “Galois Cohomology,” Springer-Verlag, 1997.

- [15] Serre, Jean-Pierre, “Local Fields,” Springer-Verlag, 1979.
- [16] Serre, Jean-Pierre, “Sur les représentations modulaires de degré 2 de $\text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$,” *Duke Math. J.* **54**, no. 1 (1987), 179–230.
- [17] Massy, Richard, “Construction de p -extensions galoisennes d’un corps de caractéristique différente de p ,” *J. Algebra* **109** (1987), 508–535.
- [18] Massy, Richard, “Formules de construction de p -extensions galoisennes,” *C.R. Acad. Sc. Paris Sér. I Math.* **303** (1986), no. 13, 591–595.
- [19] Massy, R., Nguyen-Quang-Do, T., “Plongement d’une extension de degré p^2 dans une surextension non abélienne de degré p^3 : étude locale-globale,” *J. Reine Angew. Math.* **291** (1977), 149–161.
- [20] Sharifi, Romyar, “On Norm Residue Symbols and Conductors,” submitted for publication. UIUC Algebraic Number Theory Preprint Archives, no. 149.
- [21] Swallow, John R., “Central p -extensions of Galois Groups,” *J. Algebra* **186** (1996), 277–298.
- [22] Warfield, Robert B., Jr., “Nilpotent Groups,” Lecture Notes in Mathematics 513, Springer-Verlag, 1976.
- [23] Witt, Ernst, “Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f ,” *J. Reine Angew. Math.* **174** (1936), 237–45.