Classifying Extensions of Local Fields

Maxwell Ye

Summer 2022

Abstract

Given an extension L/K of local fields, an extension of $L^\times$ by the Galois group $\mathrm{Gal}(L/K)$ can be concretely described up to equivalence using cohomological techniques. We extend this further using data from the fields in such a way that explicit computations can be made in specific cases.

Contents

1 Introduction

In number theory, particularly local class field theory, the Kronecker-Weber theorem gives a partial characterization of abelian extensions of the local field $\mathbb{Q}_p$.

THEOREM 1. (KRONECKER-WEBER). Let K be a finite abelian extension of $\mathbb{Q}_p$. Then K is contained in some cyclotomic extension of $\mathbb{Q}_p$.

Moreover, given an abelian extension L/K of local fields with Galois group $G = \mathrm{Gal}(L/K)$, we may construct a short exact sequence of the form

$$1 \longrightarrow L^\times \longrightarrow \mathcal{E} \xrightarrow{\pi} G \longrightarrow 1 \ ,$$

called a *group extension* of $L^\times$ by G. We will demonstrate a connection between these extensions, the cohomology group $H^2(L/K)$, and definable parameters in $L^\times$.

2 Preliminaries

We first present some expository material from other sources that will be helpful in our study.

2.1 Local Fields

Let $|\cdot|$ be a discrete valuation on a field K.

DEFINITION 1. A field K is a (non-Archimedean) *local field* if it is complete with respect to a valuation $|\cdot|$ and its residue field is finite.

EXAMPLE 1. Let $|\cdot|_p$ denote the p-adic absolute value on $\mathbb{Q}$. The completion of $\mathbb{Q}$ with respect to $|\cdot|_p$ generates the p-adic numbers $\mathbb{Q}_p$, a local field.

The topology of a local field K is generated by balls of the form

$$B_n = \{a \in K \mid |a| \leq n\}$$

for positive real n, such that the collection $\{b + B_n\}$ with $b \in K$ forms a basis.

Definition 2. Under the given topology, for a local field K, we may define the following:

- the set $\mathcal{O}_K = \{a \in K \mid |a| \leq 1\}$ is the *ring of integers* of K.
- the set $\mathcal{O}_K^\times = \{a \in K \mid |a| = 1\}$ are the units of $\mathcal{O}_K$.
- there exists a unique prime ideal $\mathfrak{m} = \{a \in K \mid |a| < 1\}$ of $\mathcal{O}_K$.
- a generator π of $\mathfrak{m}$ is called a *uniformizer* of K.
- the residue field k of K is given by $\mathcal{O}/\mathfrak{m}$.

Using the properties of the non-Archimedean absolute value, it is easy to see that the sets defined do in fact have the correct algebraic structure.

Example 2. For $K = \mathbb{Q}_p$, we have the ring of integers $\mathcal{O}_K = \mathbb{Z}_p$ and uniformizer $\pi = p$.

Using these definitions, there exists a description of the multiplicative group $K^\times$ of a local field K.

Proposition 1. ([NeuANT], Proposition II.5.3). Let K be a local field with uniformizer π_K, prime ideal $\mathfrak{m}$, and residue field $k = \mathbb{F}_q$. Then

$$K^\times \cong \langle \pi_K \rangle \times \mu_{q-1} \times (1 + \mathfrak{m}),$$

where μ_{q-1} is the cyclotomic group of $q - 1$ elements.

In fact, there exists a full classification of local fields.

Theorem 2. ([MilANT], Remark 7.49). Every local field K is isomorphic to one of the following:

(a) an extension of $\mathbb{Q}_p$ for some prime p,

(b) an extension of $\mathbb{F}_q((t))$ for some finite field $\mathbb{F}_q$,

(c) $\mathbb{R}$ or $\mathbb{C}$.

For the purposes of this paper, we will be primarily interested in extensions of $\mathbb{Q}_p$, which are non-Archimedean and have characteristic zero.

Given an extension of local fields L/K, we are able to "translate" valuations of L into valuations of K using the norm map.

Proposition 2. ([SerLF], Corollary II.2.4). Let L/K be an extension of local fields with degree n. Then for all $x \in L$,

$$|x|_L = |\operatorname{Nm}_{L/K}(x)|_K^{1/n}.$$

Moreover, this extension of the absolute values is unique.

Remark 1. If $x \in K \subseteq L$, then $\operatorname{Nm}_{L/K}(x) = x^n$, and so $|x|_L = |x|_K$.

Finally, given an extension L/K, we are able to describe the extension in terms of its ramification index. Given an extension of (arbitrary) fields L/K with degree n, we are able to write

$$n = \sum_{i=0}^{r} e_i f_i$$

for each prime ideal of $\mathcal{O}_L$, where e_i is the ramification index and f is the degree of the extension ℓ/k of residue fields. When L/K is an extension of local fields, there is precisely one prime ideal, so we obtain that $n = ef$.

Definition 3. Let L/K be an extension of local fields with degree $n = ef$.

- if $e = 1$ and $f = n$, then L is said to be *unramified* over K,
- if $e = n$ and $f = 1$, then L is said to be *totally ramified* over K.

Example 3. Let p be prime, and n a positive integer.

- if $p \nmid n$, then the cyclotomic extension $\mathbb{Q}_p(\zeta_n)$ is unramified,
- if $n = p^k$ for some k, then the extension $\mathbb{Q}_p(\zeta_n)$ is totally ramified.

2.2 Group Cohomology

We begin with a definition.

Definition 4. Let G be a group. A *G-module* is a $\mathbb{Z}[G]$-module.

Throughout this paper, we will be primarily interested in working in the G-module $L^\times$, where G is the Galois group of a field extension L/K.

If we fix a group G and a G-module A, then we can define cohomology groups as follows:

Definition 5. Let G be a group. For $q \geq 0$, there exists functors $H^q(G,-) : G\text{-Mod} \to \text{AbGrp}$ with the following properties:

(a) $H^0(G,-) = (-)^G$.

(b) there exist connecting homomorphisms $\delta : H^q(G,C) \to H^{q+1}(G,A)$ such that a short exact sequence $0 \to A \to B \to C \to 0$ induces a long exact sequence

$$\cdots \to H^q(G,A) \to H^q(G,B) \to H^q(G,C) \to H^{q+1}(G,A) \to \cdots,$$

(c) $H^q(G,A) = 0$ for all $q \geq 1$ if A is co-induced.

For a G-module A, the group $H^q(G,A)$ is called the q-th cohomology group of A.

The definition above uniquely determines [AtWaGC Theorem 1] the cohomology groups.

Our primary interest for this paper will be on $H^2(G,A)$. For notational purposes, when given a Galois extension L/K with Galois group G, we will denote

$$H^2(L/K) = H^2(G,L^\times).$$

We may also explicitly construct the cohomology groups as follows: fix a group G, and consider the groups $C^q(G,A) : \text{Hom}_G(\mathbb{Z}[G^{q+1}],A)$. Define $d^{q+1} : C^q(G,A) \to C^{q+1}(G,A)$ as

$$(d^{q+1}\varphi)(g_1,...,g_{q+1}) = g_1\varphi(g_2,...,g_{q+1}) + \sum_{i=0}^{q}(-1)^j(g_0,...,g_{j-1},g_jg_{j+1},...,g_{q+1}) + (-1)^{q+1}\varphi(g_1,...,g_q).$$

The G-module homomorphisms $\phi \in C^q(G,A)$ are called q-cochains. Moreover, we can define

$$Z^q(G,A) = \ker d^{q+1}$$
$$B^q(G,A) = \operatorname{im} d^q$$

called q-cocycles and q-coboundaries, respectively, such that

$$H^q(G,A) = Z^q(G,A)/B^q(G,A)$$

for all $q \geq 0$.

Because we are primarily interested in $H^2(G,A)$ later, it will be helpful to write down the 2-cocycle condition for a 2-cochain.

Corollary 1. Let φ be a 2-cochain. If, for all $g_1,g_2,g_3 \in G$, we have

$$g_1\varphi(g_2,g_3) - \varphi(g_1g_2,g_3) + \varphi(g_1,g_2g_3) - \varphi(g_1,g_2) = 0,$$

then φ is a 2-cocycle in $Z^2(G,A)$.

Proof. Let $q = 2$ in the above construction and set $d^3\varphi = 0$. $\square$

2.3 Local Class Field Theory

We briefly present two isomorphisms from local class field theory:

Theorem 3. Let L/K be an abelian extension of local fields with degree n and Galois group $G = \mathrm{Gal}(L/K)$. There exists an isomorphism

$$\theta^{-1} : K^\times / \mathrm{Nm}(L^\times) \to G,$$

called the *local Artin reciprocity map*.

Theorem 4. Let L/K be a Galois extension of local fields with degree n. There exists an isomorphism

$$\mathrm{inv} : H^2(L/K) \to \frac{1}{n}\mathbb{Z}/\mathbb{Z},$$

called the *invariant map*.

The class $u_{L/K} \in H^2(L/K)$ such that $\mathrm{inv}\, u_{L/K} = \frac{1}{n}$ is called the *local fundamental class*.

2.4 Extensions

We begin with a definition.

Definition 6. Let G be a group, and let A be a G-module. A *group extension* is a short exact sequence

$$1 \longrightarrow A \longrightarrow \mathcal{E} \xrightarrow{\pi} G \longrightarrow 1$$

such that for all $a \in A$ and $w \in \mathcal{E}$,

$$waw^{-1} = \pi(w) \cdot a.$$

Throughout this paper, we will be interested in group extensions of the multiplicative group $L^\times$ of a field extension L/K by its Galois group $\mathrm{Gal}(L/K)$.

Two extensions are *equivalent* if they are exact as short exact sequences. Moreover, we are able to identify equivalence classes of extensions using cohomology.

Theorem 5. ([ConCE]). Let G be a group and A a G-module. Equivalence classes of extensions of A by G are in bijective correspondence with equivalence classes in $H^2(G, A)$.

The structure of $\mathcal{E}$ can be described more explicitly. By choosing a set-theoretic section $s : G \to \mathcal{E}$ that sends an element of G to a coset representative in $\mathcal{E}$, we may identify $\mathcal{E}$ as a set

$$\mathcal{E} = A \times G.$$

Because our conjugation condition in the definition of an extension has been specified in advance, we obtain that for $g, h \in G$, $s(g)s(h) \in \pi^{-1}(gh)$, and so there exists some unique $c_{g,h} \in A$ such that

$$s(g)s(h) = c_{g,h}s(gh).$$

By obtaining $c_{g,h}$ across all possible g, h, we obtain a function $c : G \times G \to A$.

PROPOSITION 3. ([ConGE]). The function $c : G \times G \to A$ defined above is a 2-cocycle.

Given this cocycle, we are able to describe the group structure of $\mathcal{E}$.

PROPOSITION 4. ([ConGE]) Let $1 \to A \to \mathcal{E} \to G \to 1$ be a group extension with an associated cocycle c. Then the composition law on $\mathcal{E} = A \times G$ can be written as

$$(x, g) * (x', g') = (x + gx' + c(g, g'), gg').$$

3 Development of Theory

Given an extension of local fields L/K, we are interested in classifying all Galois gerbes up to equivalence. Let $G = \mathrm{Gal}(L/K)$, and consider the gerbe

$$1 \longrightarrow L^\times \longrightarrow \mathcal{E} \xrightarrow{\pi} G \longrightarrow 1 \ .$$

We begin by describing lifts of elements of G.

LEMMA 1. Suppose that $\sigma \in G$ has order n, and let f be a lift of σ in $\mathcal{E}$. Then $f^n \in L^\times$.

PROOF. We have that

$$\begin{aligned}\pi(f^n) &= \pi(f)^n \\ &= \sigma^n \\ &= 1.\end{aligned}$$

Thus, $f^n \in \ker \pi = L^\times$. □

In fact, given our setup, we have the following stronger condition.

LEMMA 2. The element f^n lies in the fixed field $L^{\langle\sigma\rangle}$.

PROOF. We have from earlier that $f^n \in L^\times$. Thus,

$$\begin{aligned}\sigma(f^n) &= f \cdot f^n \cdot f^{-1} \\ &= f^n,\end{aligned}$$

and so $f^n \in L^{\langle\sigma\rangle}$. □

This will be extremely useful later, so it will help to introduce some notation.

Definition 7. Let $f \in \mathcal{E}$ be a lift of $\sigma \in G$. Define $\alpha = f^n$.

Where appropriate, we will subscript α to represent lifts of different generators of G.

3.1 Cyclic Extensions

When L/K is a cyclic extension generated by σ, it is the case that $L^\times = L^{\langle\sigma\rangle}$. Thus, if we have a lift f, then we are able to specify the group law of $\mathcal{E}$.

Definition 8. Let L/K be cyclic with $G = \langle\sigma\rangle$ of order n. Then the extension

$$1 \longrightarrow L^\times \longrightarrow \mathcal{E} \xrightarrow{\pi} G \longrightarrow 1$$

is characterized as follows:

- $\pi(f) = \sigma$
- $\mathcal{E}$ is generated by f and $L^\times$,
- for all $a \in L^\times$, $faf^{-1} = \sigma(a)$,
- $\alpha = f^n \in L^\times$.

Moreover, we may identify α with a 2-cocycle in $H^2(L/K)$ as follows:

Proposition 5. Let $G = \mathrm{Gal}(L/K)$ be generated by σ and have order n. The 2-cochain defined by

$$c(\sigma^i, \sigma^j) = \begin{cases} 1 & i+j < n \\ \alpha & i+j \geq n \end{cases}$$

is a 2-cocycle.

Proof. TBD $\square$

Given an extension characterized by α, we are interested in classifying it up to equivalence. This is dependent on our choice of lift. Given a cocycle c, If we take an arbitrary lift $f = (x, \sigma) \in \mathcal{E} \cong L^\times \times G$ of σ, we obtain that

$$\alpha = \mathrm{Nm}(x) \cdot \prod_{i=0}^{n-1} c(\sigma^i, \sigma),$$

where $\mathrm{Nm} : L^\times \to K$ is the norm map.

Noting this setup, we define an equivalence relation for α as follows:

DEFINITION 9. Elements α and α' are equivalent if there exists $x \in L^\times$ such that

$$\alpha = \mathrm{Nm}(x) \cdot \alpha'.$$

Because $\mathrm{Nm}(xy) = \mathrm{Nm}(x) \cdot \mathrm{Nm}(y)$, the equivalence relation is in fact well defined.

In fact, using our formula for the cocycle c corresponding to α, we are able to prescribe a structure on our equivalence classes of $[\alpha]$.

THEOREM 6. Let the equivalence classes $[\alpha]$ and $[\alpha']$ correspond to $[c], [c'] \in H^2(L/K)$, respectively. Then the correspondence of $[\alpha\alpha']$ to the class of cocycles equivalent to

$$(cc')(\sigma^i, \sigma^j) = \begin{cases} 1 & i+j < n \\ \alpha\alpha' & i+j \geq n \end{cases}$$

endows a group structure on the classes of α.

PROOF. Because α lies in the multiplicative group $L^\times$, we only need to note that

$$(cc')(\sigma^i, \sigma^j) = 1$$

is the identity element of $H^2(L/K)$. □

3.2 Bicyclic Extensions

We now turn to a more general case of when L/K is a bicyclic extension. In this case, we have that $G = G_1 \times G_2$, where G_1 and G_2 are cyclic. Let σ_1 and σ_2 be respective generators, with respective orders n_1 and n_2. In the cyclic case, the quantity α was sufficient to encode the necessary information about the extension $\mathcal{E}$. However, we now need to track how two lifts f_1, f_2 of σ_1, σ_2 commute with each other. To do this, we will introduce a new quantity.

DEFINITION 10. For $i = 1, 2$, let $f_i \in \mathcal{E}$ be a lift of $\sigma_i \in G$. Define $\beta = f_1 f_2 f_1^{-1} f_2^{-1}$ to be the commutator of f_1 and f_2 in $\mathcal{E}$.

Furthermore, we will introduce some norm maps on $L^\times$ as follows:

DEFINITION 11. For a given index i, denote the map $N_i : L^\times \to L^{\langle \sigma_i \rangle}$ as

$$N_i(x) = \prod_{\ell=0}^{n_i - 1} \sigma_i^\ell(x)$$

We immediately note some properties of β.

PROPOSITION 6. The element β satisfies the following properties:

- $\beta \in L^\times$,
- $N_1(\beta) = \alpha_1/\sigma_2(\alpha_1)$,
- $N_2(\beta^{-1}) = \alpha_2/\sigma_1(\alpha_2)$.

PROOF. Let β be as defined. We have that

$$\begin{aligned}\pi(\beta) &= \pi(f_1 f_2 f_1^{-1} f_2^{-1}) \\ &= \pi(f_1)\cdot\pi(f_2)\cdot\pi(f_1^{-1})\cdot\pi(f_2^{-1}) \\ &= \sigma_1\cdot\sigma_2\cdot\sigma_1^{-1}\cdot\sigma_2^{-1} \\ &= 1,\end{aligned}$$

and so $\beta \in \ker\pi = L^\times$.

To prove the second claim, we proceed by induction. If $n_1 = 2$, then

$$\begin{aligned}N_1(\beta) &= \beta\cdot\sigma_1(\beta) \\ &= f_1 f_2 f_1^{-1} f_2^{-1}\cdot(f_1\cdot f_1 f_2 f_1^{-1} f_2^{-1}\cdot f_1^{-1}) \\ &= f_1 f_2 f_1^{-1} f_2^{-1} f_1^2 f_2 f_1^{-1} f_2^{-1} f_1^{-1} \\ &= f_1 f_2 f_1^{-1}\sigma_2^{-1}(\alpha_1) f_1^{-1} f_2^{-1} f_1^{-1} \\ &= f_1 f_2\ \sigma_1^{-1}\sigma_2^{-1}(\alpha_1) f_1^{-2} f_2^{-1} f_1^{-1} \\ &= f_1 f_2\ \sigma_1^{-1}\sigma_2^{-1}(\alpha_1)\ \alpha_1^{-1} f_2^{-1} f_1^{-1} \\ &= \sigma_1\sigma_2(\sigma_1^{-1}\sigma_2^{-1}(\alpha_1)\ \alpha_1^{-1}) \\ &= \alpha_1/\sigma_1\sigma_2(\alpha_1) \\ &= \alpha_1/\sigma_2(\alpha_1),\end{aligned}$$

where we use the fact that α_1 is fixed by σ_1. Suppose the relation holds for $n = k$. Using some liberties with notation, we will use f_1^k and $f_2 f_1^k f_2^{-1}$ to indicate the result for $n = k$. Then for $n = k+1$,

$$\begin{aligned}N_1(\beta) &= \left(\prod_{i=0}^{k-1}\sigma_1^i(\beta)\right)\cdot\sigma^k(\beta) \\ &= f_1^k f_2 f_1^{-k} f_2^{-1}\cdot(f_1^k\cdot f_1 f_2 f_1^{-1} f_2^{-1}\cdot f_1^{-k}) \\ &= f_1^k f_2 f_1^{-k} f_2^{-1}\alpha_1 f_2 f_1^{-1} f_2^{-1} f_1^{-k} \\ &= f_1^k f_2 f_1^{-k}\ \sigma_2^{-1}(\alpha_1)\ f_1^{-1} f_2^{-1} f_1^{-k} \\ &= f_1^k f_2 f_1^{-k-1}\ \sigma_2^{-1}(\alpha_1)\ f_2^{-1} f_1^{-k} \\ &= f_1^k f_2\ \alpha_1^{-1}\ \sigma_2^{-1}(\alpha_1)\ f_2^{-1} f_1^{-k} \\ &= f_1^k\ \sigma_2(\alpha_1^{-1})\ \alpha_1\ f_1^{-k} \\ &= \alpha_1/\sigma_2(\alpha_1)\end{aligned}$$

Thus, the second claim holds. To obtain the last claim, we simply note that $\beta^{-1} = f_2 f_1 f_2^{-1} f_1^{-1}$, such that the previous argument holds by symmetry. $\square$

REMARK 2. In the proof above, the element f_1^k (and indeed, all lower orders) may not necessarily be an element of $L^\times$ on which σ_2 may act. However, we may ignore this specification by working purely with f_1 and f_2, defining the "action" of σ_2 to work by its defined conjugation.

COROLLARY 2. Let β be as given. Then $\mathrm{Nm}(\beta) = 1$.

PROOF. We observe that

$$\begin{aligned}\mathrm{Nm}(\beta) &= N_2 N_1(\beta) \\ &= N_2(\alpha_1 \cdot \sigma_2(\alpha_1^{-1})) \\ &= N_2(\alpha_1) \cdot N_2(\sigma_2(\alpha_1^{-1})) \\ &= N_2(\alpha_1) \cdot N_2(\alpha_1^{-1}) \\ &= 1.\end{aligned}$$

Thus, the result follows. $\square$

As done previously in the cyclic case, we now describe the group law on $\mathcal{E}$.

DEFINITION 12. Let L/K be bicyclic with $G = \langle\sigma_1\rangle \times \langle\sigma_2\rangle$, where σ_1 and σ_2 have orders n_1 and n_2, respectively. Then the extension

$$1 \longrightarrow L^\times \longrightarrow \mathcal{E} \xrightarrow{\pi} G \longrightarrow 1$$

is characterized as follows: there exist lifts $f_1, f_2 \in \mathcal{E}$ such that

- for $i = 1, 2$, $\pi(f_i) = \sigma_i$
- $\mathcal{E}$ is generated by f_i and $L^\times$,
- for all $a \in L^\times$, $f_i a f_i^{-1} = \sigma_i(a)$,
- $\alpha_i = f_i^{n_i} \in L^{\langle\sigma_i\rangle}$,
- $N_1(\beta) = \alpha_1/\sigma_2(\alpha_1)$,
- $N_2(\beta^{-1}) = \alpha_2/\sigma_1(\alpha_2)$.

Because the information given by the α's and β is useful, we will henceforth, when given a bicyclic extension, refer to the element $(\alpha_1, \alpha_2, \beta)$ as a "triple".

We continue to be able to associate cocycles in $H^2(L/K)$ to extensions via triples. Because we have introduced the element β, our cocycle formula becomes slightly more complex.

Proposition 7. Let $G = \mathrm{Gal}(L/K)$ be generated by σ_1, σ_2 with respective orders n_1, n_2. The 2-cochain defined by

$$c(\sigma_1^{r_1}\sigma_2^{r_2}, \sigma_1^{s_1}\sigma_2^{s_2}) = \left(\sigma_1^{r_1} \prod_{k=0}^{r_2-1} \prod_{\ell=0}^{s_1-1} \sigma_1^k \sigma_2^\ell (\beta^{-1})\right) \left(\alpha_1^{\chi_1} \cdot \sigma_1^{r_1+s_1}(\alpha_2^{\chi_2})\right)$$

where χ_i is an indicator function given by

$$\chi_i = \begin{cases} 0 & r_i + s_i < n \\ 1 & r_i + s_i \geq n \end{cases}$$

Proof. TBD. □

Remark 3. If $r_2 = s_2 = 0$, the formula reduces to exactly that of the cyclic case.

As with before, we are interested in classifying triples to equivalence. Fix a cocycle c, and suppose we have lifts $f_1 = (x_1, \sigma_1)$ and $f_2 = (x_2, \sigma_2)$. From our remark above, the formula for α_i is the same as discussed in the cyclic case. Moreover, our β may be written as

$$\beta = \frac{x_1}{x_2} \cdot \frac{\sigma_1(x_2)}{\sigma_2(x_1)} \cdot \frac{c(\sigma_1, \sigma_2)}{c(\sigma_2, \sigma_1)}$$

Thus, we have equivalence as follows.

Definition 13. Triples $(\alpha_1, \alpha_2, \beta)$ and $(\alpha_1', \alpha_2', \beta')$ are equivalent if there exists $x_1, x_2 \in L^\times$ such that

$$\alpha_i = N_i(x_i) \cdot \alpha_i',$$
$$\beta = \frac{x_1}{x_2} \cdot \frac{\sigma_1(x_2)}{\sigma_2(x_1)} \cdot \beta'.$$

3.3 Some Remarks on Abelian Extensions

Much of the commentary on cyclic and bicyclic extensions extends to a finite abelian extension L/K. Suppose that $G = \mathrm{Gal}(L/K) = G_1 \times \cdots \times G_r$ is a decomposition into cyclic groups generated by $\sigma_1, ..., \sigma_r$. In the bicyclic case, we represented the commutator between lifts of σ_1, σ_2 using β; to extend this, we will introduce a β term for each pair of indices analogously:

$$\beta_{ij} = f_i f_j f_i^{-1} f_j^{-1}.$$

We then have the following relation.

Proposition 8. Suppose $i < j < k$. Then

$$\frac{\beta_{ik}}{\sigma_j(\beta_{ik})} = \frac{\beta_{ij}}{\sigma_k(\beta_{ij})} \cdot \frac{\beta_{jk}}{\sigma_i(\beta_{jk})}$$

Proof. We will prove the equivalent statement that

$$\sigma_i(\beta_{jk})\,\beta_{ik}\,\sigma_k(\beta_{ij}) = \beta_{ij}\,\sigma_j(\beta_{ik})\,\beta_{jk}.$$

By computation,

$$\begin{aligned}\sigma_i(\beta_{jk})\,\beta_{ik}\,\sigma_k(\beta_{jk}) &= (f_i f_j f_k f_j^{-1} f_k^{-1} f_i^{-1})(f_i f_k f_i^{-1} f_k^{-1})(f_k f_i f_j f_i^{-1} f_j^{-1} f_k^{-1}) \\ &= f_i f_j f_k f_i^{-1} f_j^{-1} f_k^{-1} \\ &= f_i f_j (f_i^{-1} f_j^{-1} f_j f_i) f_k f_i^{-1} (f_k^{-1} f_j^{-1} f_j f_k) f_j^{-1} f_k^{-1} \\ &= \beta_{ij}\,\sigma_j(\beta_{ik})\,\beta_{jk}.\end{aligned}$$

Thus, the relation holds. □

By taking a set-theoretic lift as described in [ConGE], we may explicitly construct a cocycle in terms of (α_i, β_{ij}) and the generators σ_i of G. However, because it is not relevant to the remainder of the paper, we have elected not to do so.

4 Extensions of $\mathbb{Q}_p$

Let p be an odd prime. To demonstrate our theory, consider a cyclotomic extension $\mathbb{Q}_p(\zeta_n)$, and write $n = p^k m$, where $p \nmid m$. We obtain a diagram of fields

$$\begin{tikzcd} & \mathbb{Q}_p(\zeta_n) \arrow[dl, dash] \arrow[dr, dash] & \\ \mathbb{Q}_p(\zeta_{p^k}) \arrow[dr, dash] & & \mathbb{Q}_p(\zeta_m) \arrow[dl, dash] \\ & \mathbb{Q}_p & \end{tikzcd}$$

where $\mathbb{Q}_p(\zeta_{p^k}) \cap \mathbb{Q}_p(\zeta_m) = \mathbb{Q}_p$. We have that both of these subfields are cyclic extensions, so we may write

$$\mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p) \cong \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p(\zeta_{p^k})) \times \mathrm{Gal}(\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p(\zeta_m))$$

such that our bicyclic theory may be applied.

We now present an explicit example. Let $K = \mathbb{Q}_p(\zeta_m)$ be an unramified extension of $\mathbb{Q}_p$. The Galois group $\mathrm{Gal}(K/\mathbb{Q}_p)$ is generated by a Frobenius element σ. Moreover, it is known ([MilCFT, Section III.1) that the local fundamental class $u_{K/\mathbb{Q}_p} \in H^2(K/\mathbb{Q}_p)$ is given by

$$u_{K/\mathbb{Q}_p}(\sigma^i, \sigma^j) = \begin{cases} 1 & i + j < n \\ \pi_K & i + j \geq n \end{cases}$$

Thus, in the case, if we identify α with π_K, our classification is as follows:

Theorem 7. Let $K/\mathbb{Q}_p$ be an unramified extension of $\mathbb{Q}_p$ with uniformizer π_K. Then, up to equivalence, all extensions of $K^\times$ by $\mathrm{Gal}(K/\mathbb{Q}_p)$ are classified by powers of π_K.

Proof. Identifying α with π_K, we have that the cocycle that corresponds to α is the local fundamental class. Because $\mathrm{inv}\, u_{K/\mathbb{Q}_p} = \frac{1}{n}$, we from the structure on α that the cocycle corresponding to π_K^m maps to $\frac{m}{n}$ under the invariant map for all $m < n$. □

5 Extensions of $\mathbb{Q}_2$

We now consider the special case of $p = 2$. We observed that when p is an odd prime, a cyclotomic extension of $\mathbb{Q}_p$ is bicyclic. However, in the case of $\mathbb{Q}_2$, our diagram of fields splits as

$$\begin{tikzcd}
 & & \mathbb{Q}_2(\zeta_n) \arrow[dl, dash] \arrow[ddr, dash] & \\
 & \mathbb{Q}_2(\zeta_{2^k}) \arrow[dl, dash] \arrow[d, dash] & & \\
\mathbb{Q}_2(i) \arrow[dr, dash] & \mathbb{Q}_2(\zeta_{2^k} + \zeta_{2^k}^{-1}) \arrow[d, dash] & & \mathbb{Q}_2(\zeta_m) \arrow[dll, dash] \\
 & \mathbb{Q}_2 & &
\end{tikzcd}$$

where the extension $\mathbb{Q}_2(\zeta_{2^k})/\mathbb{Q}_2$ is bicyclic over $\mathbb{Q}_2$.

As with $\mathbb{Q}_p$, we now present an explicit example. Consider the specific case of $K = \mathbb{Q}_2(\zeta_8) = \mathbb{Q}_2(i, \sqrt{2})$, with the following diagram of fields:

$$\begin{tikzcd}
 & \mathbb{Q}_2(\zeta_8) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}_2(i) \arrow[dr, dash] & & \mathbb{Q}_2(\sqrt{2}) \arrow[dl, dash] \\
 & \mathbb{Q}_2 &
\end{tikzcd}$$

This bicyclic extension is totally ramified and of degree 4. We seek to fully classify its equivalence classes of triples as described in Section 3.

In this case, the Galois group $\mathrm{Gal}(K/\mathbb{Q}_2)$ is generated by the automorphisms

$$\sigma_1 : \sqrt{2} \mapsto -\sqrt{2}$$
$$\sigma_2 : i \mapsto -i$$

such that $K_1 = \mathbb{Q}_2(i)$ and $K_2 = \mathbb{Q}_2(\sqrt{2})$. As observed earlier, a triple $(\alpha_1, \alpha_2, \beta)$ that has order 4 cannot have $\alpha_i = N_i(x)$ for an element $x \in K^\times$. Thus, it is useful to explicitly compute the norm groups of the subfields of this extension.

To compute the norm groups, we will make use of the following result:

Lemma 3. Let L/K be an abelian extension of local fields with degree n. Then the norm group $\mathrm{Nm}(L^\times)$ is of index n in $K^\times$.

Proof. Denote $G = \mathrm{Gal}(L/K)$. Because L/K is Galois, $|G| = n$. The local Artin map gives an isomorphism

$$K^\times / \mathrm{Nm}(L^\times) \cong G^{\mathrm{ab}},$$

where G^{ab} is the maximal abelian quotient of G. Because G is abelian, $\mathrm{Nm}(L^\times)$ has index n. $\square$

Because $K^\times$ is infinite and may be particularly complicated, we will first track through the n-th powers of $K^\times$. Since $K^\times$ is fixed by $\mathrm{Gal}(L/K)$, we have that for $x \in K^\times$, $\mathrm{Nm}(x) = x^n$, and so the n-th powers $(K^\times)^n$ form a subgroup of $\mathrm{Nm}(L^\times)$.

Observe that $[\mathbb{Q}_2(\zeta_8) : \mathbb{Q}_2(i)] = [\mathbb{Q}_2(\zeta_8) : \mathbb{Q}_2(\sqrt{2})] = 2$. Because K is an abelian extension, the norm groups $N_1(K^\times)$ and $N_2(K^\times)$ have index 2 over their respective fields. Thus, $N_i(K^\times)$ induces an order 2 subgroup of $K_i^\times/(K_i^\times)^2$. We'll consider each subfield separately.

Consider $K_1 = \mathbb{Q}_2(i)$. Observe that K_1 has uniformizer $\pi_{K_1} = i - 1$, so the unit group of K_1 has the structure

$$\begin{aligned} K_1^\times &\cong \langle \pi_{K_1} \rangle \times (1 + \mathfrak{m}) \\ &= \langle i - 1 \rangle \times (1 + (i-1)\mathbb{Z}_2[i]). \end{aligned}$$

By a basic computation,

$$\begin{aligned} (K_1^\times)^2 &\cong \langle -2i \rangle \times (1 + 2(i-1)\mathbb{Z}_2[i] - 2i\mathbb{Z}_2[i]) \\ &= \langle -2i \rangle \times (1 + 2\mathbb{Z}_2[i]) \\ &= \langle \pi_{K_1}^2 \rangle \times (1 + \mathfrak{m}^2) \end{aligned}$$

Thus, we obtain that

$$\begin{aligned} K_1^\times/(K_1^\times)^2 &= \langle \pi_{K_1} \rangle / \langle \pi_{K_1}^2 \rangle \times (1 + \mathfrak{m})/(1 + \mathfrak{m}^2) \\ &= \langle i - 1 \rangle \times \langle i \rangle \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{aligned}$$

The norm group $N_1(K) \subseteq K_1$ has index 2, so it is generated by an order 2 subgroup of $K_1^\times/(K_1^\times)^2$. We observe that these subgroups are precisely those generated by i, $i - 1$, and $-1 - i$. Furthermore, the uniformizer $\pi_K = \zeta_8 - 1$ must map to a uniformizer of K_1 under the norm map, so because

$$N_1(\pi_K) = (\zeta_8 - 1)(-\zeta_8 - 1) = -(i - 1)$$

and $-1 = i^2$ is a norm in K_1, we conclude that

$$N_1(K) = (K_1^\times)^2 \times \langle i - 1 \rangle.$$

Moreover, we determine the quotient group to be

$$K_1^\times/N_1(K) = \langle i \rangle.$$

Thus, up to norm, we have that $\alpha_1 \equiv i$.

Now consider $K_2 = \mathbb{Q}_2(\sqrt{2})$. Repeating the process, observe that K_2 has uniformizer $\pi_{K_2} = \sqrt{2}$, so the unit group of K_2 has the structure

$$\begin{aligned} K_2^\times &\cong \langle \pi_{K_2} \rangle \times (1 + \mathfrak{m}) \\ &= \langle \sqrt{2} \rangle \times (1 + \sqrt{2}\,\mathbb{Z}_2[\sqrt{2}]). \end{aligned}$$

Again by computation,

$$\begin{aligned} (K_2^\times)^2 &\cong \langle 2 \rangle \times (1 + 2\sqrt{2}\,\mathbb{Z}_2[\sqrt{2}] + 2\mathbb{Z}_2[\sqrt{2}]) \\ &= \langle \pi_{K_2}^\times \rangle \times (1 + \mathfrak{m}^2). \end{aligned}$$

Thus, we obtain that

$$\begin{aligned} K_2^\times/(K_2^\times)^2 &= \langle \pi_{K_2}\rangle/\langle \pi_{K_2}^2\rangle \times (1+\mathfrak{m})/(1+\mathfrak{m}^2) \\ &= \langle \sqrt{2}\rangle \times \langle 1+\sqrt{2}\rangle \\ &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \end{aligned}$$

As with before, the norm group $N_2(K) \subseteq K_2$ has index 2, and the subgroups of $K_2^\times/(K_2^\times)^2$ are generated by $\sqrt{2}$, $1+\sqrt{2}$, and $2+\sqrt{2}$. Given the uniformizer π_K, we have that

$$\begin{aligned} N_2(\pi_K) &= (\zeta_8 - 1)(\zeta_8^{-1} - 1) \\ &= 2 - (\zeta_8 + \zeta_8^{-1}) \\ &= 2 - \sqrt{2} \\ &= \frac{2}{2+\sqrt{2}}. \end{aligned}$$

We note that since $2+\sqrt{2}$ is a generator of one of our subgroups, so is $(2+\sqrt{2})^{-1}$, and because 2 is a norm, we have that the norm group is

$$N_2(K) = (K_2)^\times \times \langle 2+\sqrt{2}\rangle$$

and that the quotient group is computed to be

$$K_2^\times/N_2(K) = \langle \sqrt{2}\rangle = \langle 1+\sqrt{2}\rangle$$

Thus, up to norm, $\alpha_2 \equiv \sqrt{2}$.

It remains to determine some β such that we obtain a valid triple. For later use, it will help to glean some information about the field $\mathbb{Q}_2$.

Proposition 9. Let $a \equiv 1 \pmod{8}$. Then a is a square in $\mathbb{Z}_2$.

Proof. We apply Newton's method using $f(x) = \frac{1}{ax^2} - 1$, which will return the root $1/\sqrt{a}$, from which we can simply multiply by a. Given $f'(x) = -\frac{2}{ax^3}$, we have the iteration

$$\begin{aligned} x_{n+1} &= x_n - \frac{f(x_n)}{f'(x_n)} \\ &= x_n + \frac{1-ax_n^2}{ax_n^2} \cdot \frac{ax_n^3}{2} \\ &= x_n + \frac{x_n - ax_n^3}{2} \\ &= \frac{3x_n - ax_n^3}{2}. \end{aligned}$$

Observe that if $x_n \equiv 1 \pmod{8}$, then because $a \equiv 1 \pmod{8}$, the quantity $3x_n - ax_n^3 \equiv 2 \pmod{8}$ such that division by 2 produces an element of $\mathbb{Z}_2$. Moreover, $x_{n+1} \equiv 1 \pmod{8}$, so the iteration may be continued to convergence. Thus, taking $x_0 = 1$, we obtain a square root of a in $\mathbb{Z}_2$. $\square$

6 References

AtWaGC Michael Atiyah and C.T.C. Wall. "Cohomology of Groups". *Algebraic Number Theory: Proceedings of an Instructional Conference* (2010), ed. J.W.S. Cassels and Albrecht Fröhlich. London Mathematical Society.

ConCE Brian Conrad. *Extensions and* $H^2(G, A)$ (2011). Handout for Math 210B. math.stanford.edu/~conrad/210BPage/handouts/Cohomology&Extensions.pdf

ConGE Brian Conrad. *Group Cohomology and Group Extensions* (2012). Handout for Math 210B. math.stanford.edu/~conrad/210BPage/handouts/gpext.pdf

MilANT James Milne. *Algebraic Number Theory* (v3.08, 2020). jmilne.org/math/CourseNotes/ant.html

MilCFT James Milne. *Class Field Theory* (v4.03, 2020). jmilne.org/math/CourseNotes/cft.html

NeuANT Jurgen Neukirch. *Algebraic Number Theory* (3rd ed., 1991). Graduate Texts in Mathematics, Springer.

SerLF Jean-Pierre Serre. *Local Fields* (1st ed., 1991). Graduate Texts in Mathematics, Springer.