

# 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  $\text{Gal}(L/K)$  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

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Preliminaries</b>	<b>2</b>
2.1	Local Fields . . . . .	2
2.2	Group Cohomology . . . . .	4
2.3	Local Class Field Theory . . . . .	4
2.4	Extensions . . . . .	4
<b>3</b>	<b>Development of Theory</b>	<b>5</b>
3.1	Cyclic Extensions . . . . .	5
3.2	Bicyclic Extensions . . . . .	7
3.3	Some Remarks on Abelian Extensions . . . . .	10
<b>4</b>	<b>Extensions of <math>\mathbb{Q}_p</math></b>	<b>11</b>
<b>5</b>	<b>Extensions of <math>\mathbb{Q}_2</math></b>	<b>11</b>
5.1	Some Explicit Results . . . . .	11
<b>6</b>	<b>References</b>	<b>14</b>

## 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  $G = \text{Gal}(L/K)$ , 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  $\pi$  of  $\mathfrak{m}$  is called a *uniformizer* of  $K$ .
- the residue field  $k$  of  $K$  is given by  $\mathcal{O}_K/\mathfrak{m}$ .

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  $\pi_K$ , 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  $\mu_{q-1}$  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  $x \in L$ ,

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

Moreover, this extension of the absolute values is unique.

**REMARK 1.** If  $x \in K \subseteq L$ , then  $\mathrm{Nm}_{L/K}(x) = x^n$ , 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  $\ell/k$  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

The following is adapted from Michael Atiyah's section on group cohomology as presented in J.W. Cassels and A. Frohlich's *Algebraic Number Theory* (ref. [CaFr]).

## 2.3 Local Class Field Theory

## 2.4 Extensions

The following is adapted from Brian Conrad's article on group extensions (ref. [Conr]).

### 3 Development of Theory

Given an extension of local fields  $L/K$ , we are interested in classifying all Galois gerbes up to equivalence. Let  $G = \text{Gal}(L/K)$ , 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  $\sigma$  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 4.** Let  $f \in \mathcal{E}$  be a lift of  $\sigma \in G$ . Define  $\alpha = f^n$ .

Where appropriate, we will subscript  $\alpha$  to represent lifts of different generators of  $G$ .

#### 3.1 Cyclic Extensions

When  $L/K$  is a cyclic extension generated by  $\sigma$ , 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 5.** 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  $a \in L^\times$ ,  $f a f^{-1} = \sigma(a)$ ,
- $\alpha = f^n \in L^\times$ .

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

**PROPOSITION 3.** Let  $G = \text{Gal}(L/K)$  be generated by  $\sigma$  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 □

Given an extension characterized by  $\alpha$ , 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  $\sigma$ , we obtain that

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

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

Noting this setup, we define an equivalence relation for  $\alpha$  as follows:

**DEFINITION 6.** Elements  $\alpha$  and  $\alpha'$  are equivalent if there exists  $x \in L^\times$  such that

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

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

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

**THEOREM 3.** 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  $\alpha$ .

PROOF. Because  $\alpha$  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  $\sigma_1$  and  $\sigma_2$  be respective generators, with respective orders  $n_1$  and  $n_2$ . In the cyclic case, the quantity  $\alpha$  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  $\sigma_1, \sigma_2$  commute with each other. To do this, we will introduce a new quantity.

**DEFINITION 7.** 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 8.** For a given index  $i$ , denote the map  $N_i : L^\times \rightarrow L^{\langle \sigma_i \rangle}$  as

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

We immediately note some properties of  $\beta$ .

**PROPOSITION 4.** The element  $\beta$  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  $\beta$  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  $\alpha_1$  is fixed by  $\sigma_1$ . 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  $\sigma_2$  may act. However, we may ignore this specification by working purely with  $f_1$  and  $f_2$ , defining the “action” of  $\sigma_2$  to work by its defined conjugation.

**COROLLARY 1.** Let  $\beta$  be as given. Then  $\text{Nm}(\beta) = 1$ .



PROOF. We observe that

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

Thus, the result follows.  $\square$

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

**DEFINITION 9.** Let  $L/K$  be bicyclic with  $G = \langle \sigma_1 \rangle \times \langle \sigma_2 \rangle$ , where  $\sigma_1$  and  $\sigma_2$  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  $\alpha$ 's and  $\beta$  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  $\beta$ , our cocycle formula becomes slightly more complex.

**PROPOSITION 5.** Let  $G = \text{Gal}(L/K)$  be generated by  $\sigma_1, \sigma_2$  with respective orders  $n_1, n_2$ . The 2-cochain defined by

$$mmm$$

where  $\chi_i$  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.  $\square$

**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  $\alpha_i$  is the same as discussed in the cyclic case. Moreover, our  $\beta$  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 10.** 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

$$\begin{aligned} \alpha_i &= N_i(x_i) \cdot \alpha'_i, \\ \beta &= \frac{x_1}{x_2} \cdot \frac{\sigma_1(x_2)}{\sigma_2(x_1)} \cdot \beta'. \end{aligned}$$

### 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  $G = \text{Gal}(L/K) = G_1 \times \cdots \times G_r$  is a decomposition into cyclic groups generated by  $\sigma_1, \dots, \sigma_r$ . In the bicyclic case, we represented the commutator between lifts of  $\sigma_1, \sigma_2$  using  $\beta$ ; to extend this, we will introduce a  $\beta$  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 6.** 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,

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

Thus, the relation holds.  $\square$

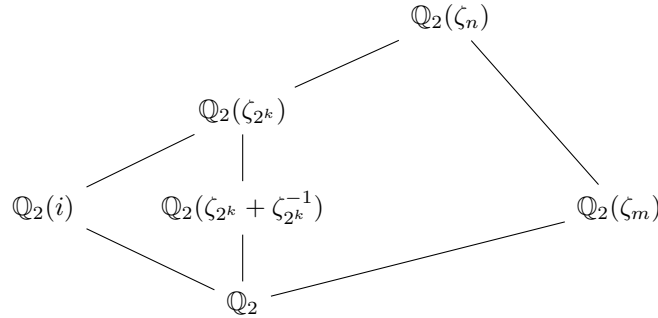
By taking a set-theoretic lift as described in [ConGE], we may explicitly construct a cocycle in terms of  $(\alpha_i, \beta_{ij})$  and the generators  $\sigma_i$  of  $G$ . However, because it is not relevant to the remainder of the paper, we have elected not to do so.

## 4 Extensions of $\mathbb{Q}_p$

Let  $p$  be an odd prime.

## 5 Extensions of $\mathbb{Q}_2$

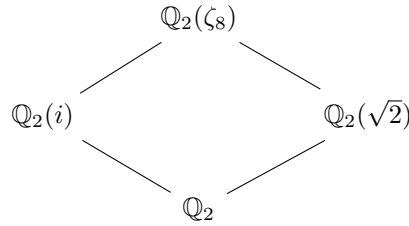
We now consider the special case of  $p = 2$ . We observed that when  $p$  is an odd prime, a cyclotomic extension of  $\mathbb{Q}_p$  is bicyclic. However, in the case of  $\mathbb{Q}_2$ , our diagram of fields splits as



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

### 5.1 Some Explicit Results

Consider the specific case of  $K = \mathbb{Q}_2(\zeta_8) = \mathbb{Q}_2(i, \sqrt{2})$ , with the following diagram of fields:



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  $\text{Gal}(K/\mathbb{Q}_2)$  is generated by the automorphisms

$$\begin{aligned}\sigma_1 : \sqrt{2} &\mapsto -\sqrt{2} \\ \sigma_2 : i &\mapsto -i\end{aligned}$$

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  $\text{Nm}(L^\times)$  is of index  $n$  in  $K^\times$ .

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

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

where  $G^{\text{ab}}$  is the maximal abelian quotient of  $G$ . Because  $G$  is abelian,  $\text{Nm}(L^\times)$  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  $\text{Gal}(L/K)$ , we have that for  $x \in K^\times$ ,  $\text{Nm}(x) = x^n$ , and so the  $n$ -th powers  $(K^\times)^n$  form a subgroup of  $\text{Nm}(L^\times)$ .

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

**PROPOSITION 7.** 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](http://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](http://math.stanford.edu/~conrad/210BPage/handouts/gpext.pdf)
- MilANT       James Milne. *Algebraic Number Theory* (v3.08, 2020).  
[jmilne.org/math/CourseNotes/ant.html](http://jmilne.org/math/CourseNotes/ant.html)
- MilCFT       James Milne. *Class Field Theory* (v4.03, 2020).  
[jmilne.org/math/CourseNotes/cft.html](http://jmilne.org/math/CourseNotes/cft.html)
- SerLF        Jean-Pierre Serre. *Local Fields* (1st ed., 1991). Graduate Texts in Mathematics, Springer.