# 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

# 2 Preliminaries

## 2.1 Local Fields

## 2.2 Group Cohomology

## 2.3 Extensions

# 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 $\sigma$ 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 1. 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 $\mathcal{E}$.

THEOREM 1. 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 $a \in L^\times$, $faf^{-1} = \sigma(a)$,
- $\alpha = f^n \in L^\times$.

PROOF. TBD □

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

PROPOSITION 1. Let $G = \mathrm{Gal}(L/K)$ 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

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

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

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

DEFINITION 2. Elements $\alpha$ and $\alpha'$ 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.

### 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 3. 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 4. 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 $\beta$.

Proposition 2. 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. □

REMARK 1. 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 $\mathrm{Nm}(\beta) = 1$.

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. □

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

THEOREM 2. 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 $a \in L^\times$, $f_i a f_i^{-1} = \sigma_i(a)$,
- $\alpha_i = f_i^{n_i} \in L^{\langle\sigma_i\rangle}$,
- $N_1(\beta) = \alpha_1/\sigma_2(\alpha_1)$,
- $N_2(\beta^{-1}) = \alpha_2/\sigma_1(\alpha_2)$.

PROOF. TBD. □

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 3. Let $G = \mathrm{Gal}(L/K)$ 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. □

REMARK 2. 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 5. 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 $\sigma_1, \sigma_2$ 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 4. Suppose $i < j < k$. Then

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

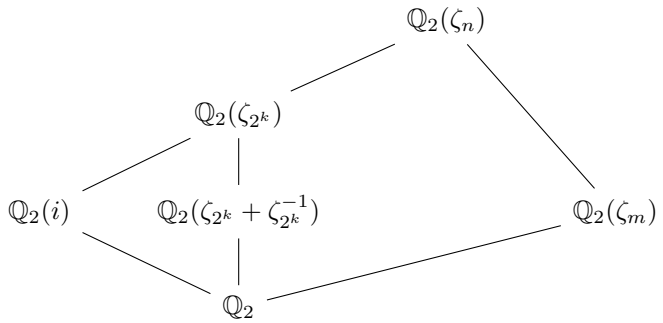
Proof. TBD. □

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

Let $p$ be an odd prime.

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

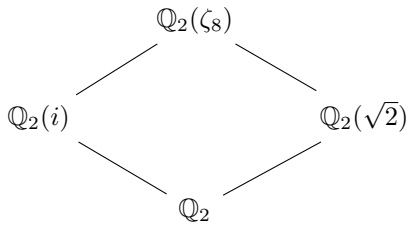
We now consider the special case of $p = 2$. We observed that when $p$ is an odd prime, a cyclotomic extension of $\mathbb{Q}_p$ is bicyclic. However, in the case of $\mathbb{Q}_2$, our diagram of fields splits as




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 $\mathrm{Gal}(K/\mathbb{Q}_2)$ 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 $G^{\mathrm{ab}}$ is the maximal abelian quotient of $G$. Because $G$ is abelian, $\mathrm{Nm}(L^\times)$ has index $n$. □

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 $\pi_K$, 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 5. 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 $\mathbb{Z}_2$. □

## 6 References